Appendix A

Excerpts from report entitled "Principles on Outsourcing of Financial Services for Market Intermediaries" issued by the IOSCO Technical Committee Standing Committee on the Regulation of Market Intermediaries (SC3) in February 2005

...

III. Outsourcing Principles

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.

...

Means for Implementation

It is expected that outsourcing firms will implement appropriate means, such as the following, for ensuring that they select suitable service providers and that service providers are appropriately monitored, having regard to the services they provide:

- Documenting processes and procedures that enable the outsourcing firm to assess, prior to selection, the third party service provider's ability and capacity to perform the outsourced activities effectively, reliably, and to a high standard, including the service provider's technical, financial and human resources capacity, together with any potential risk factors associated with using a particular service provider.
- Documenting processes and procedures that enable the outsourcing firm to monitor the third party service provider's performance and compliance with its contractual obligations, including processes and procedures that:
  - Clearly define metrics that will measure the service level, and specify what service levels are required; and
  - Establish measures to identify and report instances of non-compliance or unsatisfactory performance to the outsourcing firm as well as the ability to assess the quality of services performed by the service provider on a regular basis (*see also* topic 2).
- Implementing processes and procedures designed to help ensure that the service provider is in compliance with applicable laws and regulatory requirements in its jurisdiction, and that where there is a failure to perform duties required by statute or regulations, the outsourcing firm, to the extent required by law or regulation, reports the failure to its regulator and/or self-regulatory organization and takes corrective actions.[6] For example, procedures may include:

[6] Such a requirement is consistent with regulations in many IOSCO jurisdictions requiring that a firm notify its regulator with respect to any breaches of law that may have occur.

- The use of service delivery reports and the use of internal and external auditors to monitor, assess, and report to the outsourcing firm on performance;
- The use of written service level agreements or the inclusion of specific service level provisions in contracts for service to achieve clarity of performance targets and measurements for third party service providers.

➢ With respect to outsourcing on a cross-border basis, in determining whether the use of a foreign service provider is appropriate, the outsourcing firm may, with respect to a function that is material to the firm, need to conduct enhanced due diligence that focuses on special compliance risks, including the ability to effectively monitor the foreign service provider, the ability to maintain the confidentiality of firm and customer information; and the ability to execute contingency plans and exit strategies where the service is being performed on a cross-border basis.

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.

...

Means for Implementation

An outsourcing firm is expected to have a written, legally binding contract between itself and the third party service provider, appropriate to the materiality of the outsourced activity to the ongoing business of the firm. The contract may include, as applicable, provisions dealing with:

➢ Limitations or conditions, if any, on the service provider's ability to subcontract, and, to the extent subcontracting is permitted, obligations, if any, in connection therewith;

➢ Firm and client confidentiality (see also topic 4);

➢ Defining the responsibilities of the outsourcing firm and the responsibilities of the service provider and subcontractors, if any, and how such responsibilities will be monitored;

➢ Responsibilities relating to IT security (see also topic 3);

➢ Payment arrangements;

➢ Liability of the service provider to the outsourcing firm for unsatisfactory performance or other breach of the agreement;

➢ Guarantees and indemnities;

➢ Obligation of the service provider to provide, upon request, records, information and/or assistance concerning outsourced activities to the outsourcing firm, its auditors and/or its regulators (see topic 7);

- Mechanisms to resolve disputes that might arise under the outsourcing arrangement;
- Business continuity provisions (*see* topic 3);
- With respect to outsourcing on a cross-border basis, choice of law provisions;
- Termination of the contract, transfer of information and exit strategies (*see also* topic 6).

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.

...

Means for Implementation

Outsourcing firms are expected to take appropriate steps to require, in appropriate cases based on the materiality of the function that is being outsourced, that service providers have in place a comprehensive IT security program. These steps may include:

- Specification of the security requirements of automated systems to be used by the service provider, including the technical and organizational measures that will be taken to protect firm and customer-related data. Appropriate care should be exercised to ensure that IT security protects the privacy of the outsourcing firm's customers as mandated by law:
- Requirements that the service provider maintain appropriate measures to ensure security of both the outsourcing firm's software as well as any software developed by the service provider for the use of the outsourcing firm;
- Specification of the rights of each party to change or require changes to security procedures and requirements and of the circumstances under which such changes might occur;
- Provisions that address the service provider's emergency procedures and disaster recovery and contingency plans as well as any particular issues that may need to be addressed where the outsourcing firm is utilizing a foreign service provider. Where relevant, this may include the service provider's responsibility for backing up and otherwise protecting program and data files, as well as regulatory reporting;
- Where appropriate, terms and conditions relevant to the use of subcontractors with respect to IT security, and appropriate steps to minimize the risks arising out of such subcontracting;

- Where appropriate, requirement of testing by the service provider of critical systems and back-up facilities on a periodic basis in order to review the ability of the service providers to perform adequately even under unusual physical and/or market conditions at the outsourcing firm, the service provider, or both, and to determine whether sufficient capacity exists under all relevant conditions;
- Requirement of disclosure by the service provider of breaches in security resulting in unauthorized intrusions (whether deliberate or accidental, and whether confirmed or not) that may affect the outsourcing firm or its customers, including a report of corrective action taken; and
- Provisions in the outsourcing firm's own contingency plans that address circumstances in which one or more of its service providers fail to adequately perform their contractual obligations. Where relevant, this may include reporting by the outsourcing firm to its regulator. The outsourcing firm may need to require contractually information from the service provider to fulfill this obligation.

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.

...

Means for Implementation

Regulated firms that engage in outsourcing are expected to take appropriate steps to confirm that confidential firm and customer information is not misused or misappropriated. Such steps may include insertion of provisions in the contract with the service provider that:

- Prohibit the service provider and its agents from using or disclosing the outsourcing firm's proprietary information or that of the firm's customers, except as necessary to provide the contracted services; and
- Where appropriate, including terms and conditions relevant to govern the use of subcontractors with respect to firm and client confidentiality.

Outsourcing firms should also consider whether it is appropriate to notify customers that customer data may be transmitted to a service provider, taking into account any regulatory or statutory provisions that may be applicable.

Regulators should seek to become aware of whether outsourcing firms within their jurisdiction are taking appropriate steps to monitor their relationships with service providers with respect to the protection of confidential firm and customer information.

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.

...

Means for Implementation

Regulators should consider the following means for addressing concentration risk:

- Taking steps to become aware of cases where a significant proportion of their regulated entities rely upon a single service provider to provide critical functions. This could include, where appropriate, a monitoring program and/or a risk assessment methodology, and the collection of routine information on outsourcing arrangements from outsourcing firms and/or service providers. In this regard, regulators should be cognizant of the potential that subcontracting by service providers of a particular function may itself result in concentration risk;
- Tailoring their examination programs or related activities in light of concentrations of outsourcing activity.

Where a regulator has identified a possible concentration risk issue, outsourcing firms should consider taking steps to ensure, to the degree practicable, that the service provider has adequate capacity to meet the needs of all outsourcing firms, both during normal operations as well as unusual circumstances (*e.g.*, unusual market activity, physical disaster).

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.

...

Means for Implementation:

Outsourcing firms are expected to take appropriate steps to manage termination of outsourcing arrangements. These steps may include provisions in contracts with service providers such as the following:

- Termination rights, *e.g.,* in case of insolvency, liquidation or receivership, change in ownership, failure to comply with regulatory requirements, or poor performance;
- Minimum periods before an announced termination can take effect to allow an orderly transition to another provider or to the firm itself, and to provide for the return of customer-related data, and any other resources;
- The clear delineation of ownership of intellectual property following the contract's termination, and specifications relating to the transfer of information back to the outsourcing firm.

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.

...

Means for Implementation:

Outsourcing firms are expected to take steps to ensure that they and their regulators have access to books and records of service providers concerning outsourced activities, and that their regulators have the right to obtain, upon request, information concerning the outsourced activities. These steps may include the following:

- Contractual provisions by which the outsourcing firm (including its auditor) has access to, and a right of inspection of, the service provider's books and records dealing with outsourced activities, and similar access to the books and records of any subcontractor. Where appropriate, these may include physical inspections at the premises of the service provider, delivery of books and records or copies of books and records to the outsourcing firm or its auditor, or inspections that utilize electronic technology (*i.e.*, "virtual inspections");
- Contractual provisions by which the service provider is required to make books, records, and other information about regulated activities by the service provider available to the regulator upon request and, in addition, to comply with any requirements in the outsourcing firm's jurisdiction to provide periodic reports to the regulator.

Regulators should consider implementation of appropriate measures designed to support access to books, records and information of the service provider about the performance of regulated activities. These measures may include:

- Where appropriate, taking action against outsourcing firms for the failure to provide books and records required in that jurisdiction, without regard to whether the regulated entity has transferred possession of required books and records to one or more of its service providers;
- Imposing specific requirements concerning access to books and records that are held by a service provider and which are necessary for the authority to perform its oversight and supervisory functions with respect to regulated entities in its jurisdiction. These may possibly include requiring that records be maintained in the regulator's jurisdiction, allowing for a right of inspection, or requiring that the service provider agree to send originals or copies of the books and records to the regulator's jurisdiction upon request