ThomsonsLawyers

Information Technology Alert

Cloud Contracting – Challenges within the Government Contracting Framework

October 2011

Introduction

The Queensland Government's Information Standard 13 (**IS13**) requires Government departments, agencies and Government Owned Corporations (**agencies**) to utilise the Government Information Technology Contract (**GITC**) for the procurement of information technology products and services.

GITC is predicated on the basis that the products and services being secured can be tidily bundled and identified and will, generally, be provided to the Government entity through its in-house server or through a local area network (**LAN**). However, with the growth and development of 'paperless commerce', e-contracting and cloud contracting, the challenge is to ensure that the contracting provisions within GITC are modified (within the parameters permissible by the Government) to enable Government entities to access and benefit from the state-of-the-art technology while still protecting the integrity of its information and systems.

What is Cloud Computing?

Cloud computing is the provision of computing services over the internet from a remote location, rather than services from a desktop, laptop, in-house server, smart phone, tablet or other mobile device. Rather than provide services in-house, the individual or organisation contracts with a provider for the delivery of software, other applications and storage via the internet. In short, provided internet access is available, computer applications and information are available to the user regardless of where they are physically located.

Security

With the change in paradigm, there is now a new range of complex risk issues to identify and address. Central to these is the shift from all information and programs being stored on the Government's servers, to information being imparted and stored through the third party vendor. Key, then, is ensuring that each vendor has security systems and programs in place to protect the Government entity. For example, to obtain information from a particular server or LAN, a hacker had to specifically target that system. However, with cloud, a hacker can target and attempt to hack into a provider's system and, if they are successful, potentially have access to information from a large number of systems.

Data access

A key issue is how data is managed. Under the system where the service provider's staff physically enter the agency's offices or have access to the systems through remote access arrangements, the agency has the ability to undertake some level of security clearance and, through its own information technology personnel, to scrutinise and audit the activities of the service provider.

This level of scrutiny and audit will not, however, be easily replicated within the cloud systems. It is therefore crucial to know and understand how each vendor selects and verifies employees, the checks made in respect to them and the on-going scrutiny of their activities.

Privacy

Government agencies owe duties in respect to the personal information they collect and store about individuals. These duties arise under a range of legislation including the *Privacy Act 1988* (Cth) and *Information Privacy Act 2009* (Qld).

Under the Privacy Act, companies have an obligation to ensure that personal information is not sent overseas without the consent of the individual. Added to that, different countries have their own approaches and values

in respect to the protection of personal information. While the agency can contract with an Australian-based provider and contractually require that data be stored in a specific jurisdiction, there are practical difficulties in auditing to ensure that this is being undertaken.

Government information is often, by its very nature, sensitive. It also has a value to other people (not always with the best of intentions). If that data is stored in a shared environment with information from other sources, how will the vendor protect it and how can the agency audit to ensure that it is being protected? While encryption is one solution, it is by no means fail-safe and once it is in the cloud, the agency has significantly reduced ability to audit where it is located and the way it is managed.

While under clauses 5.5 and 5.6 of the Customer Contract Provisions, obligations of confidentiality and secrecy are imposed on contractors and approved parties, the agency's dues cannot simply be abrogated by passing the liability and responsibility through to a third party. The challenge is that, with cloud computing, there is no way of knowing where the data is actually stored.

The challenge, then, is to be able to put in place processes to enable the agency to audit the activities of the vendor in a cloud computing environment and subject them to normal good governance oversight.

Back Up

Agencies traditionally ensure that there are back-up systems in place to cover situations where there are problems within the system, the services are not provided in accordance with the contract or a service provider goes into liquidation or sells its operations to an off-shore entity which then exits the Australian market.

Having access to back-ups of software and data provides some comfort to agencies in the event of the service provider not performing and the agency wishing to terminate the engagement. The agency is better placed to prevent being 'at the mercy' of the service provider or being pressured to pay additional costs to ensure continuity of access. Previously, under section 11.7 of the GITC Customer Contract Provisions, source code could be placed into escrow. However, this may not be a practical risk mitigation solution in the cloud paradigm.

The issue for agencies is to identify the back-up systems of the service provider and how these can be accessed by the agency. Ask the simple question - how can the data and applications be securely replicated on an on-going basis and how can access be guaranteed to the agency?

Conclusions

1. Put in place risk assessment and controls which take into consideration the particular challenges and risks with cloud computing.
2. Oversee the cloud computing – transparency and on-going due diligence are fundamental aspects of the agency's risk mitigation strategy. This can be done either through the agency's internal IT capabilities or by engaging a third party to undertake on-going oversight and reporting to the agency.
3. As part of the procurement key selection criteria, include a requirement for the provider to provide evidence of its security processes and the access to its systems it can provide to enable the agency to audit the on-going compliance and effectiveness of the security systems. These can then be included in the GITC as specific requirements.
4. Choose what parts of the commercial and other operations of the agency are most efficiently serviced through cloud computing and firewall the other operations and information of the agency. Cloud computing should not be considered as a 'whole of operation' option.
5. Ensure loss is covered – the performance guarantee or financial security provided in accordance with clause 5 of the Customer Contract Provisions and the Liquidated Damages under clause 11.6 need to be sufficient to cover the loss the agency may incur in the event of a breach or the delay. It should be noted, for example, that under clause 11.6.5, where liquidated damages are payable, they will be the 'sole measure' of the agency's 'loss and damage for the Contractor's delay in performing and completing a Stage'.
6. Check insurance policies effected in accordance with clause 5.1 of the Customer Contract to ensure they are broad enough to cover the losses the agency may suffer in the event of a breach.
7. Before agreeing to an amendment to exclude 'consequential' or 'indirect' losses, consider what the particular risks and likely losses are then decide any level of exclusion for indirect loss.

About Thomsons

We have considerable experience acting for Government and for GOCs and therefore we understand the Queensland Government's requirements of its departments, agencies and GOCs to utilise GITC for the procurement of information technology products and

ThomsonsLawyers

Sydney
Melbourne
Brisbane
Adelaide

services. That experience has also provided us with the understanding of the limitations placed on public sector procurement to negotiate contracts which meet the commercial drivers of the provider, while meeting the risk and cost limitations of the Government.

We understand the limitations which GITC imposes, including its terms which are based on 'tidily bundled' products and services being procured. Equally, we are also very aware of the limitations this imposes, especially in enabling the procurement of new and developing technology, not the least of which being the development and expansion of cloud computing.

We pride ourselves on our continuous monitoring of new technologies to ensure we can assist our clients to access and gain the benefits of new technology, while understanding and addressing any risks this imposes. Our lawyers are here to work collegiately with our clients to ensure the best whole of life outcome and value for money.

Written by:

Kathie Sadler
Special Counsel
+61 7 3338 7515
ksadler@thomsonslawyers.com.au

For further information, please contact:

Ben Coogan
Partner
+61 7 3338 7503
bcoogan@thomsonslawyers.com.au

Peter Le Guay
Partner
+61 2 8248 3424
pleguay@thomsonslawyers.com.au

Kathie Sadler
Special Counsel
+61 7 3338 7515
ksadler@thomsonslawyers.com.au

Matthew Prescott
Senior Associate
+61 8 8236 1147
mprescott@thomsonslawyers.com.au

www.thomsonslawyers.com.au