EXAMINATION PROCEDURES FOR SROCC MEMBERS TO DETERMINE IMPLEMENTATION OF IOSCO PRINCIPLES ON OUTSOURCING BY MARKET INTERMEDIARIES OUTSOURCING THEIR ACTIVITIES

A REPORT OF THE

SRO CONSULTATIVE COMMITTEE OF THE

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

NOVEMBER 2007

IOSCO has laid down seven key principles to be followed by market intermediaries in respect of outsourcing of financial services to ensure that the outsourcing of responsibilities do not in any way infringe upon the customer service and compliance requirements. The IOSCO SRO Consultative Committee (SROCC) has determined to implement the IOSCO principles in the manner set forth in this document. While it is recognised that outsourcing may not have been yet specifically allowed or disallowed or rules relating to outsourcing may still have to be laid down in some jurisdictions, it is nevertheless appropriate for SROCC members to examine if the IOSCO principles are followed by the market intermediaries, to the extent applicable and allowed or not specifically prohibited, while auditing them.

This document attempts to suggest examination procedures which could be adapted by the SROCC members for undertaking such examinations. It is important for the examiner to keep the materiality principle in mind while conducting such examinations so that the intensity and scope of the SRO that is examining the regulated entity is proportionate to the degree in which a given outsourced service relates to the firm's regulated activities.

Outsourcing firms may be encouraged to have in place a process to consider which principles are appropriate for a particular service that it has outsourced. Accordingly, the examiner should also consider which principles are appropriate for a particular service that has been outsourced and conduct the examination accordingly. The SRO should also give discretion to the examiner to focus on whether the firm's overall procedures are appropriate in overseeing whatever services it has decided to outsource. Moreover, the scope of examination in respect of every principle should be tailored to the delivery of financial services, and that the details are generally most appropriate where there is a potential for a significant problem to arise in the delivery of services by the regulated entity in the event the service provider fails to adequately perform its contracted functions.

(In this document the outsourcing firm is referred as OSF; the third party service provider as SP and the Outsourcing Agreement as OA).

IOSCO Principle-Topic 1: Due diligence in selection and monitoring of service provider and service provider's performance

Principle: An outsourcing firm should conduct suitable due diligence processes in selecting an appropriate third party service provider and in monitoring its ongoing performance.

Draft Examination Procedures for SROCC Members:

An outsourcing firm (OSF) remains responsible to its customers and the regulators for providing good service and complying with the regulations even after outsourcing. Therefore, it is important for the OSF to select a service provider (SP) who will be able to meet the high standards of service and compliance expected of the OSF. For this purpose, the OSF needs to put in place a robust due diligence system to select the best SP for carrying out its

responsibilities and also to ensure that the SP continues to perform according to agreed standards while the outsourcing agreement (OA) is in force and in case of termination of OA, till the function is smoothly transferred.

The SRO's examiner may broadly see whether the OSF exercised due care, skill, and diligence in the selection of the SP to ensure that the SP has the ability and capacity to undertake the provision of the service effectively. The OSF is expected to conduct appropriate due diligence procedures not only for selecting the SP but also for subsequent monitoring of the SP and its performance. The depth of due diligence to be performed for selection and subsequent monitoring may vary and needs to be tailored according to the following factors:

- the extent of outsourcing,
- regulatory, legal and financial risk that could arise from the activities that are being outsourced,
- the reputation and experience of the proposed SP in undertaking such activities, and
- the OSF's familiarity with the SP.

While the methodology and level of examination will entirely depend on the circumstances of each case, a broad examination of the following documents or aspects might help in reaching a conclusion about the level of due diligence exercised by the OSF while selecting a SP:

- request for proposal (RFP) issued by the OSF,
- proposal submitted by SP and their competitors,
- due diligence done by OSF on the SP's background and ability to perform the function, and
- Reasoning articulated for selecting one SP over the others who had responded to the RFP, etc.

To identify the level of due diligence being exercised by the OSF in continuously monitoring the SP, the examiner may look at the procedures followed by the OSF for continuous monitoring of the SP and its performance covering the following aspects:

- periodicity of monitoring,
- deviation identification and handling,
- monitoring of other aspects which may have material bearing on performance of the SP like changes in the constitution, objectives, shareholders, clientele, financial capability, key managerial personnel and other employees who are involved in the service, service delivery capability, timeliness and its effectiveness,
- monitoring of technology, communication and process infrastructure, and
- monitoring of legal and regulatory compliance including any complaints, litigation, or regulatory actions, etc.

IOSCO Principle-Topic 2: The contract with a service provider

Principle: *There should be a legally binding written contract between the outsourcing firm and each third party service provider, the nature and detail of*

which should be appropriate to the materiality of the outsourced activity to the ongoing business of the outsourcing firm.

Draft Examination Procedures for SROCC Members:
After the completion of the detailed process of evaluations, due diligence and negotiations, the OSF will select its SP and award a contract. It is important for both parties to have a legally enforceable contract document that details the agreed expectations on all the various facets of the arrangement. The outsourcing agreement (OA) is primarily a legally enforceable commercial contract and therefore needs to have all the essential ingredients of a valid and enforceable agreement to begin with. The OA needs to contain all the essential clauses to ensure quality service and to protect the OSF's interest, the interest of its customers as well as the rights of the regulators.

The examiner of the SRO, may, inter alia, broadly peruse the Outsourcing Agreement (OA) for coverage of the following aspects:

- compliance with stamping and registration requirements, if any,
- consonance of the OA with the regulatory requirements
- the description of services,
- rights and obligations of parties
- obligation of the SP to provide records, information and assistance to OSF, regulators etc.
- maintenance of client confidentiality,
- handling of transition on expiry of tenure or termination,
- dispute handling mechanism,

IOSCO Principle-Topic 3: Information Technology Security and Business continuity at the Outsourcing Firm
*Principle**:** The outsourcing firm should take appropriate measures to determine that: (a) Procedures are in place to protect the outsourcing firm's proprietary and customer-related information and software; and (b) Its service providers establish and maintain emergency procedures and a plan for disaster recovery, with periodic testing of backup facilities.*

Draft Examination Procedures for SROCC Members:
This principle deals with the measures for IT security and business continuity adopted by the SP. It is important for the OSF to ensure that the SP has not only adopted best practices for IT security and business continuity in respect of the outsourced services provided by the SP to the OSF, but also follows the same in letter and spirit. Any failure on the part of the SP to ensure IT security and business continuity may cause irreparable damage to the OSF's reputation besides leading to huge financial damage and regulatory action. While the examiner may mostly be able to carry out the examination on his or her own, he or she may need, if he or she is not well versed in IT security and business continuity related issues, in case of outsourcing of high risk activities, expert advice from the in-house IT team of the SRO if there is one, or may have to consult outside IT experts.

The SRO's examiner, taking into account inherent risks and criticality of outsourced services, may broadly assess the IT security focusing on the availability of the following aspects:

- IT security program and procedures,
- user ID, password and other access control policies,
- data and software backup policies and procedures, and
- policies and procedures relating to handling personnel, data, premises, software and hardware for different OSFs in order to avoid mix up, misuse, wrong usage or corruption of data, etc.

In case of outsourcing particular high-risk activities, the SRO's examiner may assess more specific items including:

- disclosure policies to customers in case of leakage of information and remedial action,
- availability of contingency plans in case of misplacement or theft of data, and
- policy on usage of encryption technology.

Also, the SRO's examiner, may, among other things, assess the recovery program from disaster focusing on the availability of following aspects:

- Business Continuity Plan
- documentation and emergency procedures to support and implement the BCP,
- mock trial, live runs, testing, usage monitoring and control,
- procedure for handling of customers during the disaster backup usage period.

IOSCO Principle-Topic 4: Client Confidentiality Issues

Principle: The outsourcing firm should take appropriate steps to require that service providers protect confidential information regarding the outsourcing firm's proprietary and other information, as well as the outsourcing firm's clients from intentional or inadvertent disclosure to unauthorized individuals.

Draft Examination Procedures for SROCC Members:

The onus has been put on the OSF to ensure that its SPs protect the confidentiality of the proprietary and other information of the OSF and its clients. For this purpose, the OSF shall take appropriate steps and ensure that proper safeguards are followed by the SP for protecting confidential information. Moreover, such procedures may also require specifying measures to be taken in case of any leak of information inadvertent or otherwise.

The SRO's examiner may broadly assess the availability of the following policies and procedures:

- SP's policy relating to its agents using or disclosing the OSF's proprietary information or that of the OSF's customers, except as necessary to provide the contracted services,
- process of selection, recruitment and training of the personnel assigned to have access to the OSF's data,

- non-disclosure agreement or secrecy agreement concerning the information of OSF and its clients between the agents and staff,
- transparency agreement with OSF's customers on customer data being transmitted to an SP,
- the confidentiality requirements meeting the standards prescribed by the privacy laws and regulations of the country of OSF as well as those of the SP,
- policies and procedures for data retention and disposal of the data storage facilities like papers, CDs, hard disk and other magnetic media,
- mechanism to alert the OSF, its customers and the regulators in case of any unauthorised use or leak of confidential information, and
- review of policy and procedures relating to privacy issues periodically, etc.

IOSCO Principle-Topic 5: Concentration of Outsourcing Functions
Principle: Regulators should be cognizant of the risks posed where one service provider provides outsourcing services to multiple regulated entities.

Draft Examination Procedures for SROCC Members:
Outsourcing often leads to the sharing of facilities operated by an SP in respect of various OSFs. The facilities so shared may include the physical infrastructure, computer and telecommunication hardware, computer software, databases, manpower, etc. Such concentration of outsourced activities in the hands of a single or a few SPs, though undesirable, may not always be avoidable. It may be a matter of concern for the Regulators and SROs if all major players in the industry utilise just one or two service providers, as a failure of such a service provider could have systemic risk implications if there is a high industry concentration. However, OSFs would not necessarily be in a position to determine which outsourcing firms their competitors in the industry are using and then avoid them. Moreover, in the event an OSF chooses to concentrate its outsourcing with just one SP, such concentration of key functions may be appropriate, depending on numerous factors, such as the extent to which reputable alternatives may or may not exist, and the redundancy that a key service provider has built into its systems and processes. Therefore, for the OSF, it is an act of fine balancing between avoiding concentration and its own commercial interest and also availability of reputable alternatives.

The SRO's examiner may broadly assess if the OSF has understood the concern and made appropriate efforts to balance these factors.

IOSCO Principle-Topic 6: Termination Procedures
Principle: Outsourcing with third party service providers should include contractual provisions relating to termination of the contract and appropriate exit strategies.

Draft Examination Procedures for SROCC Members:
Any commercial contract will normally include a termination clause to end the arrangement after a certain period or on the happening of a certain event. It is important for outsourcing contracts to include a similar clause. At the same

time, it is equally important for the OA also to provide for a smooth post termination transition since any abrupt end to the relationship will bring about irreparable damage to the customers of the OSF. The SRO's examiner needs to focus on the general issue of whether or not the contract provides for a smooth transition in the event of termination.

The SRO's examiner may broadly examine the termination procedures focusing on the following aspects in the OA:

- provision to co-operate for alternate arrangement,
- rights and responsibilities of the respective parties and transition arrangements,
- compulsion on the part of the SP to co-operate and render all assistance for smooth transition of data and operations to OSF or other SPs as may be decided by the OSF,
- protection of customer data privacy in the process.

IOSCO Principle-Topic 7: Regulator's and Intermediary's Access to Books and Records, Including Rights of Inspection

Principle: The regulator, the outsourcing firm, and its auditors should have access to the books and records of service providers relating to the outsourced activities and the regulator should be able to obtain promptly, upon request, information concerning activities that are relevant to regulatory oversight.

Draft Examination Procedures for SROCC Members:

The OSF as well as the regulator should be given reasonable access to SP's book and records related to the outsourcing activities. As a matter of course, outsourcing should not vitiate the OSF's or the regulator's access to the OSF's books and records which is otherwise available. This is necessary to ensure that the OSF has full control over the activities of the SP pertaining to the job done on behalf of the OSF even after outsourcing. Likewise, the regulator's access is needed for ensuring that its inspection and enforcement rights are protected in the interest of investors.

The SRO's examiner, while auditing the access rights of the OSF, its auditors and the regulator including the SRO to the records and books of the OSF and the SP, may broadly look at the availability of the following aspects in the OA:

- provisions in the OA providing for 1) reasonable access of the regulator, the SRO, OSF, its auditors and representatives at all reasonable times to the books and records related to the outsourced activities and 2) right to examine all records and obtain statements of any member, director, partner, proprietor, employee, sub-contractor and agents of the SP,
- periodicity of audit spot, periodical or otherwise,
- right to make extracts or copies, and
- auditors' reasonable access to the premises, staff and other infrastructure , etc.