LAW INSTITUTE VICTORIA

CLOUD COMPUTING ESSENTIALS

WHAT IS CLOUD COMPUTING?

Simply put, cloud computing is the delivery of computing resources over the Internet. "The cloud" is really just a short-hand term adopted for delivery via the interent because clouds were often used to represent the internet in computer network diagrams. Other related terminology "cloud" offerings including "Software-as-a-Service" (Saas) and "Infrastructure-as-a-Service" "IaaS". The alternative to cloud computing is to use "on-premises" computing resources, such as a local "on-premises" server or software that is accessed thorugh being installed to a personal computer.

Most people are use cloud computing every day such as when using internet banking, social media and online shopping. Companies that provide cloud computing offerings are called cloud services providers and their services are delivered via a data centre, or in some cases multiple data centres, that could be located anywhere in the world. These days, there is little practical distinction between a software provider and a cloud services provider. Some software providers offer exclusively cloud solutions (eg Xero), some offer both cloud and on-premises options (eg Microsoft Office).

Some examples of cloud services that you may already be using in your law practice include:

- Data storage services such as Basecamp, Drop Box, and Amazon Web Services.
- Productivity tools such as Microsoft Office 365 and Adobe Creative Cloud.
- Online book keeping services such as Xero and MYOB online accounting.
- Social media applications like Facebook, Twitter and Linked-In.
- Webmail services such as Gmail, Yahoo, and Hotmail.
- Google Docs and Google Drive.
- Data backup services such as Mozy, iCloud, IBackup, CrashPlan and Carbonite.

WHAT ARE THE BENEFITS OF ADOPTING CLOUD COMPUTING IN YOUR LAW FIRM?

- Cloud computing services which are delivered from a good quality data centre can be expected to have high levels of physical security; employ stringent security policies, processes and systems and utilise dedicated personnel with specific expertise in managing the infrastructure located within the data centre. Often, these systems are more sophisticated and robust than a firm's equivalent security systems.
- Cloud computing can be expected to deliver better data backup and data recovery capabilities than an on-premises server sytsem. Cloud providers are likely to utilise several data centres in different geographic locations and mirror the data and applications across at least two of them. This arrangement provides a more robust capability to survive or recover from a natural disaster or major power failure.
- There is greater scalability with the ability to increase or decrease the capacity of the cloud computing service as required and without substantial capital investment, allowing an organisation to be more agile in adapting to changing needs.
- Using cloud computing minimises up-front capital expenditure, as it is the responsibility of the cloud provider to take care of providing the required infrastructure. This results in costs being moved from capital expenditure to operational expenditure, and reduces the total cost of ownership of the infrastructure.
- Cloud computing allows staff to adopt more flexible working arrangements, with the ability to more easily and cheaply access information and IT systems from home, or other locations, remotely without requiring a Virtual Private Network (VPN) or a remote access software.
- A good quality cloud provider can be expected to keep their systems well maintained and updated, which means you benefit from having systems that are always operating optimally and you get access to the latest improvements and enhancements in a more timely fashion without relying on your own firm's IT support systems.

WHAT ARE THE RISKS ASSOCIATED WITH CLOUD COMPUTING?

- The security and confidentiality of your information can be compromised if, for example, if your cloud service provider has not implemented adequate internal security measures at its data centres.
- You may not be able to access your information on demand as required. For example, if the cloud service provider's data centres are not fully operational due to maintenance or failure.
- There may be potential for unauthorised disclosure of your information stored in the cloud resulting from security breaches and/or through other forms of unauthorised disclosure, for example, if the cloud service provider does not adequately encrypt your data.
- You may face ownership and licensing issues regarding information stored within the cloud service, as it may be unclear who owns, or has the right to use, information stored within the cloud.
- You may be confronted with temporary loss of access to information stored in the cloud, for example, due to a loss of internet connection.
- You may experience permanent loss of access to information stored in the cloud, for example, if the cloud service provider fails to adequately backup your information.
- You may be exposed to geographical risks in relation to data sovereignty, as your information may be stored outside Australia and be subject to different legal regimes. This can also lead to regulatory issues, such as then being in breach of your Privacy Act obligations or inadvertently breaching the data obligations of those different legal regimes.
- You may experience problems regarding preserving, delivering, or deleting information at the end of your services contract with the cloud services provider.
- Ascloud computing is reliant on an internet connection, issues such as internet speed, quality, reliability and availability become much more important for the overall functionality of the business.
- A firm will become reliant on the level of support provided by the cloud service provider, meaning that if support responses are not provided in a timely fashion, they may impact on the functionality of your practice.

CLOUD COMPUTING ESSENTIALS CHECKLIST

1. Have you used a structured selection process (either through research or engaging an expert adviser) to both compare the offerings, including as regards your existing solution, and also to ensure that the cloud service provider's website, terms of service, service level agreement, privacy policy, security policy, data retention policy, data breach policy and other policy documents are reviewed and understood?
2. Has your cloud services provider provided proof of its compliance with the relevant industry standards, in particular as regards the standards of its data centre (see, for example, the standards produced by the Legal Cloud Computing Association – www.legalcloudcomputingassociation.org)?
3. Have your clearly defined performance obligations, including support response times, with details of how performance is measured and what enforcement mechanisms are in place if performance obligations are not satisfied?
4. Have you settled an 'exit procedure' with your cloud services provider allowing you to erase information and easily transfer it to another cloud services provider if you elect to?
5. Have you determined what will happen to your data if the cloud services provider encounters business continuity issues, for example, bankruptcy?
6. Does the cloud services provider have a policy and/or system regarding data encryption and access to your data by the system administrators and/or third parties?
7. Can your cloud services provider warrant that all data will be held within Australian data centres?
8. Have you evaluated your existing internet service and the impact on functionality moving to a cloud service might have?
9. Have you negotiated a dispute resolution procedure with your cloud service provider, which includes provisions relating to access to data during any dispute and during any migration of data, such as a data escrow arrangement?