Insurance & Reinsurance - Canada

Getting insurance regulation out of the clouds

Contributed by **McMillan LLP**

June 06 2012

Authors

Hartley Lefton

Robert Hester

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

Outsourcing and the cloud

Typically, IT outsourcing is provided by an external organisation that has agreed by contract to take over some or all of the IT functions of a business such as an insurer. These agreements may involve complete transfers of certain staff, business assets and resources to the service provider on the basis that specialists can provide IT services more reliably and affordably than if they were performed in-house.

While these new technologies provide businesses with new features and benefits, they also create new risks – these are the risks that are targeted by regulators. 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 (eg, 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 the customer when compared to conventional separate computer ownership and operation. Cloud computing may be structured to reduce these risks (eg, where a dedicated private cloud is provided to a single customer for its entire organisation), 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 must decide whether to replace (or supplement) sole-sourced IT outsourcing agreements with a number of separate arrangements involving different infrastructure, service and software vendors. In some cases, such arrangements may even include third-party cloud brokers, which outsource clients' 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, they complicate the risk profile for insurers which are required by law – and as a matter of good business practice – to safeguard vigilantly the information of their clients, including both personal information (eg, 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 their subcontractors exposes an insurer to greater risk.

For example, cloud services that allow multiple customers access to the same computing resources (ie, public clouds) introduce new data commingling security risks. Such an arrangement also makes it difficult for insurers to demand certain performance standards or oversight rights. In addition, 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 (eg, due to bankruptcy) or should the insurer seek to terminate its relationship with the cloud provider (eg, due to security breaches).

Regulatory framework

With the emergence of these new technologies, financial regulators continue to adapt their regulatory framework to ensure both consumer protection and company solvency. By a letter dated February 29 2012 the OSFI clarified the rules governing technology-based outsourcing services applicable to federally regulated financial institutions. Such contracts must comply with the requirements of OSFI Guideline B-10, Outsourcing of Business Activities, Functions and Processes.

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

The letter attempts to address some of these IT-specific concerns by drawing particular emphasis to certain compliance requirements in the guideline:

- confidentiality, security and separation of property;
- contingency planning;
- location of records;
- access and audit rights;
- subcontracting; and
- monitoring of material outsourcing arrangements.

The full obligations set out in the guideline apply to 'material' outsourcing arrangements, which have a potentially important influence - whether quantitative or qualitative - on a significant line of the federally regulated financial institution's business. Such material arrangements require the institution to have a risk management programme in place that anticipates possible IT outsourcing activities. For any particular IT outsourcing engagement, the institution 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 its other activities. Due diligence must also be performed on the counterparty IT outsourcing service provider to ensure that all relevant risks associated with the service will be addressed satisfactorily. Particular attention must be paid to outsourcing arrangements that occur in jurisdictions outside Canada. Even once an institution is satisfied that its counterparty is acceptable, it must conduct due diligence on new contracts as well as significant amendments to existing contracts.

Institutions 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 institution to assess whether it is getting full value from the arrangement;
- reporting requirements to permit the institution 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 OSFI;
- limits on subcontracting;
- confidentiality, security and separation of property;
- full disclosure of pricing; and
- disclosure of insurance coverage and an obligation by the counterparty to inform the institution if such coverage is changed.

The letter demonstrates that OSFI does not differentiate between newer IT-based arrangements, such as cloud computing initiatives, and other forms of business outsourcing. Such an interpretation is likely to mean that insurers and other federally regulated financial institutions will be precluded from engaging in some of the cheaper cloud-based IT outsourcing offerings, where they are unable to negotiate the terms of service and where the arrangement is material to the institution. However, the benefits of other cloud arrangements that offer the purchaser greater control (eg, custom services delivered by dedicated computer hardware, or private clouds) should not be ignored as a result of the letter.

Comment

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

- review their internal policies, the guideline and the letter to ensure that the potential agreement is permitted;
- assess the risks attendant with the proposed agreement, including risks to the insurer if the counterparty fails either financially or in its performance;
- consider how the proposed agreement fits into the insurer's broader outsourcing strategy and whether the activity 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.

For further information on this topic please contact Hartley Lefton or Robert Hester at McMillan LLP by telephone (+1 416 865 7000), fax (+1 416 865 7048) or email (hartley.lefton@mcmillan.ca or robert.hester@mcmillan.ca).