IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

IIROC NOTICE

Rules Notice
Guidance Note
Dealer Member Rules

Please distribute internally to:

Internal Audit
Legal and Compliance
Operations
Regulatory Accounting
Senior Management

Contacts:

Louis Piergeti
Vice President, Financial and Operations Compliance
(416) 865-3026
lpiergeti@iiroc.ca

Richard J. Corner
Vice President, Member Regulation Policy
(416) 943-6908
rcorner@iiroc.ca

14-0012
January 13, 2014

Outsourcing arrangements

Guidance Note objectives

The objectives of this Guidance Note are to:

- summarize the existing requirements and guidance relating to entering into and maintaining outsourcing arrangements,
- identify the Dealer Member business activities that may not be outsourced and those that may be outsourced,
- set out IIROC's expectations as to the appropriate due diligence procedures that must be undertaken by IIROC Dealer Members before outsourcing any business activity, and
- set out IIROC's plans to propose rules relating to outsourcing.

Background information and context are also provided on the development of regulatory principles governing outsourcing arrangements by regulated entities and relevant financial sector guidance published on this subject matter.

The concept of outsourcing is not new in the securities industry. The IIROC Dealer Member Rules set out the requirements for many of the common outsourcing arrangements that are entered into by Dealer Members, including:

- Back office sharing arrangements with an affiliated Canadian financial institution,

- Introducing broker/carrying broker arrangements,
- Security custody arrangements, and
- External portfolio management arrangements.

However, as firms face increasing competitive pressures to contain and reduce costs, there is a corresponding trend to outsource more business functions, activities and processes to third-party service providers through arrangements that IIROC Dealer Member Rules do not adequately address.

In recent years, there has been an evolution of outsourcing arrangements put in place between Dealer Members and regulated/unregulated entities that may or not be affiliated, and that may be foreign or domestic. For example, employees of Canadian banks, that own a Dealer Member, conduct certain back-office operational functions on behalf of the Dealer Member and the parent bank charges the Dealer Member for those services rendered, pursuant to a service agreement. Similar arrangements exist for US FINRA-registered parent companies of Dealer Member subsidiaries. These functions include accounting and back-office support that are outside the scope of Rule 35 – *Introducing broker/carrying broker arrangements*.

There is a growing interest by self-clearing Dealer Members to outsource the daily management of books and records, including the reconciliation of bank account balances, positions held in custody, dividend/interest income received, and stock reorganizations, to both domestic and foreign unregulated, third-party service providers. Without adequate safeguards, this industry trend may give rise to incremental investor protection, market reputation, credit and systemic risks.

Dealer Members are reminded of their obligation to provide IIROC with advance notification of material changes in their business model, including operations pursuant to IIROC Rules Notice 10-0060 – *Reporting of changes to business models* dated March 2010. **The effective date of this guidance note is April 14, 2014.**

1. What is outsourcing?

The term "outsourcing" is not currently defined within the IIROC rules. A report prepared in 2005 by the International Organization of Securities Commissions (the "IOSCO Report") sets out the following definition for outsourcing:

> *"...outsourcing is defined as an event in which a regulated outsourcing firm contracts with a service provider for the performance of any aspect of the outsourcing firm's regulated or unregulated functions that could otherwise be undertaken by the firm itself. It is intended to include only those services that were or can be delivered by internal staff and management... the service provider may be a related party within a corporate group, or an unrelated outside entity. The service provider may itself be either regulated (whether or not by the same regulator with authority over the outsourcing firm), or may be an unregulated entity .... outsourcing would not cover purchasing contracts, although as with outsourcing, firms should ensure that what they are buying is appropriate for the intended purpose. Purchasing is defined as the acquisition from a vendor of services,*

goods or facilities without the transfer of the purchasing firm's non-public proprietary or customer information"[1].

The IOSCO Report makes an important distinction between "core" and "non-core" functions of a firm and describes a core function as one that is:

> *"...critical to the ongoing viability of an entity as well as meeting its regulatory obligations to customers"*.

The IOSCO Report also sets out guiding principles that financial intermediaries should follow when planning and arranging for the outsourcing of both core and non-core activities, functions and/or processes (for simplicity referred to collectively as "activities" throughout the remainder of this guidance note). These guiding principles are included as Appendix A.

As IIROC has no current definition for the term "outsourcing" and wishes to focus its regulatory efforts on the outsourcing of critical or "core" activities, the definitions of the terms "outsourcing", "core" and "non-core", where used throughout the remainder of this notice, are the same as the definitions contained in the IOSCO Report.

2. What are the Canadian regulatory requirements relevant to outsourcing?

IIROC REQUIREMENTS

As previously mentioned, the IIROC Dealer Member Rules set out the requirements for many of the common outsourcing arrangements that are entered into by Dealer Members. These arrangements are as follows:

- **Back office sharing arrangements with an affiliated Canadian financial institution** *[Dealer Member Rule 35.1(d)]*
  This rule allows an affiliated Canadian financial institution to handle the clearance and settlement of trades, as well as the preparation of related books and records and the performance of related operational functions, on behalf of the Dealer Member, provided that proper segregation of the Dealer Member and Dealer Member client account assets is maintained.

- **Introducing broker/carrying broker arrangements**
  [Dealer Member Rules 35.1 through 35.6]

  These rules permit a dealer, the introducing broker, to outsource certain back office functions to another dealer, the carrying broker. The rules contemplate four different types of introducing broker / carrying broker arrangements that can be entered between two IIROC Dealer Members.[2] For each permitted arrangement, the rules list the various activities that are to be carried out by the carrying broker for the introducing broker as

---

[1] Source: Principles on Outsourcing of Financial Services for Market Intermediaries, Section I – Technical Committee of the International Organizations of Securities Commission (IOSCO), February 2005.

[2] The rules also include a fifth introducing broker / carrying broker arrangement that can be entered into between an IIROC Dealer Member and a foreign affiliated dealer. This arrangement may only be entered into if certain rule conditions are met and approval of the applicable District Council is obtained.

well as activities that will continue to be carried out by the introducing broker.

Consistent with other outsourcing arrangements, the introducing broker retains the responsibility for ensuring that all activities are performed properly and in compliance with relevant IIROC requirements, including those activities carried out by the carrying broker on its behalf. In addition, since the outsource services provider is another IIROC Dealer Member, the carrying broker also assumes the responsibility for ensuring that all activities it has agreed to perform on behalf of the introducing broker are performed properly and in compliance with relevant IIROC requirements.[3]

- **Security custody arrangements** *[Dealer Member Rules 17.3; 17.3A; 17.3B; 2000.1 through 2000.9; Form 1, General Notes and Definitions, Definition of "acceptable securities locations"; and Form 1, Statement , Line 20]*

  These rules require a Dealer Member to establish, maintain and comply with adequate policies and procedures for the segregation and safekeeping of client account assets. In meeting these obligations, the requirements allow the Dealer Member to outsource the security custody activity to an external custodian provided:

  - the external custodian is a depository, clearing agency, financial institution, dealer or mutual fund that maintains its financial capital at or above a specific level[4]; and
  - the written custodial agreement entered into with the external custodian prohibits the use of securities held in custody without Dealer Member consent and specifies that securities are to be delivered back to the Dealer Member "promptly on demand"[4].

  Where a Dealer Member uses an external custodian, it retains the responsibility for ensuring that all custody activities are performed properly and in compliance with relevant IIROC requirements.

and

- **External portfolio management arrangements**
  [Dealer Member Rule 1300.7]

  This rule allows a Dealer Member to outsource its discretionary authority with respect to some or all of its managed accounts to an external portfolio manager, provided:

  - the external portfolio manager is properly registered to provide discretionary portfolio management services; and
  - the external portfolio manager is subject to conflict of interest legislation or regulations that are either equivalent to or more stringent than the IIROC requirements.

---

[3] For each of the four types of introducing broker / carrying broker arrangements, Dealer Member Rule 35 requires that the carrying broker treat the introduced clients in the same manner as the carrying broker's own clients, in order to ensure that the carrying broker is performing the outsourced functions in compliance with all applicable IIROC rules.

[4] The financial capital requirements to be met by the custodian and the minimum required custodial agreement terms are set out in the "acceptable securities location" definition set out in the General Notes and Definitions to IIROC Dealer Member Form 1.

Under such arrangements, the IIROC Dealer Member retains the responsibility for ensuring that all managed account activities are performed properly and in compliance with relevant IIROC requirements.

Other than the rules that are in place that govern these specific arrangements, there are no other IIROC rules that directly reference outsourcing arrangements.

CSA REQUIREMENTS

When National Instrument 31-103 was implemented in September 2009, Part 11 of its Companion Policy introduced general principles for the establishment and maintenance of internal control systems at registrants with specific reference to the need to follow prudent business practices and to conduct a due diligence analysis when considering whether or not to outsource.

The guidance set out in the Companion Policy states that registered firms are responsible and accountable for all functions that they outsource to a service provider. Further, the functions outsourced should be set out in a written, legally binding contract between the outsourcing party and the service provider that sets out the expectations of each of the parties to the outsourcing arrangement. The guidance also requires that registered firms conduct a due diligence analysis of prospective third-party service providers, including affiliates of the firm. This due diligence analysis should include an assessment of the service provider's reputation, financial stability, relevant internal controls and ability to deliver the services being outsourced.

The guidance also states that a registrant firm should:

- ensure that third-party service providers have adequate safeguards for keeping information confidential and, where appropriate, for recovering from a business disruption;
- conduct ongoing reviews of the quality of outsourced services;
- develop and test a business continuity plan to minimize disruption to the firm's business and its clients if the third-party service provider does not deliver the services satisfactorily; and,
- consider other legal requirements, such as privacy laws, that may apply when entering into outsourcing arrangements.

Finally, the guidance specifies that the registrant firm and its regulator and auditors should have the same access to the work product of a third-party service provider as they would if the firm itself performed the activities. Firms should ensure this access is provided and should include a provision requiring it in any contract entered into with a service provider.

3. Who is responsible for complying with IIROC rules and securities legislation requirements that relate to any activities that are outsourced?

A Dealer Member who outsources activities to an outsource service provider retains the responsibility to ensure that those activities are conducted in accordance with the requirements set out in the applicable IIROC rules and securities legislation, whether or not the outsource service provider is also a Dealer Member. To carry out this responsibility, Dealer Members must, at a minimum, supervise the activities performed on their behalf by the outsource service provider in manner that is similar to the type of supervision that would be required if the activities were performed by the Dealer Member itself.

4. Which investment dealer activities may not be outsourced?

Since the IIROC rules do not specifically refer to outsourcing, the only IIROC rules that effectively prohibit the outsourcing of certain activities are those rules which require certain functions or activities to be performed by specific Approved Persons. Specifically, pursuant to Dealer Member Rule 1.1:

> ***"Approved Person"*** *means, in respect of a Dealer Member, an individual who is a partner, Director, Officer, employee or agent of a Dealer Member who is approved by the Corporation or another Canadian Self Regulatory Organization to perform any function required under any Rule;*

Given that apart from Dealer Member partners, directors and certain officers an Approved Person of a Dealer Member must be an individual that is an employee or agent of a Dealer Member, all IIROC rules that require that a certain Approved Person perform a certain activity or function are effectively prohibiting the outsourcing of that activity or function. The result of this restriction (i.e. who can be an Approved Person) is that the IIROC rules effectively prohibit the outsourcing of most client-facing activities of the Dealer Member (all of which would be considered to be "core" activities) including:

- a Registered Representative's assessment of the information collected from the client to ensure that the information is current, complete and accurate and that they comply with their "know your client" obligation *[Dealer Member Rules 39.3; 1300.1(a); 2500, Introduction; 2500, Part II and 2700, Part II]*;
- a Registered Representative's performance of suitability assessments *[Dealer Member Rules 39.3; 1300.1(p) through (s) and 2500, Introduction]*;
- a Designated complaints officer's oversight of the handling of client complaints *[Dealer Member Rule 2500B, Section 3]*; and
- Various compliance and supervision requirements, relating to client facing activities, that must be performed by Approved Persons of the Dealer Member *[including Dealer Member Rules 29.7, 30.3, 30.5, 38, 39.4, 1300.2, 1300.4, 1300.15, 1800.2, 1900.2, 2600, 3400 and 3500.6]*.

An exception to the general prohibition against the outsourcing of client-facing activities is the outsourcing of the performance of investment decision making in managed accounts. As previously

mentioned, IIROC Dealer Member Rule 1300.7 specifically allows for the outsourcing of managed account investment decision making to an external portfolio manager hired by the Dealer Member.

5. For those investment dealer activities that may be outsourced, which activities are most important to IIROC?

Not all investment dealer activities that are eligible to be outsourced under IIROC rules are of equal importance and impact. Some activities are immaterial to the overall operations of the dealer and/or are more routine/administrative in nature than others. These activities therefore pose less risk to the Dealer Member and/or its clients. In addition to focusing on material outsourcing arrangements, IIROC supports the approach taken in the IOSCO Report (i.e. distinguishing between the outsourcing of "core" and "non-core" activities) and intends to focus its regulatory resources on the review of material outsourcing arrangements involving core activities. To facilitate this regulatory focus, IIROC has performed a high-level analysis of Dealer Member activities and categorized these activities as either:

- "core" activities; or
- "non-core" activities.

Core activities

Core activities of a Dealer Member that are eligible to be outsourced include the following:

- the performance of certain activities that are not required in the IIROC rules to be performed by an employee or agent of a Dealer Member relating to the firm's:
  - account opening process
  - suitability assessment process
  - client complaint handling process
- the performance of investment decisions in managed accounts (as previously mentioned in section 2 above);
- the performance of certain client account-related operations activities, such as the clearing and settlement of client trades
- the administration of margin loans and other client account loans
- the preparation of client account statements
- the preparation of regulatory financial reports
- the preparation of non-financial regulatory reports
- the performance of registration-related filing and database maintenance activities
- the performance of treasury activities
- the performance of corporate finance activities
- the preparation of research reports and marketing newsletters
- the performance of marketing activities

- the use of outside professional services relating to the business activities of the Dealer Member, such as accounting and internal audit services
- the management and maintenance of Dealer Member information systems

Where any of these activities are to be outsourced, including where activities are outsourced to another Dealer Member, consistent with the guidance set out in the Companion Policy to National Instrument 31-103:

- IIROC expects the Dealer Member to formally assess the initial and ongoing appropriateness of the outsource service provider (see section 6 of this notice for further details); and
- the Dealer Member that has outsourced specific activities retains responsibility for ensuring that the activities are performed properly and in compliance with relevant IIROC requirements.

Non-core activities

Non-core activities of the Dealer Member that are eligible to be outsourced under the applicable IIROC Dealer Member Rules, and that would not give rise to regulatory concern if they were outsourced, include the following:

- office service management activities;
- the procurement of external consultant services; and
- human resources management activities.

Similar to the outsourcing of core activities, where any of these activities are to be outsourced IIROC expects the Dealer Member to formally assess the initial and ongoing appropriateness of the outsource service provider (see section 6 of this notice for further details).

6. What should be assessed when determining whether or not to outsource a particular activity?

As discussed in section 2 above, certain IIROC Dealer Member Rules set out detailed requirements for specific outsourcing arrangements but do not set out general requirements to be met when considering whether or not to enter into an outsourcing arrangement. On the other hand, the CSA expectations in Part 11 of the Companion Policy to National Instrument 31-103, set out general principles for the establishment and maintenance of internal control systems at registrants with specific reference to the need to follow prudent business practices and to conduct a due diligence analysis when considering whether or not to outsource.

In order to address these CSA expectations, we recommend that Dealer Members adopt formal due diligence policies and procedures relating to outsourcing arrangements. To facilitate Dealer Members' efficient assessment of individual proposed outsourcing arrangements, it would be acceptable for Dealer Members to adopt policies and procedures that acknowledge that the extent of due diligence work performed may be proportionate to the materiality and risk of the functions/activities that are proposed to be outsourced. Dealer

Members are encouraged to consider and include, where appropriate, the following as part of their due diligence policies and procedures:

- A Dealer Member should have a comprehensive outsourcing policy that guides the performance of due diligence assessment(s) that will underlie decisions regarding whether, and how, certain activities can be appropriately outsourced
- As part of the comprehensive outsourcing policy, an initial assessment should be made as to whether the Dealer Member has the internal expertise that is necessary to perform the due diligence assessment(s) and, if not, the Dealer Member should identify and obtain third party expertise to perform or assist in the performance of the due diligence assessment(s)
- A Dealer Member should never enter into an outsourcing arrangement that:
  - diminishes its ability to fulfill its obligations to clients and regulators,
  - impedes effective supervision by regulators, or
  - unduly or inappropriately concentrates its outsourced activities in one or a few outsource service providers, or
  - allows the outsource services provider to, in turn, outsource some or all of the outsourced activities to a third party without the Dealer Member's knowledge and/or without retaining the responsibility for the performance of the outsourced activities
- A Dealer Member should inform IIROC of any new outsourcing arrangements involving core Dealer Member activities that are being entered into by a Dealer Member, in accordance with IIROC Rules Notice 10-0060, *Reporting of Changes to Business Models*.
- A Dealer Member that has outsourced one or more activities should:
  - enter into written outsourcing contracts that clearly describe all material aspects of the outsourcing arrangements, including the rights, responsibilities and expectations of all parties
  - maintain a centralized list, along with copies of related agreements, of the outsource service providers to which core Dealer Member activities have been outsourced
  - establish and carry-out a comprehensive outsourcing risk management program that monitors the risks associated with:
    - the outsourced activities; and
    - the outsourcing relationship entered into with the service provider.

    The risks associated with the outsourcing relationship that need to be managed by the Dealer Member include:
    - *client harm risk*, the risk the outsource service provider will fail to provide adequate protection and timely access to client account assets and related account records;
    - *reputation risk*, the risk that poor service by the outsource provider will affect the reputation of the Dealer Member;
    - *compliance risk*, the risk that the outsource provider will not comply with regulatory or other requirements that apply to the Dealer Member;
    - *exit strategy risk*, the risk that due to over-reliance on the outsource provider and a lack of relevant skills within the Dealer Member, the Dealer Member won't be able to re-

assume performance of the outsourced activities or contract with another outsource provider on a timely basis;

- *access risk*, the risk that the Dealer Member won't have timely access to data, records or assets; and
- *individual firm concentration risk*, the risk that the Dealer Member, has a significant exposure to the outsource provider, because of the number and/or the materiality of the activities that have been outsourced to that provider

See Appendix B for a more complete list of the key risks associated with outsourcing and the major concerns associated with these risks.

- perform outsourcing agreement reviews to ensure that the outsourced activities covered by each outsourcing agreement are being performed in accordance with the agreement service level requirements without exposing the Dealer Member to undue risk
- determine the timing and frequency of the outsourcing agreement reviews by establishing and maintaining a risk-based outsourcing agreement review schedule
- where practical and/or available (such as special purpose reports regularly prepared by external auditors for outsource service providers[5]), obtain and provide to IIROC a report on the adequacy of internal controls for each outsource arrangement relating to a core Dealer Member activity; and
- include as part of its business continuity planning, plans that address the scenario where one or more major outsource service providers undergo a business disruption.

7. Are outsourcing arrangements involving affiliates subject to this guidance?

The guidance set out in this notice covers both arm's length and non-arm's length outsourcing arrangements. In addition, in the case of non-arm's length outsourcing arrangements, such as arrangements involving affiliates, Dealer members should be mindful of the *access risk* that flows from the affiliated nature of the parties. Specifically, Dealer Members should consider ensuring that the outsourcing arrangement with an affiliate includes procedures designed to limit the access and control that affiliate employees, as well as Dealer Member employees who are dually employed by the affiliate, may have over Dealer Member and Dealer Member client account data, records and assets.

Without such procedures in place, employees acting in the best interests of their affiliate employer may be able to make material changes to Dealer Member data and records or move Dealer Member and/or Dealer Member client account assets without considering or acting in the best interests of the Dealer Member and its clients.

---

[5] Reports such as the CICA 5970 (now changed to CSAE 3416) report or the SAS 70 (now changed to SSAE 16) report provide assurance that the service provider's system of internal controls is adequate and may reduce or eliminate the need for the Dealer Member to do its own assessment of the service provider's system of internal controls during its due diligence analysis of a proposed outsourcing arrangement.

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

Appendix B

Key Risks of Outsourcing

While the outsourcing of certain activities can be beneficial to a financial services organization, outsourcing can give rise to risks which need to be managed effectively.

Risk	Major Concerns
Client harm risk	▪ Inadequate third-party outsource service provider controls to ensure adequate protection and timely client access to their account assets and related account records
Strategic risk	▪ The third-party outsource service provider may conduct activities on its own behalf which are inconsistent with the overall strategic goals of the regulated entity. ▪ Failure to implement appropriate oversight of the outsource service provider. ▪ Failure to maintain adequate in-house expertise to oversee the outsource service provider.
Reputation risk	▪ Poor service from third-party outsource service provider. ▪ Customer interaction is not consistent with overall standards of the regulated entity. ▪ Third-party outsource service provider practices are not in line with stated practices (ethical or otherwise) of regulated entity.
Compliance risk	▪ Privacy laws are not complied with. ▪ Consumer and prudential laws not adequately complied with. ▪ Outsource service provider has inadequate compliance systems and controls.
Operational risk	▪ Technology failure. ▪ Inadequate financial capacity to fulfill obligations and/or provide remedies. ▪ Inadequate internal controls leading to undetected errors or fraud. ▪ Difficult/costly for firm to undertake inspections of the outsource service provider's operations.
Exit strategy risk	▪ The risk that appropriate exit strategies are not in place. This could arise from over-reliance on one firm, the loss of relevant skills in the institution itself preventing it from bringing the activity back in-house, and contracts which make a timely exit prohibitively expensive. ▪ Limited ability to return services to firm due to lack of staff or loss of institutional knowledge.
Counterparty risk	▪ Inappropriate underwriting or credit assessments. ▪ Quality of receivables may diminish.
Country risk	▪ Political, social and legal climate may create added risk. ▪ Business continuity planning is more complex.
Contractual risk	▪ Ability to enforce contract. ▪ For off shore outsourcing arrangements, choice of law is important.
Access risk	▪ Outsourcing arrangement hinders ability of regulated entity to provide timely data and other information to regulators. ▪ Additional layer of difficulty in regulator understanding activities of the outsource provider.
Individual firm concentration risk	▪ The firm has significant exposure to the third-party outsource service provider, because of the number and/or the materiality of the activities that have been outsourced to that provider
Industry concentration and systemic risk	▪ The industry, as a whole, has significant exposure to the outsource provider. This concentration risk has a number of facets, including: o Lack of control, by individual firms, over provider; and o Systemic risk to industry as a whole.