May 2012

mcmillan insurance bulletin

getting regulations out of the clouds - cloud computing, other novel technologies and the financial regulatory framework

The emergence of new technologies allowing for more efficient data capture and management has provided federally regulated financial institutions ("FRFIs"), including insurers, with new opportunities to use third parties to take over certain FRFI functions. However, the use in Canada of these technologies is limited by the regulatory framework set out by the Office of the Superintendent of Financial Institutions ("OSFI"). This short paper discusses some of these new technologies, potential risks involved in their application to FRFIs, and regulatory concerns that FRFIs should consider when evaluating these technologies for adoption.

Information technology ("IT") outsourcing typically is provided by an external organization that has agreed by contract to take over some or all of the IT functions of a business such as an FRFI. These agreements may involve complete transfers of certain staff, business assets and resources to the service provider, on the view that specialists can provide IT services more reliably and affordably than if performed in-house.

Just as businesses have outsourced claims management, billing, call centres and printing/mailing functions, new technologies, and a matured internet infrastructure, have now made it similarly

possible to outsource IT-dependent business operations. However, as with the traditional forms of outsourcing, a potential for diminished control over service performance and data integrity pose additional risks for FRFIs. These are the risks that are targeted by regulators and will be discussed below.

While these new technologies provide businesses with new features and benefits, they also create new risks. For example, businesses considering certain forms of "Cloud Computing" must live with decreased physical control over data. In a typical consumer-grade cloud computing arrangement, a service provider will offer multiple customers simultaneous access to the same set of pooled computer resources (e.g., for web applications, processing power or storage). This arrangement, often offered on a pay-per use basis, provides greater cost efficiency to both the provider and customer when compared against conventional separate computer ownership and operation. Cloud Computing may be structured to reduce these risks, such as where a dedicated "private cloud" is provided to a single customer for its entire organization, but such service arrangements typically come with a higher price tag.

As the number of business activities that can be performed "in the cloud" grows, businesses face a decision of whether to replace (or supplement) sole-sourced IT outsourcing agreements with a number of separate arrangements with a multiplicity of different infrastructure, service and software vendors. In some cases, such arrangements may even include third-party cloud "brokers" who outsource client needs to a group of cloud providers that share responsibility for contract performance.

While cloud computing service providers offer value by reaching economies of scale not typically available in traditional outsourcing arrangements, they complicate the risk profile for insurers who are required by law – and as a matter of good business practice – to safeguard vigilantly the information of their clients, including both personal information (such as name, age, address, contact information and credit history) and claims history (including

potential health concerns and the result of medical tests). Providing access to this information to more counterparties and more subcontractors of the counterparties opens an FRFI to more risk.

For example, cloud services that allow multiple customers access to the same computing resources (i.e., "public clouds") introduce new data commingling security risks. Such an arrangement also makes it difficult for FRFIs to demand certain performance standards or oversight rights. Additionally, many software service providers that employ cloud infrastructure use proprietary data formats. This practice adds switching costs and places the buyer at risk of data loss should the cloud provider cease its services (e.g., due to bankruptcy) or should the FRFI seek to terminate its relationship with the cloud provider (e.g., due to security breaches).

With the emergence of these new technologies, financial regulators continue to adopt their regulatory framework to ensure both consumer protection and company solvency. By letter dated February 29, 2012 (the "Outsourcing Letter"), the Office of the Superintendent of Financial Institutions Canada ("OSFI") clarified the rules governing technology-based outsourcing services applicable to FRFIs. Such contracts must comply with the requirements of OSFI Guideline B-10, *Outsourcing of Business Activities, Functions and Processes* (the "Outsourcing Guideline").

The Outsourcing Guideline, last revised in 2009, applies to agreements made between FRFIs and third-party service providers that perform a business activity, function or process that is or could be undertaken by the entity itself. The Outsourcing Letter makes clear OSFI's interpretation that IT outsourcing contracts, including cloud computing initiatives, are to be considered "outsourcing arrangements" for purposes of the Outsourcing Guideline.

The Outsourcing Letter attempts to address some of these IT-specific concerns by drawing particular emphasis to certain

compliance requirements in the Outsourcing Guideline: (i) confidentiality, security and separation of property, (ii) contingency planning, (iii) location of records, (iv) access and audit rights, (v) subcontracting, and (vi) monitoring the material outsourcing arrangements.

The full obligations set out in the Outsourcing Guideline apply to "material" outsourcing arrangements, which have a potentially important influence - whether quantitative or qualitative - on a significant line of the FRFI's business. Such material arrangements require the FRFI to have a risk management program in place that anticipates possible IT outsourcing activities. For any particular IT outsourcing engagement, FRFIs must have conducted an internal due diligence process to determine the nature and scope of the activity to be outsourced, how it is to be managed, and its relationship to other FRFI activities. Due diligence must also be performed on the counterparty IT outsourcing service provider to ensure all relevant risks associated with the service will be addressed satisfactorily. Particular attention must be paid to outsourcing arrangements that occur in jurisdictions outside of Canada. Even once an FRFI is satisfied that its counterparty is acceptable, the FRFI must conduct due diligence on new contracts as well as significant amendments to existing contracts.

FRFIs must ensure that the following provisions are included in any contract for outsourcing services:

- a description of the nature and scope of the services, including a description of the physical location where the service provider will provide the service;
- performance measures that will allow parties to ensure contractual compliance and will permit the FRFI to assess if it is getting full value from the arrangement;
- reporting requirements to permit the FRFI to meet its obligation to monitor and control outsourcing risks and prepare reports;
- dispute resolution provisions;

- default and termination provisions;
- ownership of assets (intellectual and physical);
- contingency planning, including a requirement that the outsourcing counterparty have a business recovery system and test it regularly;
- audit rights, including providing certain of these rights to OFSI;
- limits on subcontracting;
- confidentiality, security and separation of property;
- fulsome disclosure of pricing; and
- disclosure of insurance coverage and an obligation by the counterparty to inform the FRFI if such coverage is changed.

The Outsourcing Letter demonstrates that OSFI does not recognize a difference between newer IT-based arrangements such as cloud computing initiatives and other forms of business outsourcing. Such an interpretation likely means that FRFIs will be precluded from engaging in some of the cheaper cloud-based IT outsourcing offerings, where FRFIs are not able to negotiate the terms of service and where the arrangement is "material" to the FRFI. However, the benefits of other cloud arrangements that offer the purchaser greater control, such as custom services delivered by dedicated computer hardware (the so-called "private clouds"), should not be ignored as a result of the Outsourcing Letter.

FRFIs that are contemplating entering into IT outsourcing agreements are advised to:

- review their internal policies, the Outsourcing Guideline and the Outsourcing Letter to ensure that the potential agreement is permitted;
- assess the risks attendant with the proposed agreement, including risks to the FRFI if the counterparty fails either financially or in its performance;

- consider how the proposed agreement fits into the FRFI's broader outsourcing strategy and whether the activity is something that should be done in-house; and
- consult with legal counsel as early as possible to ensure the negotiation of an agreement that satisfies business, legal and regulatory needs.

by Hartley Lefton and Robert Hester

For more information on this topic, please contact:

Toronto	Hartley Lefton	416.307.4164	hartley.lefton@mcmillan.ca
Toronto	Robert Hester	416.865.7803	robert.hester@mcmillan.ca

a cautionary note