Framework for Risk Management in Outsourcing Arrangements by Financial Institutions

BANKING POLICY & REGULATIONS DEPARTMENT
STATE BANK OF PAKISTAN

Table of Contents

ABBREVIATIONS/ACRONYMS

AOF	Account Opening Forms
ATMs	Automated Teller Machines
BCP	Business Continuity Plan
BPRD	Banking Policy & Regulations Department
DFIs	Development Finance Institutions
e-CIB	Electronic Credit Information Bureau
FIs	Financial Institutions
IT	Information Technology
JD	Job Descriptions
MFBs	Microfinance Banks
MIS	Management Information System
NDA	Non-Disclosure Agreement
PBA	Pakistan Banks' Association
PSO/PSP	Payment System Operator/Payment Service Provider
SBP	State Bank of Pakistan
SLA	Service Level Agreement
SOP	Standard Operating Procedures

DEFINITIONS

Affiliated entity: — An entity in which an FI has beneficial shareholding of more than 20%.

Confidential customer information: — Information that relates to FI's customers/borrowers including customers' KYC (identity) data/information, details of accounts, particulars, transaction details and dealings with the FIs, but does not include any information that is public, anonymized, or encrypted in a secure manner such that the identities of the customers cannot be readily inferred.

Core banking functions: — Management high risk functions that require effective involvement of board of directors and senior management on continuing basis

Country Head: — Person occupying the position of Chief Executive Officer and include President, acting President, Managing Director, Country Head of Foreign bank, Executive assuming charge of the bank for interim period or by whatever name called, and whether under a contract of service or otherwise.

Group: — Persons, whether natural or juridical, if one of them or his dependent family members or its subsidiary, have control or hold substantial ownership interest over the other.

In-sourcing: — A business in which work that would otherwise have been contracted out is performed in-house. For example, an IT outsourcing provider may be hired to service a company's IT department while working inside the company's facilities. In addition to contracting an entire team of workers from an outsourcing provider, outside experts are sometimes hired as consultants (to improve certain processes etc.) and the internal staff thereafter implements their recommendations.

Material outsourcing: — An outsourcing arrangement which, if disrupted, has the potential to significantly impact an institution's business operations, reputation or profitability. Material functions are those that are fundamental to the carryout the business of the FIs.

Outsourcing: — Use of a third party (affiliated entity or un-affiliated) to perform activities, functions or processes normally to save money, time and/or use the skills/technology of another entity on a continuing basis that would normally be undertaken by FIs, now or in the future. However, it will not cover consultancy services, purchase contracts for tangible/intangible items, for example, contracts to purchase standardized products such as furniture, Software/IT solutions, Automated Teller Machines (ATM) etc.

Outsourcing agreement: — A written agreement setting out the contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in an outsourcing arrangement.

Personally Identifiable Information (PII): — Personally Identifiable Information or PII means any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier.

Regulator: — The term regulator refers to all supervisory and regulatory authorities that authorize firms to undertake any regulated activity and supervise the same.

Regulated entity: — An entity authorized to carry out any activity by a regulator.

Service provider: — Any party which provides a service to the institution, including any entity within the FI's group, whether it is located in Pakistan or elsewhere.

Sub-contracting: — An arrangement where a service provider which has an outsourcing arrangement with an institution, further outsources the services or part of the services covered under the outsourcing arrangement to another service provider.

Third party employees: — Employees/staff performing services for the FIs under an insourcing/outsourcing arrangement and which are not on the regular and/or contractual payroll of the FIs.

Third party service provider or Third party or Service provider: — The entity which is undertaking the outsourced activity on behalf of the Financial Institution.

I. INTRODUCTION

(a) Financial Institutions (FIs) are increasingly using third party services to carry out activities, functions and processes as outsourcing arrangements to meet new & complex challenges like innovation in technology, increasing competition, economies of scale and improvement in quality of service to stakeholders (i.e. customers, depositors or investors). The practice, however, increases their dependence on third parties and consequently impacts their risk profile. With the objective to enable FIs to effectively manage the risks arising out of outsourcing, State Bank of Pakistan has updated the Guidelines on Outsourcing Arrangements issued vide BPRD Circular No. 09 of 2007. This framework, however, does not allow outsourcing of core banking functions/activities.

(b) The FIs, while deciding to outsource any function, activity or process shall ensure that outsourcing should neither reduce the protection available to depositors or investors nor be used as a way of avoiding compliance with regulatory requirements. It will be the responsibility of the FIs to ensure compliance with all legal\regulatory requirements issued and amended from time to time, while entering into any outsourcing arrangement.

II. APPLICABILITY

(a) The guidelines contained in this framework are applicable on all outsourcing arrangements entered into by Commercial Banks, Islamic Banks, Microfinance Banks (MFBs) and Development Financial Institutions (DFIs) hereinafter jointly referred to as Financial Institutions (FIs).

(b) This framework is applicable on all outsourcing arrangements of FIs with local as well as off-shore[1] service providers.

(c) All new outsourcing arrangements by FIs shall be governed under this framework. The outsourcing arrangements already in place by the FIs shall be streamlined to comply with this framework latest by June 30, 2018.

III. POLICY FOR OUTSOURCING ARRANGEMENTS

(a) The FIs shall develop outsourcing policy to be approved by their Board of Directors. The outsourcing policy shall, at a minimum, include Roles &

[1] Outside Pakistan

Responsibilities of all stakeholders, Materiality Assessment Criteria, , Vendor Management (due diligence, on-boarding, contractual requirements, monitoring, training & development etc), Risk Assessment & Mitigation measures for all types of outsourcing risks, classification of core & non-core activities for each function, contingency planning and an exit strategy from the outsourcing arrangement etc.

(b) The FIs shall ensure effective implementation of policy and formulation of detailed Standard Operating Procedures (SOPs)/Procedural Manual for outsourcing arrangements. The outsourcing policy shall be disseminated across the institution for information, understanding and compliance.

(c) The FIs shall ensure that the staff responsible for outsourcing arrangements is trained to have reasonable understanding on the outsourcing and the outsourced functions/activities.

(d) The exceptions or deviations in the policy shall be escalated to the board or its sub-committees in the immediate next meeting.

IV. MATERIAL OUTSOURCING

(a) It is responsibility of the FIs to assess whether the function/activity/process being outsourced is material or not. The FIs shall assess various factors while deciding whether a function to be outsourced is material or not, including but not limited to:-

(i) The importance of the business activity to be outsourced in terms of its contribution to income and profit.

(ii) The impact on the institution's reputation and brand value, and ability to achieve its business objectives, business continuity, strategy and plans, should the service provider fail to perform the service.

(iii) The impact on the institutions' customers, should the service provider fail to perform the service or encounter a breach of confidentiality or security.

(iv) The cost of the outsourcing as a proportion of total operating costs of the FI.

(v) The degree of difficulty, including the time taken, in finding an alternative service provider or bringing the business activity in-house.

(vi) The aggregate exposure to a particular service provider in case where

an institution outsources various functions to the same service provider.

(vii) The ability to maintain appropriate internal controls and meet regulatory requirements due to operational problems faced by the service provider.

(viii) The affiliation or other relationship between the FI or group and the service provider.

(ix) Any other factor that the financial institution may consider appropriate for evaluating the materiality.

(b) Material outsourcing arrangements shall be approved by the board.

(c) The FIs shall list all the material outsourcing arrangements of a financial year in their annual audited accounts including the nature of service, name of the service provider and estimated cost of outsourcing etc.

V. GOVERNANCE OF OUTSOURCING ARRANGEMENTS

A. Responsibilities of the Board of Directors

1. The functions of the board, in case of a foreign bank working as a branch office in Pakistan, can be delegated to and performed by a local or regional management committee.

2. The Board of Directors shall:-

(i) Approve a framework to evaluate the risks and materiality of all existing and prospective outsourcing arrangements and the policies that apply to such arrangements.

(ii) Set a suitable risk appetite to define the nature and extent of risks that the FI is willing and able to assume from its outsourcing arrangements.

(iii) Lay down appropriate approval authorities and limits for outsourcing arrangements consistent with its established strategy and risk appetite.

(iv) Ensure that senior management establishes appropriate governance structure and processes for sound and prudent outsourcing risk management.

(v) Decide on business activities of a material nature to be outsourced and approving such arrangements.

B. Responsibilities of the Senior Management

The senior management shall:-

(i) Regularly review overall performance of service providers on outsourced activities.

(ii) Evaluate the materiality and risks from all existing and prospective outsourcing arrangements, based on the framework approved by the board.

(iii) Develop sound and prudent outsourcing policies and procedures that are commensurate with the nature, scope and complexity of the outsourcing arrangements.

(iv) Monitor and maintain effective control of all risks from material outsourcing arrangements on an institution-wide basis.

(v) Carry out evaluation and due diligence of the service providers before entering into any outsourcing arrangement.

(vi) Ensure that the outsourced functions are carried out as per the existing legal and regulatory framework.

(vii) Ensure that contingency plans, based on realistic and probable disruptive scenarios, are in place and tested on periodical basis.

(viii) Ensure that agreements with the service provider/vendor contain all necessary clauses, including regulatory requirements, which protect the interest of the bank.

(ix) Ensure that proper mechanism is in place for ongoing monitoring of the service provider as per the terms and conditions of SLA.

(x) Maintain centralized database of all outsourcing activities and regularly updating the board about the risks arising from its material outsourcing activities.

(xi) Ensure that FI has a dispute escalation and its resolution mechanism in place for outsourcing arrangement.

C. Responsibilities of Internal Audit

The FI's internal audit function shall regularly review outsourcing arrangements and report any deviation from the institution's outsourcing policy to the board or it's Audit Committee.

VI. RISK MANAGEMENT IN OUTSOURCING ARRANGEMENTS

A. Risk Assessment

(i) The FIs shall manage the risks associated with outsourcing arrangements. In this regard, the ongoing assessment by the FI shall also include operational risk and the concentration risk associated with all its outsourcing arrangements. Further, FI shall inform SBP within two working days of any material or adverse[2] development with regard to its outsourcing arrangement.

(ii) The FIs shall assess the risks arising out of outsourcing of business activity and ensure that they are adequately captured within their overall risk management framework. For this purpose, the FIs shall:

(a) Define the business requirements for the functions or activities to be outsourced

[2] Adverse development includes enterprise wide disruption in the provision of outsourced services causing regulatory non-compliance and/or affecting or compromising customer data/information and services.

and assess the risk of outsourcing those functions or activities and establish appropriate measures to manage and control the identified risks.

(b) Analyze the impact of the outsourcing arrangement on the overall risk profile of the institution, and ensure that there are adequate internal expertise and resources to mitigate the risks identified.

(c) Address all risks associated with business activity, as if it would have been performed "in house".

(d) Take into consideration the criticality of the services to be outsourced and the capability of the service provider

(e) Conduct risk assessment of outsourced activities or functions on periodic basis.

B. Service Provider Due Diligence & Selection

(i) Firstly, the FIs shall internally carry out due diligence of the business activity to be outsourced. They shall then perform a detailed due diligence of the service provider before finalizing outsourcing arrangement.

(ii) The due diligence process of service provider shall encompass assessment of all areas including its experience, technical competence, financial strength, reputation, existence of control framework, performance standards, managerial skills, policies & procedures, reporting &monitoring environment and business continuity planning.

(iii) The due diligence shall also address other issues, such as potential conflicts of interest in case service provider is related/affiliated party, or where it provides similar services to competitors. The FI's shall also identify all potential and actual conflicts in the FI are outsourcing operations to ensure that the conflicts are identified and avoided or prudently managed.

(iv) In cases where only one service provider is operating for a certain outsourcing activity, FIs shall enhance the due diligence process to identify and mitigate new risks.

(v) The due diligence and selection procedures shall also take into account the physical and IT security controls the service provider has in place, the business reputation and financial strength of the service provider[3], including the ethical and professional standards held by the service provider and its ability to meet obligations as per the requirements of the FI.

(vi) Onsite visits to the service provider, and where possible, independent reviews and market feedback shall also be obtained to supplement the institution's assessment. Onsite visits shall be conducted by persons who possess the requisite knowledge

[3] As per BPRD Circular No. 13 of 2014 on Financial Integrity Requirements for service providers to the Banks/MFBs/DFIs

and skills to conduct the risk assessment.

(vii) Any adverse findings from the due diligence shall be considered in light of their relevance and impact to the outsourcing arrangement.

(viii) The result of this due diligence shall be documented and presented for review by internal/external auditors and SBP as and when required.

C. Outsourcing Agreement

(i) All outsourcing arrangements shall be undertaken using a legally binding written agreement(s). The contract, at a minimum, shall include the following areas:

(a) Service levels and performance requirements;

(b) Audit and monitoring procedures;

(c) Business continuity plans;

(d) Default arrangements and termination provisions;

(e) Pricing and fee structure;

(f) Dispute resolution arrangements;

(g) Complaint handling procedures;

(h) Liability and indemnity;

(i) Confidentiality, privacy and security of information.

(ii) The FIs, while entering into agreements with service providers, shall ensure that:

(a) The agreement defines the rights and responsibilities of both parties and contains adequate and measurable service levels.

(b) The agreement with related parties reflects an arms-length relationship. Further entire process from start of engagement till end shall be properly documented.

(c) Service provider's physical and data security standards meet or exceed the FI's standards.

(d) The agreement contains the minimum provisions required under existing laws and SBP rules and regulations including but not limited to timely access to all sorts of information, records, data applications, databases, networks/ network devices and systems is available to internal/external auditors and SBP inspection teams as and when required.

(e) The agreement allows for renegotiation and renewal to enable the FI(s) to retain an appropriate level of control over the outsourcing arrangement.

(f) The agreements with third parties do not include the services, which are not allowed in this guideline.

(g) The agreements have clauses setting out the rules and limitation/prohibition

on subcontracting.

(h) An annual review of the outsourcing agreements is performed to assess that terms of the agreement are in line with current market practices and standards.

(i) The service provider delivers a level of service that meets the needs of the FIs.

(j) Penalty[4] clause in the agreement in case service provider fails to provide services as per mutually agreed timelines and service availability.

(k) The agreement binds the service providers to report any change in their ownership structure, key management/partners/directors immediately to the FI.

(l) The agreement sets out the procedures to enable FIs to effectively monitor the performance of the service provider.

(iii) The FIs shall increase the cost of outsourced activity only after conducting comparative analysis of the rising cost.

(iv) No outsourcing arrangement shall be made with the party having relationship with the management/employees of the FI, which may create a conflict of interest.

(v) Each agreement shall also address issues arising from country risks and potential obstacles in exercising oversight and management of the outsourcing arrangements by FIs made with a service provider outside Pakistan.

(vi) The FIs shall have the right to terminate an outsourcing agreement in the event of default, or under circumstances where: (i) service provider undergoes a change in ownership; (ii) service provider becomes insolvent or goes into liquidation; (iii) service provider goes into receivership or judicial management whether in country or elsewhere; (iv) there has been a breach of security or confidentiality; (v) breach of any relevant legal requirement and/or regulatory directive and (vi) there is a demonstrable deterioration in the ability of the service provider to perform the contracted service.

D. Performance Standards

(i) The FIs shall set out service standards in the outsourcing agreement to specify and clarify performance expectations as well as establish accountability for the outsourced activity.

(ii) The FIs shall closely monitor the service provider's compliance with key performance standards keeping in view the following aspects, among others:

(a) Availability and timeliness of services

(b) Confidentiality and integrity of data

[4] Islamic banks may follow relevant appropriate methodology in this regard.

(c) Change control

(d) Security standards compliance, including vulnerability and penetration management

(e) Business continuity compliance

(f) Help desk support

(iii) The FIs shall also monitor the service provider's contractual service standards for backup, record retention, data protection and maintenance and testing of disaster recovery and contingency plans.

E. Ongoing Monitoring

(i) The FIs shall devote sufficient resources to manage and monitor an outsourcing relationship. The FIs can assign the responsibility of managing the outsourcing arrangement to an individual or team/committee. Further, the FIs shall ensure that personnel responsible for monitoring activities shall have the necessary expertise to assess the risks and impacts thereof.

(ii) The FIs shall have access to the necessary records held by the service provider.

(iii) The FIs shall periodically assess risks in service provider relationships to determine which service providers require closer monitoring.

(iv) The FIs shall ensure that effective mechanism is in place to monitor the outsourced activity, particularly the following:

(a) Material problems encountered by the service provider which may impact the FI;

(b) Financial condition and risk profile of the service providers

(c) The results of Business Continuity Plan testing.

(v) The FIs shall ensure that any adverse development arising from any outsourced activity is brought to the attention of the senior management and the board on a timely basis.

(vi) The FIs shall continuously review the outsourcing relationship for modification and/or termination in case of adverse developments.

(vii) In case of material outsourcing, the FIs shall periodically obtain the financial statements, e-CIB and tax returns of the service providers in order to assess the financial integrity and strength of the service provider. Where possible, the institution shall also obtain independent reviews/market feedback on the service provider to supplement its own findings.

F. Contingency Planning

(i) The FIs shall take steps to evaluate and manage the interdependency risk arising

from the material outsourcing arrangements so that they are able to conduct business in the event of a service disruption or failure, or unexpected termination of the outsourcing arrangement or liquidation of the service provider.

(ii) The FIs shall determine that the service provider has in place satisfactory Business Continuity Plans ("BCP") that are commensurate with the nature, scope and complexity of the outsourcing arrangement.

(iii) The FIs shall also require the service provider to notify it of any substantial changes in the service provider's BCP plans and of any adverse development that may substantially impact the services provided to the FI.

(iv) For assurance on the functionality and effectiveness of its BCP plan, FIs shall design and carry out regular, complete and meaningful BCP testing that is commensurate with the nature, scope and complexity of the outsourcing arrangement.

VII. GENERAL CONTROLS

(a) The outsourcing arrangements shall not be considered as delegation of responsibility of FI's management.

(b) The FIs shall not outsource any decision making function and those activities which can breach confidentiality of data/information of the customers/borrowers. For in-sourcing arrangements, the list of critical functions or activities where FIs cannot place / engage the third party employees is given as Annexure-A.

(c) The FIs, before providing data to third party, shall ensure that proposed outsourcing arrangement complies with the relevant statutory requirements related to confidentiality of its customers/clients, specifically the provision of relevant laws, regulations and instructions issued by SBP from time to time.

(d) In case where outsourcing arrangement involves confidential customer information, FIs shall:

i. Seek specific consent of the customer or encrypt or anonymize Personally Identifiable Information (PII) of customers so that their identities cannot be readily inferred.

ii. Retain information of all such cases, which will be reviewed by SBP team during on-site inspection.

(e) The FIs must ensure that outsourcing activity does not violate any statutory/regulatory requirements on Anti-Money Laundering (AML) and record keeping requirements of local as well as foreign jurisdiction.

(f) The FIs shall ensure that up-to-date records relevant to its outsourcing arrangements are maintained and kept available for inspection by the SBP

inspection teams. In case of in-sourcing arrangements, the FI(s) shall also keep record (personal files) of all in-sourced staff.

(g) The FIs may outsource storage/archival of Account Opening Forms (AOF) subject to the condition that appropriate controls are put in place to ensure confidentiality/integrity of customer data/information before transferring such records to the service provider for storage/archival.

(h) The FIs shall develop SOPs in line with legal and regulatory requirements for outsourcing of collection, recovery/repossessions services. Further, FIs shall also adhere to PBA's Guidelines for Collection, Recovery and/or Repossession Agencies.

VIII. REDRESSAL OF GRIEVANCES ABOUT OUTSOURCED ACTIVITIES

(a) The FIs shall have a well defined policy for redressal of complaints of their customers regarding outsourced services. Further, FIs shall also ensure that service provider have mechanism in place to address the grievances of the customers as per policy of the bank.

(b) The FIs shall maintain proper log of the complaints relating to outsourced operations. The same shall be analyzed and escalated to the appropriate level for review. Further, the third party shall be responsible for sharing the information necessary to dispose of complaints within the defined timelines. The complaints record may be considered as one of the important factors at the time of performance evaluation of the service provider and to assess the effectiveness of outsourcing arrangement.

IX. OUTSOURCING OUTSIDE PAKISTAN

(a) Any outsourcing arrangement outside Pakistan, excluding group outsourcing, shall require SBP's prior approval subject to approval of the Country Head. All such requests shall be signed by the Head of compliance and include details of the functions to be outsourced, rationale for the outsourcing, details relating to the proposed service provider, agreement with the service provider, business continuity plan, disaster recovery arrangements and a legal opinion that the arrangement does not violate any relevant local law.

(b) The FIs shall conduct due diligence including but not limited to review of

(i) the regulatory requirements of service providers' country

(ii) political, economic and social conditions of the service providers' country

(iii) diplomatic relationships, government policies, legal requirements in service providers' country

(iv) events that may limit the foreign service provider's ability to provide the services and

(v) any additional risk factor(s) that may needs to be made part of risk management framework.

(c) The FIs, as an ongoing due diligence mechanism; shall review the service provider at least on an annual basis to ascertain its ability to deliver the outsourced services in the manner agreed as per SLA.

(d) As a part of risk management of outsourcing arrangements outside Pakistan, the FIs shall also take into account its ability to effectively monitor the service provider, and execute its business continuity management plans and exit strategy of the outsourced arrangement.

(e) No offshore outsourcing arrangement shall be allowed in case the offshore service provider is not a regulated entity. FIs shall obtain written undertaking from the service provider that it is a regulated entity and, if required, shall provide access of its operations to SBP.

(f) Outsourcing shall not be allowed to entities or jurisdictions where visits by the staff of the FIs, their external auditors or SBP officials will be impractical / prohibited. In the event SBP is prevented, for whatever reason, from accessing the service provider or its records relating to outsourced function, SBP can direct the FIs to discontinue such outsourcing arrangements.

(g) If SBP so requires, the service providers must give consent of its home regulator to release any relevant information in relation to its operations that the SBP would wish to receive and in no case should it be prohibited, implicitly or explicitly, from doing so.

(h) Sub-contracting of offshore outsourcing arrangements is not allowed. SBP reserves the right in all outsourcing cases to review proposals or restrict the FIs to enter/stop any off-shore outsourcing agreement with any party.

(i) The FIs shall ensure that all information relating to outsourcing outside Pakistan is available domestically and is also available for review or inspection by SBP at any time.

(j) The FIs shall carry out audit of the outsourced activities and submit audit findings to SBP as and when required.

X. GROUP OUTSOURCING

(a) Group outsourcing is defined as arrangement where Financial Institutions including Foreign Banks' branches enter outsourcing arrangements including technological

support services from their parent Financial Institutions/ subsidiaries/ Head Offices or other branches of Foreign Banks/ related group entities formulated for providing specialized services to group companies inside or outside Pakistan.

(b) The instructions in this section are applicable to all outsourcing arrangements with the group companies as defined in para (a) above.

(c) Group Outsourcing shall be the part of 'Outsourcing Policy' of FI(s) which will include detailed criteria for obtaining technological support and other support services from group companies. The criteria shall, at a minimum, include nature of services required from group, criteria for need analysis and risk assessment of such arrangement, terms & conditions to be covered in the agreement with group companies, pricing, primary & DR locations, contingency planning and mechanism for ongoing monitoring of terms & conditions of agreement etc.

(d) All outsourcing arrangements with group shall be approved by FI(s) in line with their 'Outsourcing Policy'. For outsourcing arrangement involving customers' information, FIs shall:

  (i) Seek specific consent of the customers or encrypt or anonymize Personally Identifiable Information (PII) of customers so that their identities cannot be readily inferred.

  (ii) Retain information of all such cases, which will be reviewed by SBP team during on-site inspection.

(e) FI (s) shall obtain legal opinion before entering into outsourcing agreement that the arrangement with group entity does not violate any law.

(f) Security, integrity, confidentiality and liability of data/information including confidential customer information and compliance with laws and regulations of host country shall be the sole responsibility of the FI(s)'s Pakistan Operations.

(g) FI(s) shall ensure that technology support services arrangements comply with information/cyber security standards and relevant provisions of SBP's Enterprise Technology Governance & Risk Management Framework issued vide BPRD Circular No. 05 of 2017.

(h) For obtaining technological/support services from group, FI(s) shall sign a written legally binding contract/Service Level Agreement (SLA) with the group companies covering at a minimum: -

  (i) Description of services;

  (ii) Roles and responsibilities of each party;

  (iii) Confidentiality & right of access;

  (iv) Contingency planning, disaster recovery and business continuity;

(v) Responsibilities in times of Recovery and Resolution of the entity;

(vi) Payment and pricing (if any);

(vii) Unhindered access of data to SBP as and when required;

(viii) Exit strategy, including data access rights to SBP in case any party ceases to exist.

(i) Requests to SBP for remittance against outsourcing services obtained from group companies shall be accompanied by a certificate from external auditor (of the group company) that the basis of costs charged to the FI are in line with the internationally accepted arm's length principles for transfer pricing. While submitting the case, FI shall refer the adopted standard; give detail of the price calculation methodology under the adopted standard and reason for adopting the standard and the particular price calculation methodology. SBP has the right to cap such remittances for an individual bank/subsidiary/branch.

(j) FI (s) shall have Business Continuity Plan in place to minimize the risk of downtime and that procedures are in place to protect against, and deal with, service disruption events. In case of exit from outsourcing arrangement, FI shall have contractual right to continue with the arrangement till such time the FI is able to switch to substitute arrangement.

(k) FI(s) shall ensure that SBP and its internal/external auditors shall have the contractual right to inspect and audit all information relating to the outsourced function at any time without restriction. For this purpose, outsourcing arrangement shall not be allowed to entities or jurisdictions where visits by the staff of the FIs, their external auditors or SBP officials will be impractical / prohibited.

(l) FI(s) shall carry out comprehensive audit for outsourcing arrangements outside Pakistan at least once every two years. However, foreign banks operating in branch mode shall follow the policy of head office for audit of such arrangements.

XI. OUTSOURCING BY FOREIGN BRANCHES OF BANKS[5]

(a) Branches shall also carry out proper due diligence of off-shore service provider. Further, the foreign branches of banks shall also take into account the following areas, as part of its due diligence, on an ongoing basis:

(i) Government policies, political, social, economic conditions in their country of operation;

(ii) Legal and regulatory developments in the foreign country; and

(iii) Ability to effectively monitor the service provider, and execute its business

[5] Branches of Pakistani banks in foreign countries

continuity management plans and exit strategy.

(b) All outsourcing arrangements by foreign branches of domestic banks shall be approved by Head Office.

(c) The foreign branches shall enter into SLA with the service provider in line with requirements as given under section VI (C).

(d) Foreign branches shall formulate comprehensive MIS to inform Head Office about all outsourced activities on periodical basis.

XII. COLLABORATION WITH FINTECHS

(a) All instructions contained in this framework shall also be applicable to FIs entering into collaboration with Fintechs for outsourcing of products and services.

(b) FIs shall not enter into agreement for outsourcing with Fintechs for those services, which come under the domain of Payment System Operators (PSO) and Payment Service Providers in terms of SBP PSO/PSP Rules 2014.

XIII. IN-SOURCING

(a) The following conditions shall apply if any FI enters into in-sourcing arrangements:-

(i) The third party staff shall not be placed in areas/functions where decision-making is involved.

(ii) The third party staff shall not be placed in areas or functions where customer data or information can be compromised.

(iii) The FIs shall ensure that credentials of third party staff are verified before hiring them for insourcing services and that the service provider has robust mechanism to assess/verify the credential of each employee provided to FI. This verification shall be documented and periodically (at least annually) assessed by FI's Internal Audit.

(iv) In case of non-availability of verification of third party employee, the FIs shall conduct verification of their credentials on its own before engaging them. For existing third party employees, FI shall ensure verification of their credentials latest by 30th June, 2018.

(v) In-sourcing arrangements shall be housed within the FIs' premises and under the direct supervision of FIs' officials.

(vi) The FIs shall sign NDA with the third party service provider & their staff before procuring their services.

(vii) In case the third party employee has previously worked with any financial institution, FI shall obtain report about conduct of the employee from his previous employer.

(viii) The FIs shall ensure that the wages and other benefits of third party employees are not below the minimum wage and other benefits declared by the Federal Government from time to time.

(ix) The FIs may hire/acquire the services of third party for printing, stuffing and delivery of statement of customers' accounts subject to the condition that FI's own staff shall supervise the entire process in the bank's premises.

(x) The FIs shall maintain the complete Job Description (JD) of each third party employee.

XIV. INFORMATION TECHNOLOGY OUTSOURCING

(a) IT outsourcing shall be the part of Outsourcing Policy to be approved by the board. IT outsourcing, at a minimum, shall take into account operational & transactional risks; risks to the confidentiality of information; risks to Business Continuity and compliance/regulatory risks.

(b) IT outsourcing of equipment and services within Pakistan (non-material) shall be approved by the IT Steering Committee of the management.

(c) The FIs shall execute Software Escrow Contracts with the software developer or service providers.

(d) IT outsourcing shall not be allowed for critical IT systems/functions and applications of the FIs like core banking applications including Branchless Banking, mobile wallets of Branchless Banking, Main database, databases relating to information of customers, information security and Primary & Disaster Recovery functions.

(e) In case the outsourcing activity or function falls under the purview of SBP's Rules for Payment Systems Operators/ Payment Systems Providers (PSO/PSP), the FIs shall collaborate with licensed PSO/PSP for the said services.

(f) Outsourcing of IT Audit is allowed subject to conditions that:

(i) The arrangement shall be approved by the board or its relevant committee.

(ii) The FIs shall formulate a comprehensive plan for capacity building of their staff enabling them to perform IT Audit internally in future, and

(iii) The existing external auditor of the financial institution shall not be assigned the task of IT audit.

ANNEXURE-A

List of Functions / Activities

Not to Be Performed By Third Party Employees in Financial Institutions

Financial Institutions have made arrangements with vendors whereby third party employees have been placed in banks for performing various non-critical functions / activities. The following is a list of functions / activities, which cannot be performed by third party employees placed in FIs' premises and FIs, must have their own employees for performing all these activities.

1. General Banking

1.1 Account Opening

a) Scrutiny of Documents i.e. Account Opening Form and related documents as required under relevant provisions of Prudential Regulations and FI's own policy
b) Authorization of customer / account data or any other data captured on systems of the FI.

1.2 Account Maintenance and amendments

a) Scrutiny of amendment requests and related documents
b) Authorization of amendments to customer / account data / any other data

1.3 Clearing

Authorization of financial transactions posted to systems for inward clearing and outward clearing (local / foreign currency).

1.4 Tellers/Cashiers

All tellers or designated tellers, cashiers, Branch Service Officers excluding Cash Sorters

1.5 Custody of vaults / lockers and safe keys / instruments

Custodian of vaults, lockers, safe containing cash & documents, cheque books, ATM Cards and any other security stationary.

2. Trade Operations

2.1 Imports

a) Scrutiny of LC Application, Contract Registration & Amendment requests
b) Scrutiny of all import documents received under LC / Contracts and on collection basis

c) Authorization of Data (Financial & Non-Financial) captured in the systems of the FI for issuance, amendments, acceptance and payments of LCs & contracts.
d) Authorization of all SWIFT Messages

2.2 Exports

a) Certification of E-Forms
b) Scrutiny of documents received under LC and on collection basis
c) Authorization of data captured on systems of the FI for LC Advising, Acceptances & payments.
d) Authorization of all SWIFT Messages

2.3 Bank Guarantees

a) Scrutiny of Bank Guarantee issuance / amendment requests and related documents
b) Authorization of data (financial & non-financial) captured on systems of the FI for FI Guarantees issuance, amendments, redemption and cancellation.
c) Authorization of all SWIFT Messages

3. Credit Administration

a) Scrutiny of Loan applications and related documents
b) Authorization of Limits captured in the system
c) Authorization of collateral data captured in the system
d) Credit files maintenance and record keeping
e) DAC (Disbursement Authorization Certificate) Issuance
f) Client stocks / Assets / Site Inspection
g) Safekeeping of securities & Vault management
h) E-CIB reporting supervision and access
i) Lien marking / removal of lien on systems of the FI

4. Consumer Banking

a) Authorization of Financial Transactions
b) Reconciliation of ATM, Debit & Credit Card transactions

5. Treasury

a) All Treasury Front Office, Middle and Back Office activities
b) Financial transactions authorization for settlement of foreign exchange, money market, equity and derivatives settlements at treasury Back Office
c) Authorization of data captured in systems of the FI
d) Deal confirmations
e) Authorization of All SWIFT messages

6. Reconciliation

All types of reconciliation including but not limited to:

a) Nostro Accounts
b) Suspense Accounts
c) Inter-Branch entries

7. Information Technology

a) System and Database Administrations
b) User IDs Management and user limits assignment activities for all IT Systems
c) All positions that have authority to change system parameters for core banking and other critical Systems of the FI.
d) Data Centre Operations & Management
e) Deployed System/Databases & Servers, and Application Deployment and /or Version Management may be added

8. Centralized Activities

The third party Employees cannot be placed on positions which are responsible for authorization of financial transactions and non-financial data.

9. Regulatory reporting

All positions responsible for regulatory reporting must have FIs' own employees.

10. Audit & Risk Management

a) Domestic & Overseas branches / Units / Centralized Functions
b) Internal Shariah Audit Unit (Head Office/ Branches / Units / IBWs / Centralized Functions
c) Financial & Management Audits
d) Business Risk Review
e) Credit Operations Audit
f) Monitoring & Reporting
g) Monitoring Bank-wide Key Risk Indicators
h) Review of new products / procedures with reference to Operational Risk
i) Managing Operational Risk Management Committee

11. Compliance

a) Coordination with SBP Inspection Teams
b) Advisory Role within the Bank
c) Review of Policy, Procedures, Product Programs with respect to Regulatory Guidelines / Regulations.
d) Monitoring / Implementation of Regulatory Guidelines / Regulations
e) Law Enforcement Agencies Coordination
f) Transaction Monitoring Activities

g) Review / Analysis & Closure of Alerts Generated through Transaction Monitoring System
h) On the basis of Review of Alerts filling of STR with Financial Monitoring Unit (FMU)
i) Review of KYC profiles of Customers on an on-going basis
j) Name Scanning of prospective customers, transaction and database of the bank
k) Perform detailed investigations of external frauds pertaining to consumer/ debit card/ net banking and issue investigation report.