

## **DISCUSSION PAPER ON OUTSOURCING OF ACTIVITIES RELATED TO INTERMEDIATION SERVICES**

SEBI has prepared a discussion paper on outsourcing of activities related to the intermediation services. The paper proposes certain principles for outsourcing, and indicates activities presently being outsourced by the intermediaries along with the suggested list of activities which should not be outsourced by them.

Specific comments / suggestions are sought on the following:

- a. The principles for outsourcing,
- b. The activities which can be outsourced,
- c. The activities which cannot be outsourced,
- d. To whom the activities can be outsourced,
- e. The terms of outsourcing,
- f. Responsibilities and obligations of the intermediary and the third party in respect of the outsourced activity towards clients, regulator and market,

The comments / suggestions may be mailed at the following e-mail addresses

On recommendations related to	Comments may be mailed at
Mutual Funds	sanchitj@sebi.gov.in
Portfolio Managers	sksingh@sebi.gov.in
Other Intermediaries	manaswinim@sebi.gov.in

or to the following address

The Deputy General Manager,  
Market Intermediaries Regulations and Supervision Department – 4,  
Securities and Exchange Board of India,  
SEBI Bhavan,  
C-4A, G-Block, Bandra Kurla Complex,  
Mumbai- 400 051

so as to reach latest by February 05, 2011

### **1. INTRODUCTION**

Outsourcing refers to use of a third party – either within or outside the group - by a registered intermediary to perform the activities associated with intermediation services. A third party may be used to perform one or more activities or one or more third parties may be used to perform different activities associated with the intermediation service. Such use may be for a specified period or on a continuing basis. In an extreme form, the third parties may be used to perform all the activities associated with the intermediation service, including legal and regulatory compliances and risk management. This includes use of successive third parties, where the first third party may use the second third party to perform the activities and so on. Over time, the outsourcing arrangements are becoming increasingly complex.

Securities market intermediaries in many jurisdictions are increasingly resorting to outsourcing with a view to reduce costs, and at times, for strategic reasons. This benefits market in terms of better access and better expertise. However, since the third parties may not be subject to the regulatory discipline and the activities and, not the accountability, can be outsourced, outsourcing raises a variety of concerns both for the regulator and the outsourcing intermediary. While it is not desirable to ban outsourcing completely for obvious reasons, the concerns need to be addressed and the outsourcing needs to be organized in an orderly manner. This paper is an attempt to develop guidelines for outsourcing by an intermediary, and not by markets.

## **2. RISKS ASSOCIATED WITH OUTSOURCING**

The risks attached to outsourcing are numerous. They can be grouped into three broad categories: operational, reputational, and legal risks. The operational risks arise because the intermediary loses direct control over the activities and the processes, procedures, systems and people engaged in these activities. Therefore, it fails to exercise due care and diligence if the activity / service falls short of the regulatory standards. The reputational risks arise from failure by the third party to deliver as per regulatory standards which may invite regulatory actions. The legal risks emanate from the failure to enforce the contractual obligations particularly when the contractual relationship is not redefined with every change in basket of activities outsourced or the way these are discharged.

Besides, an intermediary faces a few other potential risks in specific circumstances. For example, it faces country risk if the activities are outsourced to a foreign third party. Changes in foreign government policies as well as political, social, economic and legal conditions in the country where the third party is based or where the contractual relationship has been established could materially affect the outsourcing arrangement. Similarly, the intermediary runs the strategic risk if the third party acquires the necessary skills and infrastructure and develops clientele and then starts intermediation services on its own by acquiring registration from the regulator. It also runs exit-strategy risk as it loses relevant skills and infrastructure preventing it from bringing the activity back in-house. It runs counter party risks if the third party makes inappropriate credit assessments. There is also concentration and systemic risk if a large number of market intermediaries rely upon one or a few third parties for the same activity.

On being satisfied that a person has the required infrastructure and is a fit and proper person, the regulator registers him as an intermediary eligible to render intermediation services. However, the intermediary may outsource the activities to a third person who does not have the infrastructure or may not be a fit and proper person. This may lead to a situation where the market has only third parties to provide intermediation services while the registered intermediaries confine themselves to earning rent. This creates risk for the entire market.

### **3. INTERNATIONAL SUPERVISORY PRINCIPLES**

International Organization of Securities Commission (IOSCO) has prescribed a few principles on outsourcing of financial services for intermediaries. These include principles on: the selection of third party, outsourcing contracts, client confidentiality and security concerns, risks associated due to concentration of outsourced functions, termination procedures, accountability and scope of outsourcing, and the right to access books and records by market intermediary and by the Regulators. These principles are designed to assist an intermediary in determining the steps it should take and factors it should consider when considering outsourcing of activities. These require a regulator to monitor and react to the risks posed by outsourcing of activities by intermediaries.

The seven high-level principles formulated by IOSCO can be grouped broadly into three categories. The first category refers to the policies that registered intermediaries should have in place even before entering an outsourcing agreement. For example, the entity should establish a comprehensive policy for assessing whether and how certain activities can be outsourced, and the intermediary's board of directors should retain direct responsibility for that policy etc. In addition, intermediaries should establish a comprehensive risk-management programme to monitor and address issues arising from the outsourced activities and relationships with the outsourced entities.

The second category addresses concerns surrounding specific outsourcing arrangements. Outsourcing relationships should be governed by written contracts / agreements that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities, and expectations of the parties. The intermediary should also maintain

adequate contingency plans and take appropriate steps to ensure that outsourced entity protects the confidential information, particularly of the clients, from intentional or inadvertent disclosure.

The third category addresses concerns specific to supervisors. Supervisors should take into account outsourcing activities as an integral part of their monitoring responsibilities. Supervisors in charge of the market intermediaries should assure themselves that outsourcing arrangements do not hamper the ability of the intermediary to meet its supervisory requirements; that is, supervisors should be able to obtain promptly any relevant materials regarding outsourced activities and take appropriate enforcement actions.

#### **4. PRINCIPLES FOR OUTSOURCING**

Based on the principles advocated by the IOSCO and the experience of Indian market, it is proposed to have the following nine principles for outsourcing of any intermediation service:

**I. An intermediary seeking to outsource activities should have in place a comprehensive policy to guide the assessment of whether and how those activities can be appropriately outsourced. The board of directors or equivalent body representing the market intermediary shall have the responsibility for the outsourcing policy and related overall responsibility for activities undertaken under that policy.**

The Board of the intermediary (or a delegated body) should lay down a comprehensive policy relating to outsourcing and its implementation. The policy should cover activities or the nature of activities that can be outsourced, the authorities who can approve outsourcing of such activities, and the type of third party to whom it can be outsourced. For example, an activity should not be outsourced if it would impair the supervisory authority's right to assess, or its ability to supervise, the business of the intermediary. The policy should be based on an evaluation of risk concentrations, limits on the acceptable overall level of outsourced activities, risks arising from outsourcing multiple activities to the same entity, etc. Further, the Board should mandate a regular review of outsourcing policy for such activities and the arrangements made in that regard by the intermediary, especially the factors in deciding the soundness of continuing with the existing policies in the wake of changing business environment. It should also have overall responsibility for ensuring that all ongoing outsourcing decisions taken by the intermediary and the activities undertaken by the third-party, are in keeping with its outsourcing policy.

The intermediary must also have in place policies that ensure its ability to oversee effectively the activity being outsourced. An appropriate governance structure with clearly defined roles and responsibilities on the part of the intermediary should exist throughout the engagement process and the contract term. The intermediary must take appropriate steps to ensure its ability to comply with the legal and regulatory requirements, in both its home and host countries, as applicable.

Once the policy for outsourcing has been laid down by the Board of the intermediary, its senior management should review the policies and the outsourcing arrangements periodically, including the quality of work rendered by the third party in the past and emergence of new material risks, and submit a feedback to the Board. It is the responsibility of the senior management to check and ensure that appropriate contingency plans and procedures, based on realistic and probable disruptive scenarios, are in place with the third party and the same are appropriately tested.

## **II. The intermediary should establish a comprehensive outsourcing risk management programme to address the outsourced activities and the relationship with the third party.**

An intermediary should make an assessment of outsourcing risk which depends on several factors, including the scope and materiality of the outsourced activity, how well the intermediary manages, monitors and controls outsourcing risk, and how well the third party manages and controls the potential risks of the operation, etc. The factors that could help in considering materiality in a risk management programme include:

- a. The impact of failure of a third party to adequately perform the activity on the financial, reputational and operational performance of the intermediary and on the customers and their counterparts;
- b. Ability of the intermediary to cope up with the pressures, in case of non performance or failure by a third party;
- c. Consequences of outsourcing on the ability and capacity of the intermediary to conform to regulatory requirements and changes in requirements, inter relationship of the outsourced activity with other activities within the intermediary;
- d. Affiliation or other relationship between the intermediary and the third party;

- e. Regulatory status of the third party, including its fitness and probity status;
- f. Degree of difficulty and time required to select an alternate third party or to bring the business activity in-house, if necessary;
- g. Complexity of the outsourcing arrangement. For example, the ability to control the risks where more than one third party collaborates to deliver an end-to-end outsourcing solution.
- h. Situations involving conflict of interest between the intermediary and the third party. The measures put in place by the intermediary to address such potential conflicts, etc.

Data protection, security and other risks may be adversely affected by the geographical location of the third party. To this end, specific risk management expertise in assessing country risk related, for example, to political or legal conditions, could be required when entering into and managing outsourcing arrangements that are taken outside of the home country. More generally, a comprehensive outsourcing risk management programme and a need to conduct enhanced due diligence that focuses on special compliance risks, including the ability to effectively monitor the activities of the foreign outsourced entities, the ability to maintain the confidentiality of the intermediary and its customers, the ability to execute contingency plans and exit strategies where the service is being performed on a cross-border basis should be scrupulously studied by the market intermediary before outsourcing activities to foreign third parties.

While there should not be any prohibition on a group entity / associate of the intermediary to act as the third party, systems should be put in place to have an arm's length distance between the intermediary and the third party in terms of infrastructure, manpower, decision-making, record keeping, etc. for avoidance of potential conflict of interests. Further, necessary disclosures in this regard should be made as part of the contractual agreement. It should be kept in mind that the risk management practices expected to be adopted by an intermediary while outsourcing to a related party or an associate would be identical to those followed while outsourcing to an unrelated party.

The outsourcing contracts should clearly contain provisions which address the monitoring and control of the third party. The records relating to all activities outsourced should be preserved centrally so that the same is readily accessible for review by the Board of the intermediary and / or its senior management, as and when needed. Such records should be

regularly updated and may also form part of the corporate governance review by the management of the intermediary.

Regular reviews by internal or external auditors of the outsourcing policies, risk management system and requirements of the regulator should be mandated. Additionally, intermediary should at least on an annual basis, review the financial and operational capabilities of the third party in order to assess its ability to continue to meet its outsourcing obligations. Such due diligence reviews and checks, which can be based on all available information about the third party should highlight any deterioration or breach in the performance standards, confidentiality and security lapses and lacunae in business continuity preparedness. In the event of termination of the outsourcing contract by any intermediary, it is expected that the concerned intermediary makes such information about the termination of the third party public knowledge so that any clients / customers of the intermediary do not continue to take the services of the third party. As part of monitoring and control of outsourcing activities, the intermediary should:

- a. Clearly define parameters that will assess the performance levels or specify what performance levels are required / expected from the third party;
- b. Establish measures to identify and report instances of non-compliance or unsatisfactory performance of the third party and also the ability to assess the quality of services provided on a regular basis; and
- c. Lay down procedures so as to ensure that the third party is compliant with the applicable laws/regulatory requirements at all points in time and in case of any non-compliance that is noticed by the intermediary, the same should be reported to the regulator. The procedures for ensuring compliance can include internal / external auditor's reports on a regular basis, specifying service performance levels or any kind of adverse reports against the third party which has been brought to the notice of the intermediary.

**III. The intermediary should ensure that outsourcing arrangements neither diminish its ability to fulfill its obligations to customers and regulators, nor impede effective supervision by the regulators.**

Outsourcing arrangements should not affect the rights of a customer against the intermediary in any manner. The intermediary would be liable to the investors for the loss

incurred by them due to the failure of the third party and also be responsible for redressal of the grievances received from investors arising out of activities rendered by the third party. The facilities / premises of third party will be deemed to be those of the registered intermediary and the Regulator should have the right to access the same at any point of time. Outsourcing arrangements should not impair the regulator's ability to exercise its regulatory responsibilities such as proper supervision of the intermediary. The intermediary should ensure that it has a robust investor grievance redressal mechanism, which is not compromised in any way due to part of the activities being outsourced to a third-party. The investor grievance redressal mechanism should redress any grievance pertaining to any of the outsourced activities carried out by the third party.

#### **IV. The intermediary should conduct appropriate due diligence in selecting the third party and in monitoring of its performance.**

It is important that the intermediary exercises due care, skill, and diligence in the selection of the third party to ensure that the third party has the ability and capacity to undertake the provision of the service effectively. An intermediary must develop criteria that enable it to assess, prior to selection, the third-party's capacity and ability to perform the outsourced functions effectively, reliably and of a high standard, together with any potential risk factors associated with using a particular third party. An intermediary may of course pursue any applicable legal rights it may have against a third-party.

The due diligence undertaken by an intermediary should include assessment of:

- a. third party's resources and capabilities, including financial soundness, to perform the outsourcing work within the timelines fixed;
- b. compatibility of the practices and systems of the third party with the intermediary's requirements and objectives;
- c. market feedback of the prospective third party's business reputation and track record of their services rendered in the past;
- d. level of concentration of the outsourced arrangements with a single third party; and
- e. the environment of the foreign country where the third party is located.

Any special needs, such as servicing geographically dispersed activities, must be determined and met by using third parties with similar reach or capability. Activities should not be



outsourced to a third party that does not meet the criteria. If a third party fails, or is otherwise unable to perform the outsourced activity, it may be costly or problematic for the intermediary to find alternative solutions. Transition costs and potential business disruptions should also be considered before an intermediary decides to outsource activities. Additional concerns exist when an intermediary decides to outsource activities to foreign third party. For example, in an emergency, the intermediary may find it more difficult to implement appropriate responses in a timely fashion. Accordingly, senior management of the intermediary may assess the economic, legal and political conditions that might adversely impact the third party's ability to perform effectively the functions for the intermediary.

**V. Outsourcing relationships should be governed by written contracts / agreements that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of the parties to the contract, client confidentiality issues, termination procedures, etc.**

Outsourcing arrangements should be governed by a clearly defined and legally binding written contract between the intermediary and each of the third parties, the nature and detail of which should be appropriate to the materiality of the outsourced activity in relation to the ongoing business of the intermediary. A written contract is an important management tool and appropriate contractual provisions can reduce the risk of non-performance or disagreements regarding the scope, nature and quality of the service to be provided. Every such agreement should address the risks and risk mitigation strategies. The contract should be sufficiently flexible so as to allow the intermediary to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations. A written contract also facilitates the monitoring of the outsourced entities. The care should be taken to ensure that the outsourcing contract:

- a. clearly defines what activities are going to be outsourced, including appropriate service and performance levels;
- b. provides for mutual rights, obligations and responsibilities of the intermediary and the third party, including indemnity by the parties;
- c. provides for the continuous monitoring and assessment by the intermediary of the third party so that any necessary corrective measures can be taken up immediately, i.e., the contract should enable the intermediary to retain an appropriate level of

- control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations;
- d. includes, where necessary, conditions of sub-contracting by the third-party, i.e. the contract should enable intermediary to maintain a similar control over the risks when a third party outsources to further third parties as in the original direct outsourcing;
  - e. has unambiguous confidentiality clauses to ensure protection of proprietary and customer data during the tenure of the contract and also after the expiry of the contract;
  - f. specifies the responsibilities of the third party with respect to the IT security and contingency plans, insurance cover, business continuity and disaster recovery plans, force majeure clause, etc.;
  - g. provides for preservation of the documents and data by third party;
  - h. provides for the mechanisms to resolve disputes arising from implementation of the outsourcing contract;
  - i. provides for the circumstances and manner of termination and renewal of contract;
  - j. addresses additional issues arising from country risks and potential obstacles in exercising oversight and management of the arrangements when intermediary outsources its activities to foreign third party. For example, the contract should include choice-of-law provisions and agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction;
  - k. neither prevents nor impedes the intermediary from meeting its respective regulatory obligations, nor the regulator from exercising its regulatory powers; and
  - l. provides for the intermediary and /or the regulator to have the ability to access all books, records and information relevant to the outsourced activity with the third party.

**VI. The intermediary and its third parties should establish and maintain contingency plans, including a plan for disaster recovery and periodic testing of backup facilities.**

While intermediaries should have a global institutional policy addressing contingency planning, more specific contingency plans should be separately developed for each outsourcing arrangement, as is done in individual business lines. An intermediary should take

appropriate steps to assess and address the potential consequence of a business disruption or other problems at the third party level. Notably, it should consider contingency plans at the third party; co-ordination of contingency plans at both the intermediary and the third party; and contingency plans of the intermediary in the event of non-performance by the third party. Recurring performance problems coupled with the absence of a comprehensive contingency plan by the third party and the intermediary may result in unintended financial losses, missed business opportunities, reputational and legal concerns.

To ensure business continuity, robust information technology security is a necessity. A breakdown in the IT capacity may impair the ability of the intermediary to fulfill its obligations to other market participants/clients/regulators and could undermine the privacy interests of its customers, harm the intermediary's reputation, and may ultimately impact on its overall operational risk profile. Intermediaries should, therefore, seek to ensure that third party maintains appropriate IT security and robust disaster recovery capabilities. The intermediary can specify the security requirements in the third party's systems, including software specifications, so as to protect the privacy of data entrusted to the third party. The rights of the parties concerned to alter the security arrangements should also be clearly specified. Special care may be needed where the security arrangements are sub-contracted, so that the risks arising out of subcontracting are minimized.

The entities should have an appropriate level of control over the third party's with a right to intervene in certain cases. Periodic tests of the critical security procedures and systems and review of the back-up facilities should be undertaken by the third party to confirm the adequacy of the third party's systems. Contingency plans, in the event of deteriorating performance, must account for the costs of alternative options. In the face of unsatisfactory responsiveness from the third party, an intermediary's option include changing the third party and shifting the activities to alternate third party, moving the activity internally to the institution, i.e., exploring the possibility of bringing the outsourced activity back in-house, or sometimes even exiting the business. These could be very costly options, which are often taken only as a last measure. Nevertheless, these eventualities and associated costs should be studied during the negotiation process and specified in the contract which is entered into with the third party. Additional issues arising out of undertaking services of a foreign third party should also be suitably addressed. The intermediary should have its own contingency

procedures and systems to address situations of failure of third party. This can be ensured by devising a system of taking regular feedbacks from the third party to ascertain adequacy of latter's procedures and systems.

**VII. The intermediary should take appropriate steps to require that third party's protect confidential information of both the intermediary and its customers from intentional or inadvertent disclosure to unauthorised persons.**

An intermediary that engages in outsourcing is expected to take appropriate steps to protect its proprietary and confidential customer information and ensure that it is not misused or misappropriated. Such steps should include provisions in the contract with the third party prohibiting the third party and its agents from using or disclosing the intermediary's proprietary information or that of its customers, except as necessary to provide the contracted services and to meet regulatory and statutory provisions. The terms and conditions for protection of information should also govern the sub-contracting arrangements, wherever applicable. An intermediary should notify customers that customer data may be transmitted to a third party, taking into account any regulatory or statutory provisions that may be applicable. The details of outsourced activities and the terms of outsourcing to a third-party should be suitably disclosed by the intermediary in a public domain for the information of its customers and the regulator.

The intermediary should prevail upon the third party to ensure that the employees of the third party have limited access to the data handled and only on a "need to know" basis. The third party should have adequate checks and balances to ensure limited data access by its staff. In cases where the third party is providing similar services to multiple entities, the intermediary should ensure that adequate care is taken by the third party to build safeguards for data security and confidentiality. The security practices and the control process should be reviewed by the intermediary through an internal / external auditor on a regular basis. In case of any breach, the same should be immediately notified to the regulator. The intermediary is liable for damages in case of any eventualities.

**VIII. Regulators should take into account outsourcing activities as an integral part of their ongoing assessment of the regulated entity. Regulators should assure themselves by appropriate means that any outsourcing arrangements do not hamper the ability of the intermediary to meet its regulatory requirements.**

Regulators should consider outsourcing activities as part of their overall risk assessment of an intermediary. In order to be able to assess and monitor the outsourcing policy and the risk management programme of a intermediary, regulators should be able, upon request, to obtain promptly any relevant books and records pertaining to the outsourced activity, irrespective of whether they are in the possession of the intermediary or the third-party and to obtain additional information concerning outsourced activities.

A regulator's access to such books and records may be direct or indirect, though the intermediary should always maintain direct access to such books and records. This may include a requirement that the books and records be maintained in the regulator's jurisdiction, or that the third party agrees to send originals or copies of the books and records to the regulator's jurisdiction upon request. In this regard, the outsourcing agreement or contract that is entered into between the intermediary and the third party should inter alia specify provisions for preservation of records and data by third party in accordance with the legal /regulatory obligations vested upon the intermediary under the law.

Regulators should consider implementation of appropriate regulations and measures designed to support access to books, records and information of the third party about the performance of outsourced activities. This may include the requirement that intermediaries include contractual provisions that provide the intermediary with access to, and a right of inspection of the third party's books and records dealing with outsourced activities and similar access to the books and records of any subcontractor, as well as contractual provisions by which the third party is required to make books, records and other information about outsourced activities by the third party available to the regulator upon request.

**IX. Regulators should be aware of the potential risks posed where the outsourced activities of multiple intermediaries are concentrated with a limited number of third parties.**

When a limited number of third parties (sometimes just one) provide outsourcing services to multiple intermediaries, operational risks concentrate which may pose a systemic threat. Similarly, if multiple third parties depend upon the same provider for business continuity

services (e.g., a common disaster recovery site), a disruption that affects a large number of those entities may result in a lack of capacity for the business continuity services. Accepting that some form of concentration risk is inevitable as firms use outsourcing to search for improved efficiency and economies of scale, when assessing and monitoring the outsourcing policy and risk management programme of an intermediary, regulators should pay special attention to the way in which the intermediary takes account of the potential risk posed by such concentration.

In instances, where the third party acts as an outsourcing agent for multiple intermediaries, it is the duty of the third party and the intermediary to ensure that strong safeguards are put in place so that there is no commingling of information /documents, records and assets. Whilst concentration risks may exist, there are mitigating tools available to address the potential systemic risk attached to such concentration of activities at third party's level. These include, primarily, adequate contingency planning within the intermediary as well as other supervisory mitigating tools such as ongoing monitoring and awareness programmes, adapting supervisory programmes, risk assessments and other actions, etc.

## **5. OTHER GENERAL ISSUES**

**Reporting To FIU** - The intermediaries would be responsible for reporting of any suspicious transactions / reports to FIU or any other competent authority in respect of activities carried out by the third parties.

**List Of Defaulters** - A caution list of third parties who have defaulted while servicing any of the intermediaries should be informed to the regulator and the same may also be shared among the intermediaries.

**Need for Self Assessment of existing / Proposed Outsourcing Arrangements** – In view of the changing business activities and complexities of various financial products, intermediaries may conduct a self assessment of their existing outsourcing agreements within a time bound plan and bring them in line with the requirements of the above guidelines expeditiously.

## **6. ACTIVITIES THAT ARE PRESENTLY OUTSOURCED**

There is no study to ascertain the level of outsourcing in Indian securities market. Based on informal feedback, it is understood that a few intermediaries are currently outsourcing some

of their activities related to data entry, record keeping, despatch, front-desk customer services, KYC verification, etc. The intermediary-wise activities which are presently outsourced by a few intermediaries are as under:-

#### **I. DEPOSITORY PARTICIPANT (DPs)**

- Capturing of client data
- Record keeping
- Attending to client queries through phone banking services
- Printing and packing of welcome kits
- Despatch of statement of accounts and DIS booklets etc.

#### **II. REGISTRAR & SHARE TRANSFER AGENTS (R & T AGENTS)**

- Data capturing work for public issues / right issues.
- Despatch of dividends, refunds orders etc.
- Packing and franking activities

#### **III. BANKERS TO AN ISSUE (BTIs)**

- Courier pick up of applications from the syndicate members in the book built IPOs
- Processing of applications collected - data capturing, encoding of cheques, scheduling etc.

#### **IV. STOCK BROKERS**

- Data entry and opening of trading accounts
- Scanning and storage of account opening forms
- Printing and despatch of welcome kits and despatch of quarterly transaction statements
- Customer services
- Despatch of contract notes
- Stock brokers acting as distributors for Mutual Funds schemes - distribution, maintenance of nomination details by distributors for the various schemes of Asset Management Companies, etc.

#### **V. PORTFOLIO MANAGERS**

- Client servicing
- Fund accounting

- Custodian services
- Research activity
- Financial accounting
- Account opening
- Data entry
- Operational Activity

## **7. ACTIVITIES THAT SHOULD NOT BE OUTSOURCED**

Since the intermediaries are registered based on their strength, outsourcing of key activities by them to unregistered third parties defeats the purpose of regulation. It is therefore felt that the key activities which are crucial to the intermediation service may be delivered by the intermediary itself. The informal feedback indicates that the compliance with securities laws, investor grievance redressal and KYC must not be outsourced under any circumstance. Besides, the following activities ought not be outsourced to third parties:

### **I. DEPOSITORY PARTICIPANT (DPs)**

- Core management functions such as defining organisation structure, formulating policies and procedures, monitoring internal control mechanism & supervision of outsourced activities.
- Authorization for issue of DIS booklets
- “Checker” activity (as in “maker-checker” concept) esp. checker of instructions including debit instructions, pledge instructions, BO modifications etc
- Analysis of PMLA alerts and other surveillance activities and decision based on such analysis.

### **II. REGISTRAR & SHARE TRANSFER AGENTS (R & T AGENTS)**

- Electronic record keeping of the investor database
- Basic IT infrastructure, as declared at the time of registration
- PMLA obligations
- Finance and Accounts
- Computational / validation activities relating to corporate actions, like dividends / bonus, transactional activities, statutory activities like TDS, STT etc.



- Data validation with respect to the bid data captured by the SM/SSM and ASBA bankers with the demographic details obtained from the Depositories, in a public issue, *mutatis mutandis* in a rights issue.
- Finalisation of allottees and non-allottees
- Comparison of specimen signature available with the STA with the request received from investors.
- Processing of demat/remat/physical transfer of securities
- Other requests of investors like transmission of shares, issue of duplicate shares etc.
- Reconciliation of issued capital.

### **III. BANKERS TO AN ISSUE (BTIs)**

- Processing of applications collected which includes data capturing, preparation of bank schedules, etc.
- Clearing of instruments
- Controls over processes
- Tallying of Instruments and Reconciliation

### **IV. STOCK BROKERS**

- Creation of user id/login id, password generation for internet clients
- Order management
- Operation of trading terminals
- Operations & Monitoring of Bank A/cs & DP A/cs
- Pay in / pay out of funds and securities
- Generation & dispatch of contract notes, quarterly statement of accounts, daily margin statement and monitoring of the said activities.
- Control of servers and online trading platform
- Maintenance & monitoring of client database & client financial information
- Surveillance function
- Allotment / surrender of trading terminals, opening & closing of branches
- Implementation of PMLA policies
- Risk Management system (which includes margins, trading limits, scrip / terminal enablement etc.
- IT Technology Infrastructure

- Printing of contract notes

## **V. PORTFOLIO MANAGERS**

- Fund management/ portfolio management.

## **VI. MERCHANT BANKERS**

- Due diligence of all nature except :-  
To the extent of outsourcing legal and financial due diligence and obtaining expert opinion on specialist areas  
(However the responsibilities in terms of disclosure and due diligence shall lie with the Merchant Banker only even in the above matters)
- Pricing of the issue.
- Supervision of other intermediaries (viz. Registrars to the issue, Bankers to the issue, etc.)

## **VII. MUTUAL FUNDS**

- All investment related activities including trading.

## **8. GUIDELINES**

Keeping in view the principles enunciated in Section 4 above and current practice of outsourcing in the market, it is proposed to streamline outsourcing by intermediaries through appropriate guidelines. The guidelines may provide for:

- The activities which can be outsourced,
- The activities which cannot be outsourced,
- To whom the activities can be outsourced,
- The terms of outsourcing,
- Responsibilities and obligations of the intermediary and the third party in respect of the outsourced activity towards clients, regulator and market,

\*\*\*\*\*