Cloud Computing

Risks and Rewards

Useful for: Government, Local Government, Government Business (all kinds)
Article looks at: Cloud Based Contracting

Last updated on 1 January 2025

SOFTWARE IN THE CLOUD

In Brief

- Cloud computing enables a user to hold and access their data over the internet. The data is held in the cloud on servers hosted by a third party provider (supplier).
- A Software as a Service (SaaS) agreement is a sub-category of cloud computing. This model comprises a standard online platform and grants Users a restricted user licence (which may or may not be able to be tailored to the needs of the particular User).
- Advantages of SaaS agreements over bespoke software development and management by the organisation of systems held on its own premises are:
    - they are able to streamline business systems and decrease time and costs sunk into management and maintenance of IT systems; and
    - Enables efficient communication between User and its customers and suppliers and can automate a number of processes.

BUT

- a potential downside is that your business information (which may include confidential information and personal information of your employees/third parties) is held in the cloud which carries its own risks.
- governments and some corporations will have policy restrictions on where their information can be held.
- the features of the platform will be restricted and may not be customisable to meet the needs of your business.

CLOUD COMPUTING

What is Cloud Computing?

Short answer – the availability of computer system resources on demand through a model that does not require (or often even allow) specific management actions to be carried out by the user.

Cloud computing enables a user to customize and manage any software application on a server hosted remotely by a third-party supplier. Cloud computing lets you provide access to your data on public servers via the internet – you can use different devices interchangeably and you don't have to store data on your own physical hard drive. Users do

however, need to be connected to a network in order to use an online application or retrieve data that is stored in an online database.

Cloud computing offers a few different other service models in addition to SaaS - IaaS (infrastructure as a service) and PaaS (platforms as a service). Each of these models covers an aspect of IT management as an alternative to your servers being located on your own premises. SaaS agreements are used to manage and solve particular business processes and needs, whereas IaaS or PaaS provide basic tools for businesses that want to build and customize their own applications.

An organization can have a multi-cloud infrastructure, using more than one cloud platform to meet its various needs. Additionally, services may be provided via public cloud, private cloud, or a hybrid of the two – essentially a hybrid cloud is a mixed computing, services and storage environment made up of a public cloud solution, private cloud services, and on-premises infrastructure. Hybrid approaches may be used to reduce business risk by ensuring a business meets its regulatory and data sovereignty requirements, as well as those of highly sensitive clients it may be contracting to, such as governments.

SaaS based Applications

SaaS agreements involve the delivery of an application as a service that is ready-to-use and hosted in the cloud, whether public, private or a combination of both. Contracts are usually entered into via "click wrap" arrangements to either a pay-per-use or a subscription service – that is, you read the terms and conditions, privacy statement and any other relevant material and tick boxes online to indicate acceptance of the terms, resulting (usually) in a monthly or annual commitment. There is often (but not always) very limited ability to negotiate terms, so do your own due diligence as to where the data is being held and read the terms and conditions generally to ensure that there are the required levels of protection of your data built in.

SaaS provides fully developed software, without any responsibility on users to maintain it and in that way is often a cheap and effective way to ensure the business is efficient in sales, communications, customer service and project management, and is not outlaying resources on maintaining, updating and dealing with problems with the platform.

Some well-known and commonly used examples of SaaS applications are Salesforce, Dropbox, DocuSign, Adobe. A SaaS agreement can also be for an application or system developed as a bespoke solution for the User with the data held and potentially moving between public and private cloud locations.

LEGAL ISSUES TO CONSIDER

Before clicking "Accept" on the terms and conditions, or entering into a tailored SaaS agreement for services, care needs to be taken by the User to ensure they are getting what they need from the particular application or platform and that their information (which often includes personal and/or confidential data and information of their own customers as well as

their own commercial in confidence business information) is going to be adequately protected and secured.

Consider the following points:

- Are you signing up to standard terms of use that cannot be modified at the front end and may be changed unilaterally by the supplier simply by them giving notice in the form of new terms and conditions on their website? If so, read and understand the terms and consider their possible flow on effects on your business and any affected third parties, such as your employees/customers. Also give consideration to whether you run any major risks if the supplier does change its standard terms. Can you terminate your usage easily and without penalty?

- Does the supplier have an appropriate privacy policy that explains the extent of protection of their customer's data/personal information that they hold?

- How well known is the supplier? What is its reputation in the market? Does it have any history of action being taken against it for security breaches? If it is a young/small developer what is the situation if a third party's intellectual property is infringed in the supply? Does supplier warrant that it owns the IP? If you are storing your own IP in the platform and it is compromised, does the supplier indemnify you against losses?

- What are the services being provided and the KPI's the supplier will meet? Look for simply stated but technically specific descriptions of the service, as opposed to broad "woolly" advertising type material that is unlikely to be enforceable (especially where the SaaS agreement is being tailored to your business);

- What support/updating of the software does supplier have to provide you? How often? What is the extent of updates provided free, and what will you have to pay extra for? Does the proposed support system suit your particular needs? For example, depending on the nature of your business, it might be imperative that specific standards are set for emergencies, such as risk of significant impact on your own clients if the system fails, even for a very short period of time.

- What happens if supplier breaches a specified term or standard? Being able to terminate the contract may not be an appropriate remedy for you. Are financial penalties a viable option?

- How does the liability risk as between you and the supplier and third parties fall? If a failure causes damage to a third party (for example, breach of Intellectual Property laws, breach of Privacy laws) does the supplier carry liability? Does the supplier carry appropriate insurances (public liability/professional indemnity/cyber security?). Should you consider carrying a cyber security policy to cover your risk under SaaS agreements and other general business risks associated with cloud computing generally.

- A cyber security insurance policy may include coverage for risks such as:

- Revenue loss from the business interruption caused by system failure
- Negotiators
- Data recovery or replacement
- Third party data loss and liability
- Legal defence claims
- Government Investigation
- Copyright infringement
- Intellectual property misuse (online)
- Crisis management and monitoring
- Prevention of further attacks

- In what physical location is the data centre or server farm where your business data (and potentially that of your staff/contractors/customers) will be held? If outside Australia, this may create issues for you under Privacy legislation (Commonwealth State or Territory), the EU General Data Protection Regulation (GDPR) or other legislation relevant to use and/or location of your customer information overseas. Government officers should also be aware of local legislative controls in each State and Territory in relation to where a government can hold personal information.

- What rights do you have to make adaptations or further developments to the software (customisation)? Does the supplier make its application product interface (API) available to you to enable further development of your business systems?

- Transition out issues - How long after the term of the agreement will your data be held? Does the supplier have an obligation to securely delete your data at any point, or on request? Does the supplier promise to return all your data to you at the end of the contract in the format that you choose?

Depending on the supplier you are contracting with and the extent and nature of the service model being designed/delivered to you, some or all of these questions may be relevant. The risk/reward analysis will be different for each kind of service, but proper risk management up front will help avoid damage occurring to your business where there is a breach of data security or other unforseen problems with the contract.

Important Note: This information is general and is not intended to be a substitute for specific legal advice in relation to your particular contract. If a contract is important enough to you to ensure it is right, seek legal advice.