MOVING TO CLOUD:
Key Considerations for Government

TELSTRA REPORT

October 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cloud computing offers significant financial and operational benefits for Australian government organisations; by shifting IT resources from traditional internal infrastructures to cloud platforms, costs can be reduced, flexibility increased and efficiencies improved.

Already Australian private and public-sector organisations are taking advantage of cloud computing in a range of different ways. Some are partnering to create internal (private) clouds to extract more value from existing IT infrastructures. Others are making use of the growing number of external (public) cloud providers and moving computing resources into their data centres. Meanwhile others are using a mix of both, by linking internal IT assets with external resources to create a hybrid cloud infrastructure.

By 2015, research company IDC believes cloud technologies and services will not exist on a discrete basis but will be integrated into every facet of business service delivery

In fact the rate of adoption is so high that by 2015, research company IDC believes cloud technologies and services will not exist on a discrete basis but will be integrated into every facet of business service delivery.[1]

For public-sector bodies at federal, state and local government levels, the benefits offered by the cloud are particularly significant. Tasked with providing services to citizens across a broad range of areas - from health care to national security – government is constantly looking for ways in which its investment in IT can deliver bigger returns. The cloud can help meet this requirement.

However, while cloud computing offers big benefits, there are a number of challenges to be considered in association with its use. These include data security and sovereignty, privacy, and application performance. Each must be viewed in the context of exactly how planned cloud services will be used and the systems and infrastructures on which they are to be built.

Cloud computing is well positioned to assist forward-thinking government agencies to adopt a more strategic, business-focused approach while at the same time reducing costs and improving efficiencies

Also, stretching across the whole area of cloud computing, is a range of regulatory requirements dictating how user and customer data must be handled. Privacy laws require careful consideration of how personally identifiable information is stored, while other legislation affects how data residing in different geographic locations can be subject to access requests by law enforcement bodies and government agencies.

Telstra has established an extensive and robust cloud computing offering. Built on an AU$3 billion investment in its national Telstra Next IP® network and Next G® network and incorporating a series of cloud-ready data centres, the company's cloud services portfolio is already supporting private and public sector organisations around the country. To further enhance its offerings, Telstra has committed to a further investment of AU$800 million over the next five years to support the growing demand for cloud services.

Cloud computing is well positioned to assist forward-thinking government agencies to adopt a more strategic, business-focused approach while at the same time reducing costs and improving efficiencies. The time to consider the benefits the cloud can deliver is now.

INTRODUCTION

There is a fundamental change occurring in the way computing resources are supplied to and used by Australian government and enterprise organisations. Accompanied by the benefits of cost reductions, greater efficiencies and improved organisational agility, these changes are causing a significant shift in the way information technology is viewed.

Dubbed 'cloud computing', the trend has been embraced by organisations both in Australia and around the world. Buoyed by the prospect of extracting more value and flexibility from their investments in IT, they are taking advantage of the rapidly evolving range of services on offer.

Cloud computing involves a move from traditional, in-house IT systems to either internal or externally provided flexible infrastructure or services

At its essence, cloud computing involves a move from traditional, in-house IT systems to either internal or externally provided flexible infrastructure or services. Rather than purchasing, designing, building and managing complex computing systems, enterprise and government organisations purchase capacity in an "on-demand" model. This is a form of utility computing where IT resources can be dynamically procured as and when they are needed.

Such an approach can be taken in a number of ways. Existing internal systems can be re-architected to create so-called internal 'private clouds'. A second approach involves shifting computing resources to an external cloud service provider that takes responsibility for their management and maintenance. A third approach involves computing capacity being 'rented' from a public cloud provider under a usage-based billing model.

Another alternative involves making use of a mix of these approaches. By combining internal IT systems with externally provided resources, an organisation can create a hybrid cloud. Such an approach allows extra processing and data storage capacity to be accessed as required to cover times of peak demand.

The four forms of cloud computing can be described in the following ways:

- *Private cloud* – The cloud infrastructure is operated solely for an organisation. It may be managed by the organisation or a third party and may exist on premise or off premise;
- *Community cloud* – The cloud infrastructure is shared by several organisations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organisations or a third party and may exist on premise or off premise;
- *Public cloud* – The cloud infrastructure is made available to the general public or a large industry group and is owned by an organisation selling cloud services;
- *Hybrid cloud* – The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application.[2]

INTRODUCTION

Many Australian enterprise organisations are currently either adopting or evaluating cloud computing. According to the recent IDC Asia Pacific Cloud Computing Survey 2011[3], 35.3 per cent of Australian respondents considered cloud to be maturing with either "a good foundation of offerings in the market" or "a broad and deep portfolio in the market". A further 60.7 per cent considered cloud computing to be "developing" but with issues that still need to be resolved.

At the same time, the Australian public is increasingly looking to interact with enterprise and government organisations online. With four out of five Australians now using the internet, demand for online access to information and services is growing.

The cloud computing phenomenon is gathering pace and it is vital Australian government agencies understand what it has to offer and position themselves to take full advantage of its benefits

The rise of services like Facebook, Google and Twitter, along with the growing use of ubiquitous 'always on' fixed and mobile broadband networks, means end-users are growing accustomed to this style of computing. Governments must start to think about how they implement services like this to meet citizens' needs for better, more efficient services and information from all levels of government. Cloud computing is one extremely efficient way of meeting these needs.

The cloud computing phenomenon is gathering pace and it is vital Australian government agencies understand what it has to offer and position themselves to take full advantage of its benefits.

Key drivers

The key drivers for the adoption of cloud computing by governments include:

- The need to reduce overall expenditure on IT infrastructure and maintenance;
- A desire to improve organisational flexibility and productivity;
- The need for a more scalable IT platform that allows an organisation to focus on business or service priorities and future growth.

According to recent research by IDC, up to 80 per cent of Australian organisations believe functions such as email and collaboration tools will be operating within a public cloud environment by 2014

Already cloud computing usage is growing around the world. According to recent research by IDC, up to 80 per cent of Australian organisations believe functions such as email and collaboration tools will be operating within a public cloud environment by 2014.[4] While recognising that the area is still rapidly evolving, those surveyed indicated they planned a steady adoption of cloud platforms and services in the future.

Governments across the world see major opportunities to move existing services to the cloud. In February 2011, Vivek Kundra, the former US Government CIO to the Obama Administration, estimated that US$20 billion out of a total IT spend of US$80 billion could move to the cloud.[5]

INTRODUCTION

For the US Government, the following chart encapsulates the reasons why cloud is a compelling proposition for it:[6]

Figure 2. Cloud Benefits: Efficiency, Agility, Innovation

EFFICIENCY	
Cloud Benefits	**Current Environment**
Improved asset utilisation (server utilisation > 60-70%)	Low asset utilisation (server utilisation < 30% typical)
Aggregated demand and accelerated system consolidation (e.g., Federal Data Centre Consolidation Initiative)	Fragmented demand and duplicative systems
Improved productivity in application development, application management, network, and end-user	Difficult-to-manage systems

AGILITY	
Cloud Benefits	**Current Environment**
Purchase "as-a-service" from trusted cloud providers	Years required to build data centres for new services
Near-instantaneous increases and reductions in capacity	Months required to increase capacity of existing services
More responsive to urgent agency needs	

INNOVATION	
Cloud Benefits	**Current Environment**
Shift focus from asset ownership to service management	Burdened by asset management
Tap into private sector innovation	De-coupled from private sector innovation engines
Encourages entrepreneurial culture	Risk-adverse culture
Better linked to emerging technologies (e.g., devices)	

INTRODUCTION

Investment

In Australia, cloud providers are investing considerable amounts of money in the data centres and networking infrastructure that underpin cloud services. This comes at a time when large international cloud providers, such as Amazon and Google, are pushing hard to encourage customers to make use of their infrastructures, based within offshore data centres.

In June 2011, Telstra announced it would invest more than $800 million during the next five years in response to increasing customer demand for domestically based cloud services

In June 2011, Telstra announced it would invest more than $800 million during the next five years in response to increasing customer demand for domestically based cloud services. This investment will cover a range of initiatives including:

- Construction of a new state-of-the-art, cloud-ready data centre;
- Modernisation of existing data centres;
- Expansion of the range of enterprise applications being offered;
- An increase in the automation of utility computing services.

Government direction

In response to growing interest in cloud computing among public-sector organisations, the Australian Government Information Office (AGIMO) released a Cloud Computing Strategic Direction Patper[7] in April this year. The paper encourages a strategic approach to the adoption of cloud services by public-sector organisations.

Under the guidelines, private clouds are to be used by agencies and departments for internal sensitive data. Public clouds, meanwhile, will be used to deliver public-facing services.

There has already been a range of successful proofs-of-concept of cloud computing undertaken by Australian government agencies

The recommendations reflect the high dependency government departments and agencies have on IT to support their day-to-day activities. Through review processes such as that undertaken by the Government 2.0 taskforce, it is anticipated that opportunities offered by cloud computing will be identified and achieved.

There has already been a range of successful proofs-of-concept of cloud computing undertaken by Australian government agencies. These include:[8]

- **The Australian Taxation Office:** The successful eTax, Electronic Lodgement System (ELS) and Tax Agent Board administrative support systems are all supported by cloud-based services;
- **The Australian Bureau of Statistics:** Implementation of virtualisation software as part of a transition to a private cloud infrastructure;

INTRODUCTION

- **Treasury:** Standard Business Reporting (SBR) and Business Names projects have made use of private cloud capabilities;
- **Dept of Immigration and Citizenship:** Adoption of a cloud computing proof-of-concept to investigate provision of an end-to-end online client lodgement process.

It is clear cloud computing has significant benefits to offer both public-sector and private organisations

It is clear cloud computing has significant benefits to offer both public-sector and private organisations. Through careful planning and staged adoption, the introduction of cloud-based platforms and services can do much to meet future challenges faced by Australia while building on initiatives already underway.

WHY CLOUD COMPUTING?

When interest in cloud computing first began growing earlier this decade, it was fuelled by the promise of significant financial and productivity benefits. Rather than being weighed down by complex and expensive internal IT infrastructures, the cloud offered a more flexible and responsive alternative.

As organisations have taken their first steps down the cloud computing path, many are finding those promises to be accurate. By unshackling themselves from existing hardware and software systems, they are better able to meet the demands of both internal users and external customers.

A shift in expenditure

For public-sector organisations, the most enticing prospect offered by cloud computing is the ability it brings to change the way money is spent on IT systems

For public-sector organisations, the most enticing prospect offered by cloud computing is the ability it brings to change the way money is spent on IT systems. Rather than needing to invest in servers, networking equipment, storage resources and software, organisations can shift to a utility-based model. As a result, funds can be allocated to more customer-facing and service activities.

The impact on expenditure can be profound. Rather than requiring a significant upfront capex investment, expenditure becomes opex. No longer does IT equipment need to be depreciated over time. Instead, it becomes a pay-as-you go resource, freeing up business capital for other purposes.

Further financial benefits become clear when associated costs are also considered. When computing systems are moved from in-house facilities to a third-party cloud provider, there can be a reduction in energy consumption and accompanying electricity charges. Also, the removal of systems can result in reduced demand for systems management and maintenance staff, leading to further cost savings. Potentially, cloud computing can deliver significant reductions in the total cost of ownership (TCO) of IT over a five-year period.

Close collaboration will be needed between CIOs and CFOs to smooth the transition from what traditionally have been large capex investments to what will now be long-term opex spending

Gaining such benefits, however, will require a change in the traditional funding models used by many public sector agencies. Close collaboration will be needed between CIOs and CFOs to smooth the transition from what traditionally have been large capex investments to what will now be long-term opex spending. This challenge is not likely to be encountered, however, in green field projects and this is where opportunities to make use of cloud platforms should be seized.

Improved productivity and agility

As well as reducing costs, moving existing IT systems to cloud-based platforms can also deliver a significant boost to organisational agility and productivity. Rather than focusing time and money on establishing and managing IT, this effort can be redirected to supporting core business activities. The result is a more efficient and productive organisation.[9]

A recent Gartner survey of CIOs in the Asian region found cloud computing ranked as their number one technology priority.

"CIO technology priorities reflect a transformation in infrastructure, and the 'cloud' is dominating CIO plans and attention," said Terick Chiu, executive partner, Gartner Executive Programs.[10]

For public-sector bodies, the improved agility offered by cloud assists in meeting the recommendations put forward by the Government 2.0 taskforce.[11] More funding can be allocated to public-facing activities rather than being needed to keep back-end IT systems functioning.

As public demands evolve over time, cloud-based systems are also better placed to meet changes as they occur. Where once alterations to services and activities would have required significant re-architecting of the underlying IT infrastructure, cloud computing streamlines and simplifies the process. As a result, government organisations may be better able to serve their customers and rapidly implement new policies to better serve the Australian public.

Changes in demand levels can also be more readily covered. Cloud-based systems offer the ability to 'dial up' and 'dial down' resources as demand for them changes. Rather than having to invest in sufficient IT infrastructure to cover peaks in demand, extra resources can be brought online only as they are required, further enhancing organisational agility.

Rather than having to invest in sufficient IT infrastructure to cover peaks in demand, extra resources can be brought online only as they are required, further enhancing organisational agility

Case study – Cloud services assisting the community

Telstra cloud services have helped Australian business and communities during times of natural disaster. In January 2011, Telstra together with Microsoft® and local partner Productiv, provided free and instant communications to businesses that had their email server damaged or destroyed by the Queensland floods.

Following the 2009 bushfires, Telstra worked with the Victorian Government to create a cloud-based emergency warning system that activates mass outbound calling to direct citizens in imminent danger to safer ground. Telstra's Emergency Warning System (EWS) is a government private cloud providing citizen centric services. The EWS enables emergency services organisations to send targeted communications to individuals in danger zones.

FACTORS TO CONSIDER WHEN MOVING TO THE CLOUD

While cloud computing may offer significant benefits to both enterprise and government organisations, there are a range of factors and perceptions that may lead to some hesitation in exploring this new method of IT service delivery.

For enterprises, an ongoing focus on cost reduction and productivity improvement means IT infrastructures must continue to function without disruption. For public sector organisations, the focus remains on a need to maintain service levels while ensuring sensitive data remains secure.

As with any new development in technology, there have been early adopters who have quickly embraced cloud computing and put it to work within their operations. For some, this has taken the form of shifting certain applications from in-house platforms onto a public cloud. For others, activity has centred on evolving existing internal IT systems into a private cloud infrastructure.

Meanwhile other organisations have maintained a watching brief, interested in the benefits but at the same time aware of some of the challenges that can also be faced. These challenges fall into three distinct categories: **operational, data sovereignty and privacy,** and **data security.**

Operational

Through its very nature, cloud computing requires a fundamental shift in the way an organisation's IT services are provisioned. Rather than running on dedicated, locally managed equipment, applications and data are shifted to an external (and often multi-tenanted) infrastructure.

For this reason there is sometimes the perception that application performance could be reduced. Concern is sometimes expressed that software designed to work on a dedicated, stand-alone platform will be degraded if moved to a shared environment. This concern stems from the fact that the majority of applications running within enterprise and government organisations were not specifically designed to run in a virtualised or shared (cloud) environment.

Existing networks must also be reviewed with cloud services in mind. Because applications and data will likely be housed in remote facilities, ensuring connectivity and performance is at required levels becomes critical

Existing networks must also be reviewed with cloud services in mind. Because applications and data will likely be housed in remote facilities, ensuring connectivity and performance is at required levels becomes critical.

Concern has also been expressed about the potential for disruption to services during the migration from existing platforms to the cloud. When applications and data are critical to the functioning of an organisation, any disruption - no matter how brief - can have a significant and detrimental effect.

FACTORS TO CONSIDER WHEN MOVING TO THE CLOUD

Hesitation to move to the cloud can also be caused by fears that the performance of software applications will be reduced due to network latency. Because there will be increased physical distance between users and the software and data they need, peaks in network traffic could translate into delays and performance issues.

Finally, concerns are also expressed about the potential for an organisation to be 'locked in' to a cloud provider, thereby limiting future choices. If critical systems are hosted on a platform provided by one supplier, there could be challenges associated with moving should that relationship come to an end.

Telstra's position

As Australia's largest telecommunications company, Telstra is well placed to address operational concerns. The company is making significant investments both in its network infrastructure and in data centres designed specifically to support cloud computing services.

Telstra's national Next IP® and Next G® networks feature inbuilt quality of service (QoS) and WAN (Wide Area Network) optimisation technology, which prioritises network traffic and reserves network capacity for applications to ensure they perform at their peak. As a result, customers can access their cloud-based applications and data in more places as required. Bandwidth can also be dynamically allocated, ensuring users remain connected and productive. The entire network is robust and sufficiently extensive to provide reliable service to users in urban and rural areas.

Telstra's range of cloud services have been designed with customer operational requirements top of mind:

* **Infrastructure as a Service (IaaS)** provides immediate access to our powerful, state-of-the-art data centres, shared or private servers and highly secure storage in our Australian data centres.

* **Software as a Service (SaaS)** provides the latest business software, unified communications, video and web conferencing which end users can access either in the office or remotely.

Telstra also provides experienced and dedicated account management teams that manage network and cloud services through a single point of contact and end-to-end Service Level Agreements .

The company also works closely with customers during cloud migration projects to ensure seamless transition to cloud services. In conjunction with Accenture and other strategic cloud alliance partners, Telstra reviews client requirements and works to develop a cloud solution designed to meet specific needs.

Having been involved in cloud computing since its inception, Telstra has developed a breadth of strategic relationships with key global technology companies. This gives access to the latest tools and techniques that can smooth migration projects and reduce the risk of interruption to critical services or application performance.

FACTORS TO CONSIDER WHEN MOVING TO THE CLOUD

Data sovereignty and privacy

At the very centre of cloud computing is the concept that software applications and data are unshackled from underlying hardware. As a result, they can be effectively hosted anywhere and shifted in response to changes in demand.

Yet it is this core underlying benefit that also causes a significant concern: data sovereignty. Where once an organisation could know definitively where its data was stored, in a cloud environment this is no longer the case. Cloud service providers can shift a client organisation's resources between servers within a data centre and even between data centres as required. Those data centres can potentially be located anywhere in the world.

This flexibility brings the issue of data sovereignty into sharp focus. Enterprise and government organisations have a fiduciary duty to protect data relating to their employees and clients. A concern is that this could be compromised if the geographic location of that data is not known.

According to Gartner, "Data sovereignty has emerged as the single biggest concern for clients outside the US that are looking at adopting public cloud computing"

Indeed, according to Gartner, "Data sovereignty has emerged as the single biggest concern for clients outside the US that are looking at adopting public cloud computing". [12]

"During the next five years, data sovereignty problems will diminish as more providers turn their attention to this issue. However, the problem will not completely disappear," says Gartner.

These concerns are also shared by some clients who believe there are risks associated with having their personal details stored outside Australia. If located offshore, they fear that data could be more susceptible to unauthorised access or harder to retrieve should a disaster occur.

There are also legal implications. If an organisation's data is stored offshore, it is likely to be subject to the laws of the country in which that storage facility is located.[13] This could lead to scenarios such as foreign government requests for access to stored information.

Such legal requests for stored information have already occurred, years before the concept of cloud computing had been devised.

In Australia, a case occurred in 1999 between the Malta-based Bank of Valetta and the National Crime Authority.[14] In that case the bank was required to produce records stored in Malta for use in an Australian court case.

Such cases serve to illustrate the issues that could be faced by organisations that choose to have data hosted offshore by a cloud services provider.

FACTORS TO CONSIDER WHEN MOVING TO THE CLOUD

The cloud also raises issues of privacy. When sensitive or identifiable customer data is shifted from in-house systems to an external provider, certain laws become relevant.

The cloud also raises issues of privacy. When sensitive or identifiable customer data is shifted from in-house systems to an external provider, certain laws become relevant

As part of the Commonwealth Privacy Act, overseen by the Office of the Australian Information Commissioner, there is a set of Information Privacy Principles (IPPs).[15] IPP 4 states that an agency in possession of personal information must ensure that records are protected "by such security safeguards as it is reasonable in the circumstances" to ensure they remain secure.

State governments also have relevant legislation that has an impact on the use of cloud services. For example, under the Information Privacy Act 2000 (Vic) organisations need to be careful if storing personal information about an identifiable individual in a public cloud.[16] Cloud providers should only be used if they adhere to the guidelines contained in the Act.

Additionally, in a paper released in April 2011, the Federal Government's Defence Signals Directorate (DSD) provided the following guidance to government agencies:

"DSD recommends against outsourcing information technology services and functions outside of Australia, unless agencies are dealing with data that is all publicly available. DSD strongly encourages agencies to choose either a locally owned vendor or foreign owned vendor that is located in Australia and stores, processes and manages sensitive data only within Australian borders. Note that foreign owned vendors operating in Australia may be subject to foreign laws such as a foreign government's lawful access to data held by the vendor." [17]

Telstra's position

Telstra is acutely aware of the issues surrounding data sovereignty as it relates to cloud computing environments. Having worked as a trusted provider of telecommunications and computing services for enterprise and government clients for decades, the company has in place rigorous frameworks to ensure customer data is protected.

Telstra's data management complies with Australian Laws, including Privacy legislation, providing customers reassurance that their sensitive company information is managed by Telstra in accordance with Australian laws.

Telstra is also aware of the issues raised by authorities such as the Victorian Privacy Commissioner, who released 'Info Sheet 03.11' in May 2011, focused on privacy considerations and cloud computing. Ensuring company and personal data is held securely is of fundamental importance to Telstra.

Because Telstra's telecommunications infrastructure and IT infrastructure are located on Australian shores, data stored with Telstra's Infrastructure as a Service (IaaS) Dedicated and Utility Hosting cloud services remains under Australian jurisdiction.

FACTORS TO CONSIDER WHEN MOVING TO THE CLOUD

Data security

Allied to concerns about data sovereignty are those that relate to security. Many organisations feel that moving important information into the cloud potentially makes it less secure and more exposed to threats and attacks.

Such fears are exacerbated by ongoing media reports of cyber and viral attacks aimed at extracting information for criminal activity. If data is no longer stored on physical, trusted devices within an organisation, some remain concerned that proper levels of protection may no longer be put in place.

For public-sector organisations, such concerns are particularly acute. Successful attacks could result in the theft of personal data or significant disruption to critical government services. They could also result in a loss of trust and an ensuing reluctance (eg for tax payers) to 'trust' government with information.

As such, these concerns can then lead to reluctance on the part of public-sector organisations to embrace cloud services and a tendency to remain with existing, in-house infrastructures.

Such concerns can be addressed by thoroughly assessing cloud service providers before any service agreements are entered into. Careful examination of everything from physical security of data centres and disaster recovery capabilities, to the software tools in place to prevent unauthorised access, should be carried out as a matter of course.

According to Gartner, "Enterprises using cloud service providers need to make the security level of the cloud provider a key evaluation criterion during selection and continue to monitor security service levels during use".

According to Gartner, "Enterprises using cloud service providers need to make the security level of the cloud provider a key evaluation criterion during selection and continue to monitor security service levels during use"

"High-security service providers are not always the most expensive choice, but paying more upfront for strong security can save money in the long term."[18]

It is only through rigorous assessment of potential weaknesses and the accompanying safeguards that concerns over data security be remediated.

FACTORS TO CONSIDER WHEN MOVING TO THE CLOUD

Telstra's position

Telstra has a long-term track record of working with enterprise and government agency clients. Through a thorough understanding of the types of data used and stored by these organisations, Telstra has developed a comprehensive approach to security issues.

With years of experience in managing network security for critical industry sectors including Australia's largest banks, and agencies such as the Australian Federal Police and the Department of Defence, Telstra is an industry leader in security.

Telstra is one of only a few organisations that has selected products and associated security processes certified to ISO27001 Security Management Standard and the AS/NZS 31000:2009 Risk Management Standard. Additionally, data security is a critical part of Telstra's own business, because the company's own customer database is one of the largest privately held databases in the country.

Telstra also maintains a 400-strong information security team that has built and oversees the robust security features at the core of Telstra's cloud services. These features include network-based firewalls, Managed Internet Gateway, Internet Protection, Denial of Service Protection, remote access security, disaster recovery and backup/restore capability. Telstra also maintains separate internet and private IP networks, which provides the ability to isolate and contain Distributed Denial of Service Attacks.

The security of Telstra's cloud computing platforms is the responsibility of the Telstra Security Operations Centre (TSOC). This ASIO T4-accredited facility provides a 24/7 monitoring and security incident response capability. It also provides government accredited Information Security Manual (ISM) compliant products to deliver secure services to enterprise and government clients.

TELSTRA CONNECTED GOVERNMENT CLOUD

As part of its comprehensive Connected Government Cloud portfolio, Telstra offers a range of cloud services. Delivered through a number of strategic partnerships, including those with Accenture®, Cisco® and Microsoft®, the cloud services are built upon the national Telstra Next IP® network and Next G® networks and use the company's growing network of data centres.

As part of its comprehensive Connected Government Cloud portfolio, Telstra offers a range of cloud services

Telstra's cloud services are also available under flexible payment models, including monthly subscription and pay-as-you-go. This allows for a shift from opex to capex expenditure and reduction in total cost of ownership (TCO).

Telstra Connected Government Cloud offerings include:

Infrastructure as a Service (IaaS)

Telstra's IaaS offering provides government agencies with access to the computing power they require, when they need it, delivered over a secure private network. The offer encompasses a range of different computing models, operating system platforms, suite of cloud protection services and data storage options.

Existing internal IT infrastructures can be augmented by making use of external Telstra computing capacity. Tiered storage options are available as are mail, web and data security tools and processes.

Telstra's Canberra data centre currently provides co-location and secure gateway services. Customers also have the option of locating their own servers within a secure, state-of-the-art Telstra data centre with 24/7 expert monitoring and maintenance

This managed, secure on-demand infrastructure can be provided from shared public servers or dedicated T-4 compliant private facilities in Canberra. Telstra's Canberra data centre currently provides co-location and secure gateway services. Customers also have the option of locating their own servers within a secure, state-of-the-art Telstra data centre with 24/7 expert monitoring and maintenance.

In the second half of 2011 Telstra's cloud computing infrastructure was certified by software companies SAP and Red Hat. This provides customers with the confidence that their critical applications will be fully supported by Telstra's cloud platforms. Telstra's cloud platforms also support all major operating systems. This means customers do not need to port applications, thus reducing migration times and associated costs.

Specifically, Telstra's IaaS offering includes:

Dedicated Hosting: Provides a highly secure server platform for a client's exclusive use. This can be expanded as demands for capacity increase.

Utility Hosting: Provides customers with immediate access to shared storage and processing capacity, hosted within Telstra's dedicated cloud data centres.

TELSTRA CONNECTED GOVERNMENT CLOUD

Software as a Service (SaaS)

Telstra's SaaS offering provides government and enterprise customers with access to a range of fully managed business applications

Telstra's SaaS offering provides government and enterprise customers with access to a range of fully-managed business applications. The software is hosted in a secure data centre and accessed remotely over secure private networks.

Business productivity applications on offer include hosted email, secure online portals, instant messaging and telepresence. Specific applications include Microsoft® Office 365, Microsoft® Exchange Online, Microsoft ®Lync Online and Microsoft® SharePoint Online.

For the public sector, Telstra is working on a tailored Government Cloud SaaS offering in conjunction with strategic partner Microsoft®. The intent is to provide state and federal government agencies with access to a range of cloud-based collaboration and productivity tools hosted within Telstra's Australian data centre network.

Communications products include Cisco WebEx®, Cisco and Polycom telepresence and Telstra IP Telephony (TIPT). Customer service applications include contact centres using Telstra's Web Contact Centre.

Professional Services

In conjunction with... Accenture, Telstra has developed a series of proven assessment and deployment methodologies which...allow customer organisations to seamlessly migrate to the cloud over time

As migration from existing in-house IT infrastructure to a cloud platform can be a complex and challenging task, Telstra provides a portfolio of professional services to assist.

In conjunction with global management and consulting firm Accenture, Telstra has developed a series of proven assessment and deployment methodologies which can smooth migration and integration projects and ensure their success. The methodologies allow customer organisations to seamlessly migrate to the cloud over time.

Working together, Telstra and Accenture can provide valuable insight into how the cloud can best be used to deliver value to a customer's unique circumstances.

Cloud Trials

To support gradual adoption of cloud services and deployments, Telstra offers the ability for government agencies and enterprise organisations to trial cloud-based services. This trial option can help government agencies assess the most promising opportunities, then test them thoroughly in a real cloud environment.

CONCLUSION

Cloud computing has the potential to revolutionise the delivery of information technology services to Australian enterprise and government organisations. Through the use of private, public and hybrid cloud infrastructures, costs may be reduced, efficiency gains may be realised and productivity improved.

For public sector organisations, benefits associated with the adoption of cloud services can be profound. Capital expenditure on IT equipment may be significantly reduced, while the ability to quickly match resources with demand enhanced

For public sector organisations, benefits associated with the adoption of cloud services can be profound. Capital expenditure on IT equipment may be significantly reduced, while the ability to quickly match resources with demand enhanced.

Where it would have taken months, or even years, for agencies to put in place the infrastructure required to support a new initiative, such support can be delivered in just weeks or months.

Applying cloud technologies across government can yield tremendous benefits in efficiency, agility, and innovation. According to the former US Government CIO, Vivek Kundra:

"Cloud computing has the potential to play a major part in addressing these inefficiencies and improving government service delivery. The cloud computing model can significantly help agencies grappling with the need to provide highly reliable, innovative services quickly despite resource constraints."[19]

At the same time, organisations need to be aware of the issues that must be considered before adoption of cloud services is contemplated. These include restrictions around data privacy and sovereignty as well as operational constraints.

Proper assessment of these issues is vital to the success of every cloud-related initiative. A thorough understanding of objectives and assessment of potential cloud service partners is essential.

Telstra Connected Government Cloud provides a secure, robust, agile and scalable platform on which government and enterprise organisations can build computing capabilities that will provide real business advantage and assist them in better serving their clients.

Australian Government Agencies requiring further information on this document can contact **Alex Stefan, National General Manager Government and Public Safety and Security:** alex.stefan@team.telstra.com.

The latest version of this document is available at www.telstra.com/cloud and www.telstra.com/government

REFERENCES

1 IDC: Australian Cloud Services 2011-2015 (Special Report Release – Australian Cloud Research)

2 Federal Cloud Computing Strategy, February 8, 2011, p.5

3 IDC Asia Pacific Cloud Computing Survey 2011

4 IDC Insight – The Evolving Maturing of Cloud in Australia

5 *Federal Cloud Computing Strategy,* February 8, 2011, p.1

6 Ibid

7 *Cloud Computing Strategic Direction Paper: Opportunities and applicability for use by the Australian Government, Version 1.0.*

8 Ibid

9 2011 Gartner Executive Programs CIO Agenda Survey

10 Gartner press release: Gartner Survey of CIOs in Asia shows Cloud Computing Tops the Technology Priority List as Businesses Focus on Growth in 2011: June 22, 2011

11 http://www.finance.gov.au/publications/govresponse20report/index.html

12 Gartner "Data Sovereignty Can Be a Hurdle for the Adoption of Cloud Computing": Brian Prentice, published 11 July, 2011

13 Dept of Defence Intelligence and Security – Cloud Computing Security Considerations, 12 April 2011

14 http://www.austlii.edu.au/au/cases/cth/FCA/1999/1099.html 15http://www.privacy.gov.au/law/act/ip

15 http://www.privacy.gov.au/law/act/ipp

16 Privacy Victoria – Info Sheet 03.11, May 2011

17 DSD, *Cloud Computing Security Considerations,* 12 April, 2011

18 Gartner research - ID number G00216359: Critical Security Questions to Ask a Cloud Service Provider, pub Sept 7, 2011

19 *Federal Cloud Computing Strategy,* February 8, 2011, p.1

Why Telstra?

Telstra provides network services and solutions to more than 200 of the world's top 500 companies. They rely on us to do business across 240 countries and territories and to enable greater productivity, efficiency and growth.

Telstra solutions offer the best of all worlds – skilled people and a rich portfolio of services delivered on our world-class Telstra Next IP® network and Next G® network. To ensure reliable performance, they're monitored and maintained from our dedicated centres using advanced management and operational systems. And they're backed by Telstra Enterprise-grade Customer Service® and one of Australia's largest and most qualified field and technical workforce.

FOR MORE INFORMATION
PLEASE CONTACT YOUR
TELSTRA ACCOUNT EXECUTIVE
VISIT **TELSTRA.COM/GOVERNMENT**
CALL **1300 TELSTRA**

NEXT G® NETWORK | NEXT IP® NETWORK | NEXT GENERATION SERVICES®