

Cloud Computing Technology – Supporting Business Continuity

Issue 8

Cloud computing is a general term for anything that involves delivering hosted information technology services over the Internet.

A fully cloud dependent organisation may not run a computer server on any of its premises, instead operating live over the internet to the cloud service provider hosted computers, which could be located anywhere in the world.

This is a very versatile and cost effective way of working, when demand is changing or growing rapidly, computing capacity can be easily increased to support this. Where software is provided by a cloud service, changes can be deployed rapidly for all users. The service also provides broad network access allowing use of mobile devices to access data.

Many organisations are avoiding the high capital costs for server purchase or upgrade and are beginning to utilise a remote service provider for part, or all of their computing and data storage requirements. This may present an emerging risk to an organisation.

When considering a cloud service, the organisation may avoid difficulties by asking questions to ensure an acceptable level of risk control is provided. How safe and secure is data hosted by a cloud computing service? Who owns and can access the data? Where exactly is it stored? In the event of a major interruption to computing services the cost of restoring lost data can be significant.

Cloud technology operates from fixed hardware operating in a service provider premises, using an internet connection linked to a communications company. If the premise is within Australian jurisdiction, our building codes apply. Public utility services such as power supply and communications are rated reliable. Australian based services are expected to comply with local government policy and business principles.



A large cloud service provider is likely to offer better computing infrastructure, security and reliability. This may include un-interruptible and filtered power supply with a stand-by electrical generator set to power computing systems and air conditioning should there be a public supply failure.

Fire protection may include an early warning air sampling system linked to automatic gaseous fire suppression to minimise fire and equipment damage. Fire compartmentation may provide separation between computer main frames and other hardware services to limit the extent of damage and interruption.

Premises security surrounding computer hardware may be more comprehensive including access control and intruder detection.

Further questioning requiring technical knowledge or legal support may be required before a service provider is chosen and a contract is completed. The type of data and network, (public, private or hybrid) may determine the level of computer system security required for staff and or public access. If there is a breach of data security what response is expected from the service provider? What external services is the Cloud company dependant on and do these services have a known level of redundancy?

Larger cloud computing companies have duplicated sites or contracts with a secondary company to provide independent automated backup to services offered. This means that a changeover will be unseen if the main data centre operation is interrupted or a public communication link fails.

Legal questions include ownership and portability of data when held in custody by a third party. If at some time in the future an alternate cloud service provider was used, would the business data be in a form that permits portability and compatibility with another service provider? In the event of the cloud host becoming insolvent what provisions exist for service continuity?

Trusting business information technology to an external cloud service provider can be advantageous. Establishing and managing this correctly will ensure that an acceptable level of data access, security and reliability exists.

For more information:

Contact us at
riskengineering@vero.com.au