Assessing legal risks in the move to cloud

By Wendy Tembedza

4 Jul 2019

With the fourth industrial revolution in full swing, businesses are looking for faster and more efficient ways to service customers. Customers are also increasingly tech-savvy and demand more from their service providers, including quicker access and more tailored offerings.

© Rungaroon taweeapiradeemunkohg – 123RF.com

To meet this demand, many businesses are moving to cloud computing to reap the many benefits that cloud can provide. These include scalability, agility and an ability to analyse data and interpret it in such a way that can help meet client demands.

However, before moving any business functions to the cloud, a business must carefully assess legal issues that will have an impact on the ability not only to move to cloud, but also to have full beneficial use of cloud services. These issues relate primarily to:

i. the regulatory environment in which the business operates, which may impact a move to cloud;

ii. internal data hygiene related to compliance with data protection legislation; and
iii. ensuring that the business implements best practice in its corporate governance regarding risk mitigation.

Regulatory environment

The cloud customer will remain responsible for its own compliance requirements. As such, businesses should ensure that they understand the regulatory environment in which they operate. Certain sectors are required to comply with specific rules regarding how data is managed. For example, in the banking sector, the Prudential Authority issued a Directive D3/2018 and related Guidance Note G5/2018 (Banking Cloud Rules) on cloud computing and the offshoring of data for banks on 5 September 2018. In general, the Prudential Authority acknowledges that cloud computing is becoming an integral aspect of banking business operations and is permissive of the use of cloud computing. The Banking Cloud Rules also set out comprehensive guidelines which banks must follow in order to comply with the regulator's requirements on the use of cloud computing and/or offshoring of data. Any bank considering a move to cloud must first ensure that it is compliant, and is continually taking the necessary steps to comply, with the Banking Cloud Rules.

We anticipate that with the ever-increasing adoption of cloud, this approach may filter through to other sectors that will soon be subject to similar regulatory requirements. It is incumbent on the business to ensure that any move to cloud is compliant with the applicable regulatory regime.

To assist businesses to understand their regulatory requirements, some cloud service providers (CSP) have produced useful materials assisting businesses' to understand the cloud offering in the context of the regulatory requirements applicable to specific sectors. Businesses should make use of such resources to understand their regulatory obligations before appointing a CSP.

Internal business data hygiene

In order to facilitate a move to cloud, a business should first conduct a data hygiene exercise to determine:

- what data it has (for example sensitive personal information);
- where the data is stored; and
- who has access to the data.

This exercise will help a business better understand the level of risk attached to moving any category of data to the cloud. Importantly, this exercise will help determine whether it is even appropriate to move all or part of the data to the cloud.

An internal data hygiene exercise will also assist a business to comply with data protection legislation. In this regard, the Protection of Personal Information Act, 2013 (POPIA) will, once fully operational require entities that handle personal information to implement various controls regarding such personal information. This exercise will therefore assist a business to determine whether it complies with POPIA requirements and what further steps may need to be taken to comply.

This exercise will also help a business determine whether it has in place data processing documentation to meet its data management requirements. This may include a cloud computing policy, privacy policy, acceptable use policy and personal device usage policy. Importantly, any move to the cloud should be aligned with a business' data governance framework.

Understanding cloud service options

Some businesses may tend to think that implementing a cloud solution is a plug-and-play exercise which absolves the business from any responsibility for how cloud services are managed. Cloud services will not, in general, be tailored to the needs of a particular business. As such, a business will need to research various cloud offerings to ensure that the CSP's offering meets the particular needs of a business in terms of, for example, cross-border transfer restrictions and requisite security controls.

Businesses should also understand the importance of mitigating its risk outside of the CSP relationship. The prudent approach is to identify risk and put in place internal measures to mitigate this risk. Guidance on what is required of businesses from a risk mitigation perspective can be found in the King IV Report on corporate governance. The Report

provides that a business' governing body should govern technology and information in a way that supports the organisations strategic objectives.

Importantly, when negotiating the CSP contract, a business should use the opportunity to ask questions about the nature and extent of the cloud service in order to determine whether the offering is suited to the business' needs. Important questions include the CSP's contingency plan, data storage (locally or abroad), service levels, access to data and audit rights.

Established CSPs understand the importance of open communication in building trust in the cloud and are open to having discussions with businesses about various product offerings. Businesses should take advantage of this opportunity to satisfy them that a cloud service offering meets their requirements.

ABOUT THE AUTHOR

Wendy Tembedza is a senior associate at Webber Wentzel.