A GUIDE TO THE CLOUD
CLOUD COMPUTING
What is it and how does it work?

STORED IN THE CLOUD
Files are uploaded via the internet to a cloud service located in a data centre. Businesses are choosing to use software that is served from the cloud.

A public cloud is the standard cloud model, open to a largely unrestricted universe of users. Designed for a market, not a single enterprise.

A private cloud is designed for, or access restricted to, a single enterprise.

A hybrid cloud includes a variety of public and private options with multiple providers.

A community cloud is accessed by organisations that want to use a common cloud environment.

Total cloud computing market in Australia will increase from $884 million in 2012 to $2.7 billion in 2017. (source IDC)

BACK DOWN TO DEVICES
Individuals and companies can then access files on the go from phones, tablets or computers connected to the internet.
Business interest in cloud computing has grown significantly over the last few years. This is likely to continue to increase as businesses focus on keeping costs under control and gain a better understanding of the benefits cloud computing may have for them. While cloud computing has potential for many businesses of all sizes, it is not without issues.

Moving to the cloud or switching software or service providers can be a major decision for many SMEs. As with any big decision, it is good business practice to subject the idea to a rigorous cost–benefit analysis. If you do decide to move or switch, it is important to have clear reasons and objectives to ensure you are successful. This will help you in deciding the cloud service provider that best meets your needs.

This guide provides useful insights on what the cloud is and examines key issues, including security and legal issues you should consider before making a decision, be it a move to the cloud, change of your provider or software solution.

Cloud computing creates possibilities for every business that have previously only been available to the very largest. It means a company’s IT capital budget no longer has to constrain its thinking, a physical location need no longer define where and when work gets done, brilliant ideas and innovation can be shared and collaborated on in real time - no longer put off or forgotten. It is one of the truly great productivity enabling tools available to business today.

I have seen how cloud has benefitted businesses in ways they never expected and that’s why I’m proud to present this guide to cloud computing and make the concepts understandable and accessible to more businesses.

Industry experts and case studies will take you through the benefits while also discussing the risks, security and privacy issues presented by this new model of corporate computing and operating.

On behalf of every business that gains insights and improves as a result of this guide, I’d like to thank the contributors for their time and insights. I trust they will answer many of your questions and provide the impetus to get moving into all the cloud has to offer – because your business should only be limited by your imagination, not your hardware.
THE INS AND OUTS OF CLOUD COMPUTING

Why small and medium enterprises (smes) may be interested

**PRODUCTIVITY**

It can increase productivity.

If your computing takes place in the cloud, your staff can use the internet to access the business systems they need when they are on the go through laptop computers, tablets or smart phones. This is good news for any business with staff who work offsite for whatever reason, be it from home, with a customer, or in the field.

The same benefits apply if your business is a link in a supply chain. You can communicate with others in that supply chain through common systems stored in the cloud.

**SCALABLE**

Cloud computing can allow small companies to act like big ones.

With an elastic supply of processing power at their disposal, SMEs can use big data to road test new ideas.

**CAPITAL SPENDING**

Cloud can reduce capital spending.

Upfront costs of computer equipment into predictable operational expenditure.

**ONGOING COSTS**

Cloud can help ongoing costs fall.

Cloud providers spread the expense of infrastructure and technical specialists across many customers. IT maintenance costs are likely to be less as the cloud provider takes over maintenance, upgrades and security.
THE INS AND OUTS OF CLOUD COMPUTING

Why small and medium enterprises (SMEs) may be interested

1. **THE QUALITY OF INTERNET CONNECTION IS CRUCIAL.**
   Given data is transported to and from the cloud via the internet, intermittent or slow access will slow processing times. Many software suppliers have taken this into account and allow for local processing and back-up but this can’t be assumed.

2. **YOUR IT STAFF MAY NEED SOME CONVINCING.**
   Some may feel threatened by a move to the cloud. An alternative view is many employees are already using internet storage that the IT department does not control. An enterprise shift means IT can work with business on the optimum cloud solution.

3. **THE LOCATION OF YOUR SUPPLIER IS IMPORTANT.**
   There are important security and privacy issues to be considered in the cloud and legislative requirements differ depending on whether your cloud supplier is Australian based or not. This is explored in more detail later in this document.

4. **YOU NEED TO GET THE RIGHT ADVICE.**
   There are pertinent technical, corporate and IT governance issues as well as security and privacy considerations. It is recommended you discuss cloud computing intentions with an advisor you trust before making any big decisions.

---

Some factors to watch out for:

- **IAAS**
  Infrastructure as a Service allows a business to relocate its applications to run in virtual servers located within the cloud computing service provider, but the business remains in control of, and responsible for, its software and data.

- **SAAS**
  Software as a Service (SaaS) is the full cloud package, where the applications a business runs, its data and its server are managed and operated offsite by the cloud service provider.

---

<table>
<thead>
<tr>
<th>UTILITY HOSTING</th>
<th>DEDICATED HOSTING</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAAS</td>
<td>SAAS</td>
</tr>
<tr>
<td>INFRASTRUCTURE AS A SERVICE</td>
<td>SOFTWARE AS A SERVICE</td>
</tr>
<tr>
<td>PRIVATE &amp; PUBLIC NETWORKS</td>
<td>INFORMATION ASSURANCE</td>
</tr>
<tr>
<td>SECURITY</td>
<td>MANAGED SERVICES</td>
</tr>
<tr>
<td></td>
<td>MOBILITY</td>
</tr>
<tr>
<td></td>
<td>APPLICATION ASSURANCE</td>
</tr>
<tr>
<td></td>
<td>SERVICE ENABLERS</td>
</tr>
<tr>
<td></td>
<td>SECURITY</td>
</tr>
</tbody>
</table>

---

ON THE MOVE | AT HOME | REMOTE BRANCH | HEADQUARTERS | OVERSEAS BRANCH

---

**IAAS**

**SAAS**

---

**A GUIDE TO THE CLOUD**
Migrating to the cloud

This needs to be carefully planned.

If you are considering infrastructure as a service, you need to know how your application is going to work in the cloud.

If the application is susceptible to latency, it could have a significant impact if you shift it to the cloud (this is a good reason to consider an Australian based data centre).

It’s also important to know if your application can start and stop easily, a quality that is known as check pointable. Many cloud providers offer spot pricing on systems that can make a huge difference to your costs. That price goes up and down depending on demand. If the spot price goes up, you might get booted off until it goes down again.

Companies need to consider the cloud as another piece of infrastructure. The great thing about cloud resources is you can switch them on and off but you need to consider how your software will run on this new infrastructure.

“YOU NEED TO KNOW HOW YOUR APPLICATION IS GOING TO WORK IN THE CLOUD.”

Security

Cloud providers are generally more secure than their customers. Their reputation relies on it. They really can’t afford to get it wrong.

Nearly all cloud-related dangers can be guarded against and I would recommend a detailed evaluation of your chosen supplier before you shift any data.

If managed well, a shift to the cloud is an opportunity for SMEs to become more secure.

Once you’re there

One of the big benefits is that you can dial up as much power as you want. So you may well be able to run some big computations in parallel rather than sequentially; that’s one aspect of cloud computing economics that many people don’t realise.

At the moment we are exploring this for a group that processes images. To fully analyse these images takes about a week running on nearly a thousand computers. But in the cloud we can run, say, ten of these processes in parallel for the same price as running them sequentially. That is a massive improvement.
Privacy
Cloud service providers can operate anywhere in the world, and you often do not know where they are located, or where the data you store with them is located. So you need to understand what privacy obligations you take on when you provide data to a cloud service provider.

Recent changes to the Privacy Act mean that if an Australian business discloses personal information to a company that does not carry on business in Australia – and is therefore not subject to the Privacy Act - the Australian business will be liable for any privacy breach by the recipient.

If you are not prepared to take this responsibility on, then you should make sure your cloud provider carries on business in Australia.

Data sovereignty
Another concern that many commentators have identified with cloud computing relates to data sovereignty, which refers to the ability of foreign government agencies to access data that is stored in the cloud network. In particular, cloud commentators have focussed on the US Patriot Act as a cause for concern as it may allow US government agencies to access information stored on cloud networks operated by US companies.

“IF AN AUSTRALIAN BUSINESS DISCLOSES PERSONAL INFORMATION TO A COMPANY THAT DOES NOT CARRY ON BUSINESS IN AUSTRALIA THE AUSTRALIAN BUSINESS WILL BE LIABLE FOR ANY PRIVACY BREACH.”

While the Patriot Act did significantly bolster some existing laws that give US law enforcement agencies various investigatory powers, extra-territoriality was already a feature of the existing law. Moreover, many other countries, including Singapore and Australia, also have wide-reaching information gathering laws.

Although data sovereignty issues are complex and nuanced, they have received less publicity in recent times and have been overshadowed by other events.

At the end of the day, businesses need to be aware that once they store data externally, including on cloud services, then governments and law enforcement agencies may well be able to obtain access to that data under relevant information gathering laws.

Of course, even if data is retained by businesses on in-house systems, governments and law enforcement agencies will be able to access that data – but in this situation at least the business will be able to manage and deal with that information access request itself and will not have to rely on a third party to defend its interests.
About the Privacy Act

- The Act does not apply to businesses with an annual turnover of $3 million or less but there are exceptions.
- If you are in the health industry, or in the business of selling information, or contract with a Commonwealth department to provide outsourcing services, you are likely to be subject to the Act, no matter how big your business is.
- At a practical level, if you contract with a large company, that company will very often require you comply with the Privacy Act.
- The Act is not intended to be difficult but to provide a reasonable standard for security of information. So if you want to be able to say to your customers, "I take reasonable steps to keep your information safe," you should consider observing the standard set out in the Act, even if the Act does not apply to you.

KEY POINTS

- **Minimise liability** by using a supplier that is subject to the Australian Privacy Act.
- Even if you are exempt from the Privacy Act, it is wise to comply.
- Be aware of privacy obligations imposed on you under contracts – particularly with government agencies that may impose stricter obligations on you.
Why businesses are shifting
The beauty with a pay-as-you-go model is you can try something out and if it doesn’t work, you can shut it down. That agility is the key reason businesses are interested in the cloud. Without the need for capital investment in IT, the cost of failure is lower.

Everyone’s appetite for cloud services will be different and there are many aspects to consider. The potential cost advantages, for example, need to be weighed against future considerations such as the potential difficulty involved in migrating from one cloud service provider to another.

We don’t know many organisations that are packing everything up and putting it in the cloud. It’s more about simplifying the existing environment. Instead of having to expand their hardware, organisations can use their existing assets for a bit longer.

I think small organisations, by their very nature, can be more nimble and they’ll probably consume and migrate to cloud services long before large organisations, many of which have big legacy applications that have a significant life left in them.

Key considerations
The key issues are availability, identity management, security, a tangible return on investment, reporting on Service Organisation Controls by the cloud provider and alignment with your risk appetite, especially in relation to regulatory and contractual obligations.

An organisation considering moving to the cloud needs to examine its business governance of IT and make sure it’s aligned with a cloud-provided IT environment.

One challenge for an organisation that chooses to select the cloud is to ask ‘What is the disaster recovery strategy now?’ That organisation is used to an environment where it probably has automatic switchovers in place, backups and off-site storage and it owns and controls the assets. The word control is key here. In the cloud, that organisation doesn’t control what happens.

“THE KEY ISSUES ARE AVAILABILITY, IDENTITY MANAGEMENT, SECURITY, A TANGIBLE RETURN ON INVESTMENT, REPORTING ON SERVICE ORGANISATION CONTROLS BY THE CLOUD PROVIDER AND ALIGNMENT WITH YOUR RISK APPETITE, ESPECIALLY IN RELATION TO REGULATORY AND CONTRACTUAL OBLIGATIONS.”
Availability in the cloud or outsourced entity should not be assumed just because the provider is a large organisation. There are still risks of uncontrolled downtime, cyber-attack, natural disaster or business failure resulting in receivership, or the cloud provider choosing to no longer be in that business.

An organisation might, for example, decrease the risk by working with two cloud providers. But replicating data or business functionality with a different provider in a different data centre will obviously cost more. Keep in mind that the second cloud strategy may not provide full functionality but rather minimal processes necessary for survival.

**Access management**

It’s important that people only have access to the data and services they need to perform their duties, and it is equally important to have controls in place for when employees or users leave.

In a classic, active directory, locally-controlled server based organisation, if the right controls are in place, the HR department tells the IT department John Smith is leaving the company on this date and IT takes Mr Smith off the network that day. But unless controls are enhanced in a cloud environment, IT may either no longer be aware of the departure, or assume it’s a business responsibility.

**Continuous controls monitoring**

You need to know the right systems and monitoring are in place to identify if controls are still working. In other words, if your key controls are broken, then your risk appetite assumptions are also broken.

Organisations that are considering adopting a cloud computing model can consider seeking an independent report from the cloud provider on the effectiveness of its control environment.

“POTENTIAL COST ADVANTAGES NEED TO BE WEIGHTED AGAINST FUTURE CONSIDERATIONS.”
Do I need to ask customers and staff about moving personal data to the cloud?
Changes to privacy law that came in early 2014 require businesses covered by the law and government agencies to be more transparent about how they handle personal information.

Personal information is data that could identify an individual. This includes names, addresses, telephone numbers, dates of birth, medical records and bank account details.

Some important points to note:

• If entities disclose personal information to an overseas organisation or agency, they need to make sure the data will be handled in accordance with Australian privacy law. Note some SMEs will be exempt from this law.

• If personal information is mishandled by the overseas organisation or agency, the entity that disclosed that information may be legally responsible for this.

• These obligations don’t apply in some circumstances, such as when customers or staff specifically agree to their information being disclosed to an overseas organisation or agency.

What about migration of data in the event I want to change cloud service providers?
It is important to consider not just the initial move to the cloud but possible future moves between providers. Some cloud service providers have begun to address concerns about data interoperability however data portability remains a key concern. Some of the larger cloud service providers are incorporating de-facto standards which are specifically addressed by software vendors. Once again, this is an area SMEs need to consider carefully and should seek advice on.

How should an IT manager approach the cloud?
IT specialists will be well aware that the advent of public cloud services has already changed the way people think about IT. If a marketing department, for example, wants a new website it can either go to IT or to a third party who may host that website off-premise.

IT departments and managers should aim to become a trusted adviser for cloud services, to assist in procurement and ensure cloud services are managed in a way that does not put the organisation at risk.
Who is responsible for software upgrades?
The contract between the cloud provider and the customer should indicate when updates and enhancements will occur. One point to watch out for is compatibility. In the world of on-premise computing, a business would typically take the update from the supplier and do some testing before rolling it out but there has often not been a lot of governance around that. This needs to be cranked up in the cloud as the provider is unlikely to be responsible for whether an upgrade is compatible.

What level of service can a cloud provider give to a small business?
Small businesses should always be on the lookout for ways in which they can improve their operational efficiency. Cloud computing can assist in this pursuit because businesses will only have to pay for the services they use. You could compare it to turning on the tap when you want some water. It is much easier to be connected to a mains supply than to run your own processing plant. Large cloud providers have invested considerable amounts in monitoring and security and small businesses can take advantage of economies of scale and the specific technical skills of cloud service providers.
The need
Since 1992, KinCare has been a family owned company providing high quality, in-home care for elderly people and people with a disability. A recent merger made the organisation national but it also brought some serious ICT challenges. The company suddenly doubled in size and had four different IT systems running its operations. It needed to get them all onto a single platform, it needed to get a lot of new people onto its IT systems and it had a shortage of capital for infrastructure investment.

“WE’RE ABLE TO SCALE AS OUR EMPLOYEES GROW AND AS OUR CUSTOMER BASE INCREASES”

The solution
The company decided to shift its business operations and client data to the cloud. The migration to a Telstra solution took just three weeks. The move enabled KinCare to think about new ways of service delivery. Working with Telstra, it created a smart device app that links field staff to its cloud-based customer relationship management (CRM) system.

Security priorities
The nature of KinCare’s business means it is handling some very private information for some very vulnerable customers. Data security was a key issue. It wanted its data to be hosted in Australia.

The benefits
IT staff that used to be focused on infrastructure management now concentrate on more important tasks like software development.

KinCare estimates it has saved $300,000 in capital expenditure and it is able to scale its IT as its employees and customer base grows.

One of the most important things that came from the cloud is agility, said KinCare chief executive officer Jason Howie. “We’re able to scale as our employees grow and as our customer base increases.”
NEW ERA FOR DBM CONSULTANTS

The situation
DBM Consultants is a market research company that gathers insights to help its clients to gain market share. The company has grown at about 15 per cent annually in each of the last five years. It needed a robust, flexible and manageable solution that would allow for increased network speed, greater control and security management reporting and a higher level of network reliability.

The solution
A wide area network (WAN) to link DBM’s three offices in Melbourne and Sydney.
- A WAN optimisation tool Riverbed.
- A Telstra IP Telephony.
- A security solution provided by Symantec.cloud

The benefits
- The TIPT solution has increased the reliability and frequency of inter-office videoconferencing from bi-annually to fortnightly for DBM Consultants’ clients.
- Riverbed boosted the efficiency of its network in addition to staff productivity, driving a saving of 30 hours per month.
PROCEED CAUTIOUSLY
Take it slowly. A cautious move to the cloud could take longer than expected but the outcome is likely to be better.

Know where you are coming from. Do a full cost-benefit analysis to determine what it costs to have in-house IT. You may find that it costs more than you think.

LOCATION
Where is the cloud provider’s data centre? If it is outside Australia, there could be legal implications and latency issues that greatly affect performance.

Consider the jurisdiction the contract is signed in. If you have a dispute with your cloud service provider, the dispute may only be able to be resolved through the US court system.

COMPATIBILITY
Look for a provider you have a business relationship with – don’t just go for price.

Effective communication with your supplier is going to be central to success. Consider common data formats and hardware compatibility.

Run trials to test whether the cloud solution meets your needs.

Look for good governance arrangements, for example, will the provider’s client manager meet regularly with the business?

CHOICE
Do not make your decision on your preferred service provider based on cost. A large, reputable service provider may cost more but may provide you the level of service you require and it can help mitigate some of the risks.

Ask about the level of security provided.

CONSIDER CLIENTS
Advise your clients where and how their data is stored. It may also be necessary to amend your agreements with clients to allow you to store confidential client information in the cloud.

BACKUP
Make sure that data is backed up as part of the service. Do not assume it is part of the service.

Make sure you have a Service Level Agreement (SLA) and that you read the terms carefully to understand the limitations of the service. The SLA should have clauses on response times, business continuity and disaster recovery.

DIVORCE TERMS
There may come a time when you want to part ways with your cloud supplier. What arrangements will be in place to enable an exit?

Ask what happens to your data if you choose to leave a service provider, such as deletion of data.
A survey of CPA members run in June 2014 showed:

**WHAT DO YOU SEE AS THE MAJOR BENEFIT(S) FOR YOUR BUSINESS IN UTILISING A CLOUD SERVICE?**

Rate based on importance 1 most important 4 least important

- Freeing up capital
- Increasing service levels/reducing down time
- Reducing IT infrastructure operating costs
- Creating operational efficiencies
- Improving application availability
- Improving productivity and speed to market
- Driving and support business growth
- Accessing best-practice business processes and applications
- Adhering to regulatory and/or compliance requirements
- Other

**WHAT DO YOU SEE AS THE MAJOR ROADBLOCKS TO MOVING TO THE CLOUD?**

Rate based on importance 1 most important 4 least important

- Data housed outside of Australia (Data Sovereignty)
- Assurance that the data is secure and protected
- Cost of moving to the cloud
- Lack of knowledge in the organisation
- Current line of business applications used by the organisation

Source: CPA member survey
WHAT ACCOUNTANTS THINK ABOUT CLOUD

IN THE LAST 24 MONTHS, HOW OFTEN HAS CLOUD COME UP IN MEETINGS IN YOUR ORGANISATION?

1-2 TIMES

MORE THAN 5 TIMES

3-5 TIMES

IF YOU USE CLOUD APPLICATIONS, WHAT DO YOU USE CLOUD FOR?

- Email
- Collaboration and Document Sharing
- Application Development and Test
- Hosting and Management
- Backup and Disaster Recovery
- E-commerce
- Sales Management Tools (CRM)
- Business Reporting
- Financial Applications
- Security
- Storage
- System and Network Management

Source: CPA member survey
For more information from CPA Australia on cloud computing please visit:

For more information and personalised advice on cloud services from Telstra, please email:
cloudsolutions@team.telstra.com

Things you need to know:
The views expressed in this guide are not a substitute for independent professional advice. You should seek your own independent professional advice where appropriate. TM and ® are trade marks and registered trade marks of Telstra Corporation Limited ABN 33 051 775 556.