Deloitte.

AWS

2019

Harnessing public cloud opportunities in the government sector

AWS

2019

Deloitte
Access **Economics**

Contents

Executive summary

Change and uncertainty have always been a part of the economy and the government landscape. But the pace of change is increasing, and uncertainty is at new highs. The government sector is facing the challenge of growth in service expectations and its costs of delivery, amid constrained resources and declining public trust. This makes the case for a new approach to government service delivery, and is aligned with a desire within the sector to embrace new opportunities.

Digital technology has the potential to support government in meeting the needs of its citizens and policies are focused on increasing its use over time. The Federal Government's Digital Transformation Agency released a new strategy in November 2018 with a vision for Australia as one of the top three digital governments in the world by 2025.

Public cloud, a digital services platform, can enhance government operations and support it in overcoming the challenges it faces in an increasingly complicated environment. Public cloud offers on-demand delivery of computing power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing.

Deloitte Access Economics' research into government sector use of public cloud includes analysis of the sector's performance relative to its policy aspirations, a new survey of federal and state government sector decision makers, and case studies with agencies that have successfully made a move to using public cloud.

The benefits of public cloud are well recognised. Government sector decision makers identified the **main benefits as being improved agility in terms of being able to better scale operations as needed**, such as during times of peak demand for agency services or applications, **improved productivity**, for example, achieved through time savings in analysing data or in streamlining processes, **and improved services, reliability and data security** (see Chart i). Further, public cloud is a platform for the future, providing a foundation for a range of emerging technologies ranging from artificial intelligence to virtual reality.

The cumulative productivity benefits of public cloud to the government sector could already be over $2 billion over the last 5 years.

Chart i: Main benefits of cloud experienced by agencies surveyed
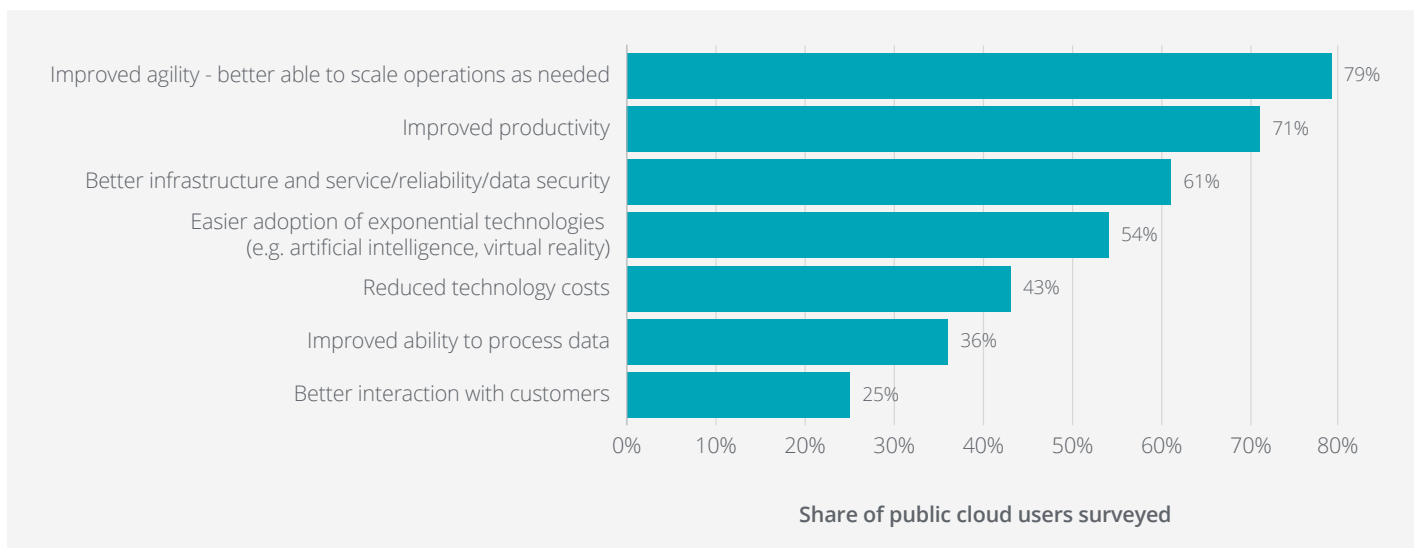
Source: Deloitte Access Economics, 2019

The Federal Government, states and territories have existing cloud policies or strategies. The government sector has performed relatively well in terms of use of public cloud. For example:

- When compared with business use of public cloud, **government sector expenditure is proportional to its share of the Australian economy** (24%) (ABS, 2018).

- Compared with international counterparts, **the Australian government sector's posture towards using cloud for net new IT services is ahead of international comparators**; being more likely to consider cloud among available options, while internationally, decisions are more likely to be made on a case by case basis (IDC, 2018b).

- **However, government sector uses of public cloud tend not to be sophisticated,** with data storage and production/service operations being the most reported use of public cloud (82% and 68% of survey respondents respectively), indicating scope to use public cloud for more advanced applications such as machine learning in the future.

The government sector is a significant user of public cloud, spending almost $1 billion on public cloud in 2018 (IDC, 2018a). This is around 23% of total public cloud spending in Australia (IDC, 2018a), and the **cumulative productivity benefits of public cloud to the government sector could already be over $2 billion over the last 5 years**.

There is significant potential for this value to be even greater over time as take up increases, and acknowledging that traditional measures of productivity are not as applicable to the government sector, where measuring the value of 'service' is not as straightforward as measuring businesses' inputs and outputs via costs and revenues.
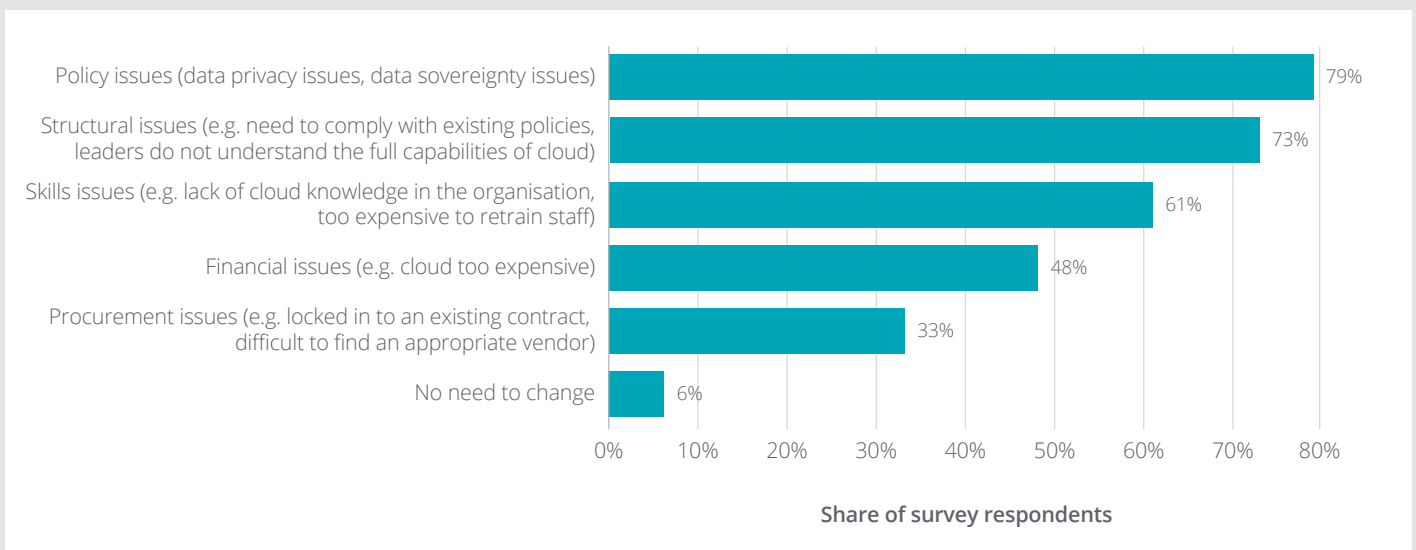
There is potential for government sector use of public cloud to grow; Deloitte Access Economics' survey of government sector decision makers has found that, on average, public cloud accounts for only one quarter of an agency's IT structure. A move towards a more flexible and adaptable operating environment through use of public cloud will support government sector productivity and its delivery of citizen-centric services.

As shown in Chart ii, the **most reported barriers to adopting or expanding the use of public cloud were policy related – namely data privacy concerns and data sovereignty concerns,** cited by 79% of respondents. However, the Australian Cyber Security Centre (ACSC) Protected Certification now granted to a range of public cloud providers enables greater certainty around the security of certified entities, meaning that data can now be stored and processed at the protected security classification level, which overcomes this barrier to public cloud use.

While some agencies have started the move to public cloud, it was noted that leaders do not understand the full capabilities that cloud offers, that is, understanding the cases for public cloud beyond data storage to more advanced uses such as machine learning and the internet of things.

A common theme discovered through both consultations and the survey of government sector decision makers is that **insufficient knowledge of, or understanding about, using public cloud is holding agencies back**. In fact, 73% of agencies reported that leaders do not understand the extent of capabilities that public cloud offers. Even when they do, agencies are lacking the skills to use cloud. Almost two-thirds cite skills issues as a key barrier to using public cloud (see Chart ii).

Chart ii: Barriers of adopting or expanding use of public cloud by government agencies

Barrier	Share
Policy issues (data privacy issues, data sovereignty issues)	79%
Structural issues (e.g. need to comply with existing policies, leaders do not understand the full capabilities of cloud)	73%
Skills issues (e.g. lack of cloud knowledge in the organisation, too expensive to retrain staff)	61%
Financial issues (e.g. cloud too expensive)	48%
Procurement issues (e.g. locked in to an existing contract, difficult to find an appropriate vendor)	33%
No need to change	6%

Share of survey respondents

Source: Deloitte Access Economics, 2019

3

There is a perception in the government sector that government data centres or 'government cloud' is the same as public cloud. It should be acknowledged that government cloud can be a good first resource consolidation step, but in order to unlock the full benefits of technology and cost savings over time, the government sector is now on the verge of needing to make the next step to public cloud.

The lack of **provision for additional operational expenditure in place of capital expenditure in an agency's budget was also identified as a challenge in adopting cloud**. These barriers are similar to those experienced by the private sector, namely inadequate skills, legacy systems and costs of adoption.

But overall, surveyed **government sector leaders are overwhelmingly in support of greater cloud take up**; 94% of government sector leaders agree that procurement processes should be modernised and that government should invest in upskilling its workforce to be better prepared for public cloud.

Based on five case studies of successful transitions to public cloud, Deloitte Access Economics has identified the **six key considerations for success** below. There is a clear need to increase education around public cloud to help address the understanding of its use, capabilities and how to successfully make the transition. This will also help to manage concerns around real or perceived risks to using public cloud, and will assist in the organisational change required around finances and overcoming decision inertia.

94% of government sector leaders agree that procurement processes should be modernised and that government should invest in upskilling its workforce.

To support a successful transition to public cloud, government sector considerations should include:

Finding the right opportunity

Prepare for a move to public cloud – while contracts renewals are an opportunity to consider future use of public cloud, prior preparation may enable an earlier or smoother transition.

Managing risks

Public cloud has been used successfully in high profile and sensitive situations such as by the Australian Bureau of Statistics for the Australian Marriage Law Survey, and the Australian Taxation Office for logging tax returns. A considered risk management approach is required to mitigate the residual risks of running sensitive workloads in public cloud. There is a need to understand data rules in an agency's jurisdiction and the management of preventable, strategic and external risks to the agency.

Financial considerations

There is a need to consider the implications of a move to a consumption based pricing model and a need to educate the relevant staff managing these changes to government sector budgets.

Upskilling staff

An understanding of the organisational staff capability, skills gaps and the change management is required.

Governance

Agency leadership is critical for driving change. There is a need to align skills and processes to IT strategy and the agency's operating strategy.

Supporting others

The transition to cloud can be harder for larger agencies and those with more complex legacy systems. Agencies can learn from success in other agencies, and lessons and skills learnt can be shared across the government sector.
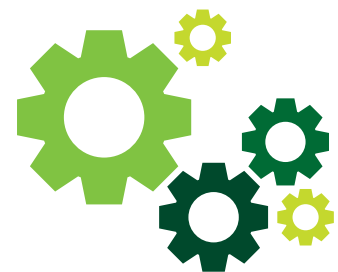
The following **recommendations for action** are intended to guide public sector leaders and provide concrete steps that could be implemented to encourage greater use of cloud, and ensure technology can leverage and help drive better agency and citizen outcomes.

- Central/whole of government policies to be established and implemented, setting a timeframe for the majority of systems to be in the public cloud by 2025.

- Government sector leaders to bring forward approaches to shift capital budgets to operating budgets in fiscally sustainable ways.

- Review and implement government policies for operating in the public cloud, especially around risk sharing arrangements.

- Government sector to prepare for public cloud by considering its existing and required skills.

- Use cloud as a platform for greater change in a more outcomes-focused and data-driven decision making environment, leveraging this for better agency and citizen outcomes.
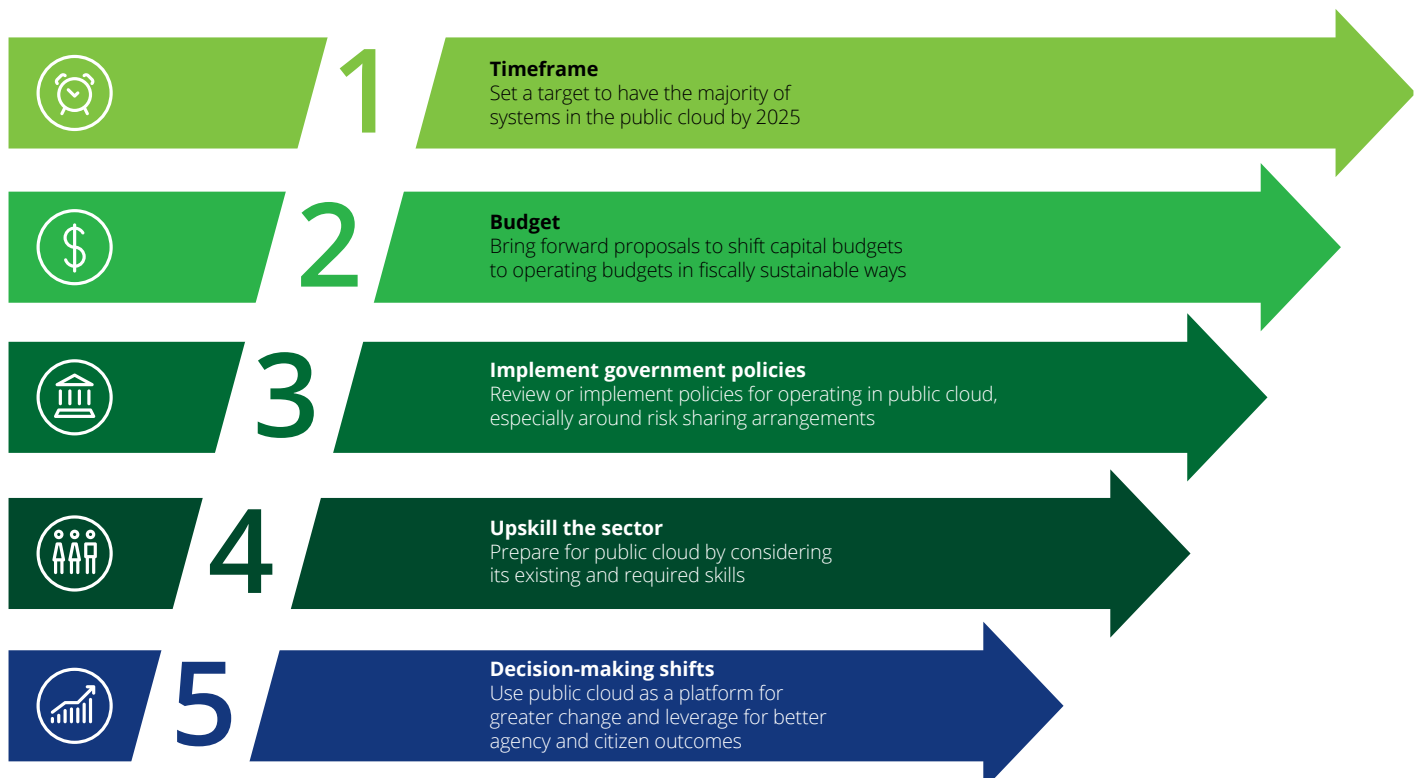
What is public cloud?

Public cloud computing is the on-demand delivery of compute power, database storage, applications and other IT services through a cloud services platform via the internet with pay-as-you-go pricing. Services include:

– **Software as a Service (SaaS)**
Applications that run on cloud infrastructure, such as client relationship management systems or communications mediums.

– **Platform as a Service (PaaS)**
The programming languages, libraries, services, and development tools the applications are built on that exist on cloud.

– **Infrastructure as a Service (IaaS)**
Processing, storage, networks, and computing resources that are provided on-demand from cloud.

– **Business Process as a Service (BPaaS)**
Uses cloud tools to outsource processes like payroll or supply chain planning to specialist vendor or advisor teams.

A public cloud provider owns and maintains the network connected hardware required for services, while users provision and use what they need via a web application.

This differs from the government's exclusive private cloud, where services and infrastructure are maintained on a private network and dedicated to government sector use.
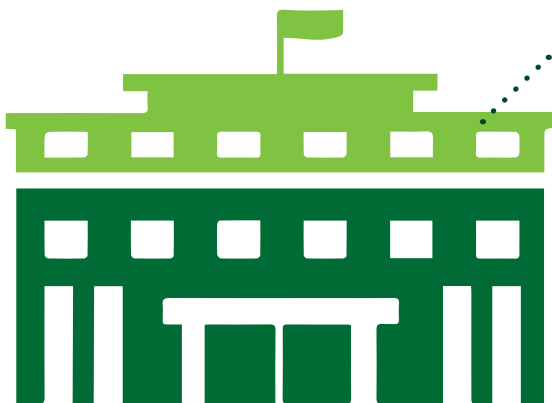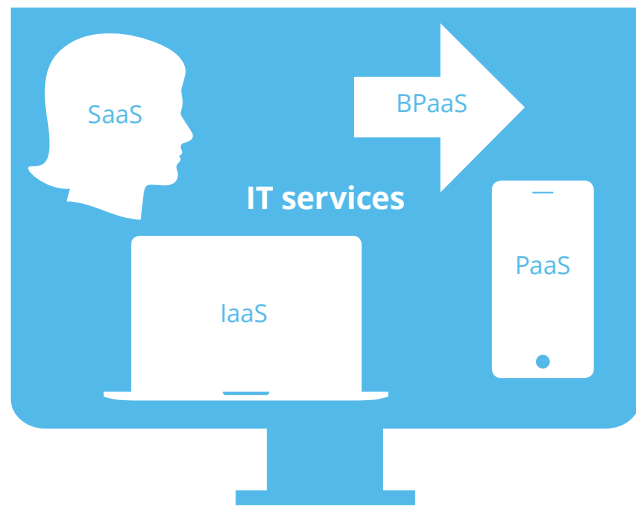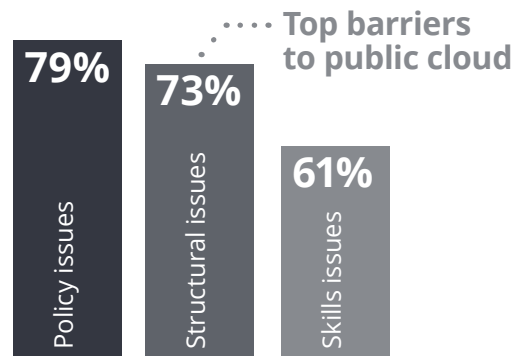
1
Timeframe
Set a target to have the majority of systems in the public cloud by 2025

2
Budget
Bring forward proposals to shift capital budgets to operating budgets in fiscally sustainable ways

3
Implement government policies
Review or implement policies for operating in public cloud, especially around risk sharing arrangements

4
Upskill the sector
Prepare for public cloud by considering its existing and required skills

5
Decision-making shifts
Use public cloud as a platform for greater change and leverage for better agency and citizen outcomes

Public cloud

Government sector use of public cloud

23%, almost $1 billion[1] of Australian public cloud spending comes from the government sector

Network ●

Compute ●

Storage ●

Database ●

Governance ●

Security ●

Analytics ●

Machine Learning ●

Internet of Things ●

SaaS

BPaaS

IT services

PaaS

IaaS

Only **24%** of the average government agency's IT structures are in the public cloud

79% Policy issues

73% Structural issues

Top barriers to public cloud

61% Skills issues

1. IDC (2018a)

1 The future of government and role of cloud

Change and uncertainty have always been a part of the economy and the government landscape. From the geopolitical environment of the cold war, to deregulation and public sector change in the 1980s and 1990s, through to internationalisation and the growth of trade and finance.

But the pace of change is increasing, and uncertainty is at new highs. For example, while population growth has supported the growth of the size of the labour force, automation has resulted in the rare occurrence of total employment levels declining in occupations that are highly susceptible to automation. Countering this, there has been significant job growth in occupations where technology is less likely to replace workers (Edmonds & Bradley, 2015).

The Commonwealth Science and Industrial Research Organisation (CSIRO) (2016) has modelled four possible future scenarios with wide ranging potential impacts for the country (see Chart 1.1).

Change in the government sector has not been limited to changes in regulations and privatisation, rather, a more fundamental shift in focus has occurred. Technology has enabled the rise of business models tailored to consumer preferences, and government likewise has shifted to being more citizen-centric.
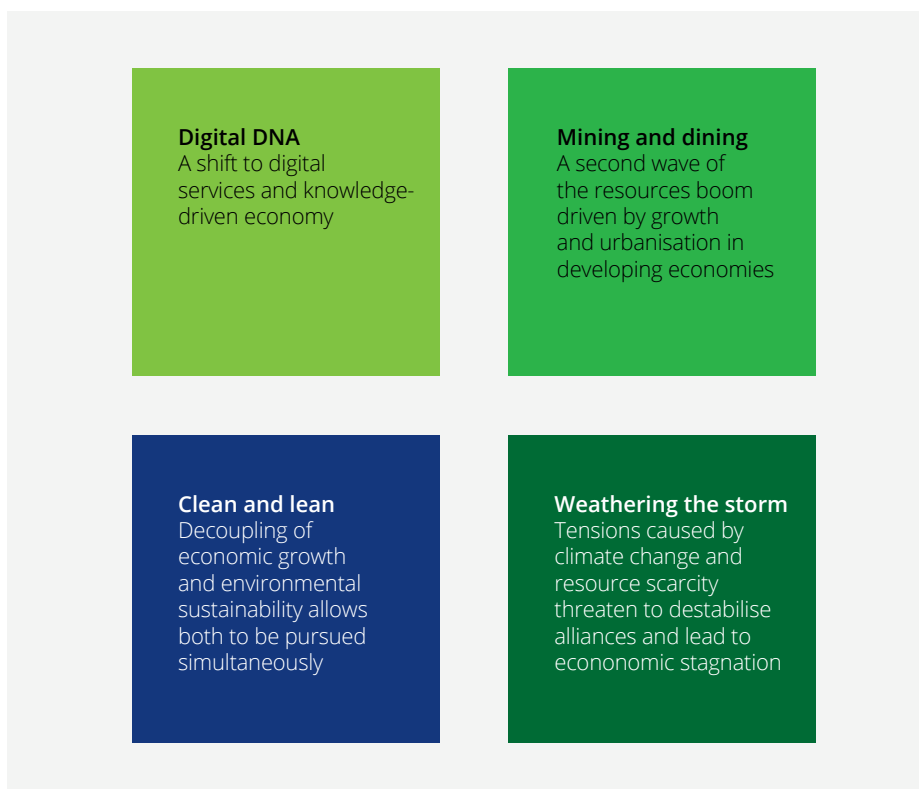
About this research

Deloitte Access Economics has been engaged by AWS to conduct research into government sector use of public cloud. The benefits to cloud are widely discussed, so the focus of this study is to identify the barriers to cloud, and develop recommendations on how to drive better take up in the future.

This report is based on a survey of 33 federal and state government sector decision makers around Australia who were responsible for or were familiar with the cloud strategy in their departments or agencies. The survey included perspective from agencies both currently using public cloud and those that had not yet started their public cloud journey.

This report is structured as follows:

• **Chapter 2** briefly outlines some of the benefits associated with use of public cloud

• **Chapter 3** explores current use of public cloud in the context of government policies and compared with international experience

• **Chapter 4** discusses the barriers identified to cloud take up

• **Chapter 5** provides guidance on the transition to public cloud, through a series of case studies

• **Chapter 6** presents recommendations for the government sector to support increased take-up and use of public cloud.

Chart 1.1 Australia in 2030 – four possible futures

Digital DNA
A shift to digital services and knowledge-driven economy

Mining and dining
A second wave of the resources boom driven by growth and urbanisation in developing economies

Clean and lean
Decoupling of economic growth and environmental sustainability allows both to be pursued simultaneously

Weathering the storm
Tensions caused by climate change and resource scarcity threaten to destabilise alliances and lead to econonomic stagnation

Source: CSIRO, 2016

In this uncertain environment, the role for government is changing. Government will need to help people to transition to new jobs as automation and economic change disrupts existing careers, it will need to find ways to keep energy costs down as the natural environment continues to change, and it will need to help upskill people to use digital tools as they become an increasingly important part of life.

This is a difficult task, and people are expecting more of government than they have in the past. There is a demand for more and better services, for instance the National Disability Insurance Scheme now provides personalised care for disabled people. Increasingly crowded cities means more demand for better public transport options. There is also demand for greater government investment in education and health.

Government resources are not matching the growth in expectations; the costs of delivery are increasing, and population ageing is shifting the taxpayer base. The Australian public service has shrunk to employing just over 150,000 people – the lowest it has been since 2006 (Australian Public Service Commission, 2018). While in 2007 there was one public servant for every 133 Australians, there is now just one per 165 (Mannheim, 2018).

At the same time, citizen trust in government is declining. Less than half (42%) of Australians now say they trust the government to do what is right, compared to 52% who say they trust business, and 56% who trust the United Nations (Edelman, 2019). Since the destabilisation of the Rudd/Gillard Government and ensuing uncertainty over political leadership, social cohesion in Australia has declined 11% (Scanlon Foundation, 2018). This environment presents challenges for government in achieving positive change.

The benefits of digital are substantial, and the government is focused on increasing use.

1.1 The role of digital

Digital technology has also had major impacts on the government sector in recent years. On one hand, technology has supported an increase in efficiency and enabled online services, from online form applications to licence renewals. On the other hand, there have been some high profile issues, such as the 'robo-debt' recovery program and the problems experienced during the introduction of the myki system for public transport in Victoria.

But the benefits of digital are substantial, and the government is focused on increasing its use over time. For example, Digital Transformation Agency works with agencies across government to improve digital services and ultimately people's experience of these government services. In November 2018, the Digital Transformation Agency released Australia's Digital Transformation Strategy with a vision for Australia as one of the top three digital governments in the world by 2025. The Federal Government, states and territories have existing cloud policies or strategies.

Public cloud in particular can be a valuable tool in meeting this goal and assisting government in overcoming the challenges it faces in an increasingly complicated environment. Public cloud offers on-demand delivery of computing power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing.

This enables a range of innovative services across the government sector, for instance, the Australian Taxation Office has developed a platform that allows taxpayers to submit their taxes online, making the process more simple and less time consuming both for individuals and the government. Similarly, the NSW Government has built a one-stop shop for all citizens to access government services. Service NSW (a whole of New South Wales Government Service access point that provides online, and in-person offices that handle more than 800 types of transactions) is able to help people with all their dealings with government, from obtaining licences and permits, to registering births or paying fines.

The opportunities that public cloud can offer are significant, and increasing, as cloud offerings evolve. In 2016, Deloitte's 'Gov2020' paper theorised that by 2020, federal and state governments would be using cloud computing for a significant portion of its functions. This would enable large-scale shifts in government, such as:

- Mobile services – government would make almost all services mobile, so people could remotely access services rather than going in-person to get a permit (for example).

- Data-smart government – government would be using predictive modelling to influence behaviour; for instance, analytics of utility usage can be used to show consumers' usage compared with their neighbours, influencing lower consumption over time.

- Funding shake-ups – more of government's systems would be dynamic or pay-as-you-go systems meaning a reduction in costs.

- Flexible staffing – a significant portion of government staff would be tied to projects rather than departments, and move to where they are needed, meaning a more agile workforce.

However, despite cloud first policies, government sector take up of public cloud could be more extensive, meaning that many of these benefits are still waiting to be realised.

2 Benefits of public cloud

Public cloud can bring big benefits for agencies in the government sector. From improved productivity and reduced costs, to providing a platform for innovation and access to exponential technologies, public cloud has the potential to change the way that government operates and interacts with the people it serves.

This chapter outlines these benefits, and the experience of these benefits by the Australian government sector.
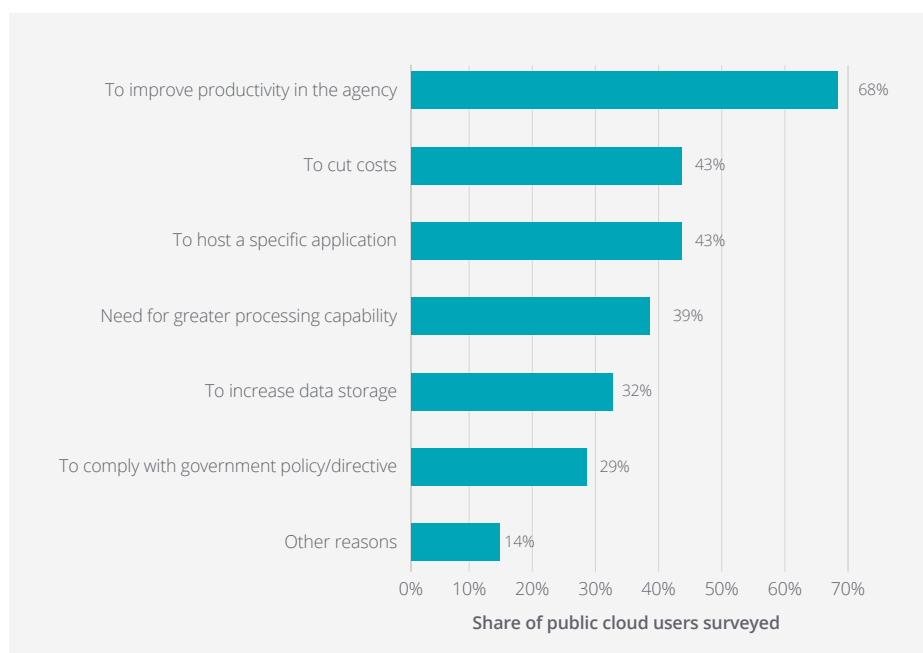
2.1 Public cloud decision making

The survey of government sector decision makers found that the most common driver of adopting public cloud use was to improve productivity (cited by two-thirds of respondents, as shown in Chart 2.1). For 43% of agencies, cost cutting was a driver to moving to cloud and another 43% noted a move to cloud to host a specific application.

Over time, the transition to cloud could also see the government sector going beyond basic uses of cloud to hosting bespoke applications, enterprise resource planning, or enabling next-wave technologies.

CSIRO has started using next-wave technologies in its research. Using public cloud, CSIRO has developed a custom machine learning library to uncover information in the millions of dimensions from genomic data. These vast clinical datasets filter data in real-time to identify medically similar patient cohorts, and compare their genomes to search for causative changes.[2]

These advanced uses of cloud will become ever more vital in enabling business digital transformation and meeting the evolving needs of citizens. Agencies are increasingly facing the challenge of providing services that can scale efficiently, are cost-effective and are ever more reliable. Public cloud will have a significant role to play in enabling

Chart 2.1 Why did your agency begin using public cloud?

Share of public cloud users surveyed

To improve productivity in the agency	68%
To cut costs	43%
To host a specific application	43%
Need for greater processing capability	39%
To increase data storage	32%
To comply with government policy/directive	29%
Other reasons	14%

Source: Deloitte Access Economics, 2019

the government sector to keep up with these trends.

Yet, given that some jurisdictions have 'cloud first' policies, it is surprising that only 30% of respondents stated that policy compliance influenced their initial take-up of public cloud. This indicates that drive for public cloud take up may have been led from the bottom up rather than the top down, and also demonstrates a clear understanding of public cloud's efficiency benefits, rather than agencies moving to cloud purely as a compliance measure.

2.2 Benefits of a move to public cloud

From specific, small innovations, to benefiting from the scale and elasticity of cloud, to whole organisational change, there are many gains that stem from integrating public cloud as part of an agency's IT structure.

As our survey results indicate, agencies that have already incorporated public cloud have experienced a range of key benefits (see Chart 2.2). The most commonly identified benefit, cited by 79% of respondents, was improved agility, where agencies could better scale operations up and down as required. Emergency Management Victoria (EMV) and the NSW Rural Fire Service, for example, require significant increases in computing power during emergencies. EMV uses public cloud to provide a mobile application that allows over 1 million Victorians to receive personalised information about developing incidents, and during large fire events, user views of NSW Fire Service sites and apps can increase from 6 million to 14.1 million within two weeks.[3]

---

2. AWS customer story
3. AWS customer story

Public cloud has also enabled improved productivity for 71% of respondents, which is explored further in the following section on economic benefits.

The third most identified benefit was improved services, reliability and data security, identified by 61% of respondents. For Geoscience Australia, the service availability of one of its 'mission critical' applications increased from 90% when hosted on-premises to 100% when using public cloud.[4] In a complex cybersecurity environment, public cloud can play an important role in supporting government sector operations. Public cloud operators are responsible for the security of their IT infrastructure and implement technical and physical measures to prevent unauthorised access to data, including 24/7 monitoring of IT assets and environments. Users can choose to encrypt highly sensitive content or use supported third party security solutions. Certified public cloud providers focus on the ongoing security of the cloud to mitigate against cybersecurity risks.

Further, public cloud is a platform for the future, providing a foundation for a range of emerging technologies ranging from artificial intelligence to virtual reality. Previous research by Gartner (2018) has found the key drivers of public cloud take up in the government sector are increased efficiency of service delivery and cost savings.

The survey findings reflect the positive experiences detailed in the case studies presented in Chapter 5, and also broadly align with the major technology drivers for businesses in adopting public cloud, namely cost savings, agility in accessing resources as required, and being able to instantly scale up and down. Importantly, the benefits of cloud are generally not coming at the expense of employment in the government sector. Only 18% of agencies reported a decrease in IT staff after the implementation of public cloud. For non-IT staff, 93% of agencies reported no change in employment levels (with the other 7% unsure if this had changed).

2.3 Economic benefits of government sector use of cloud

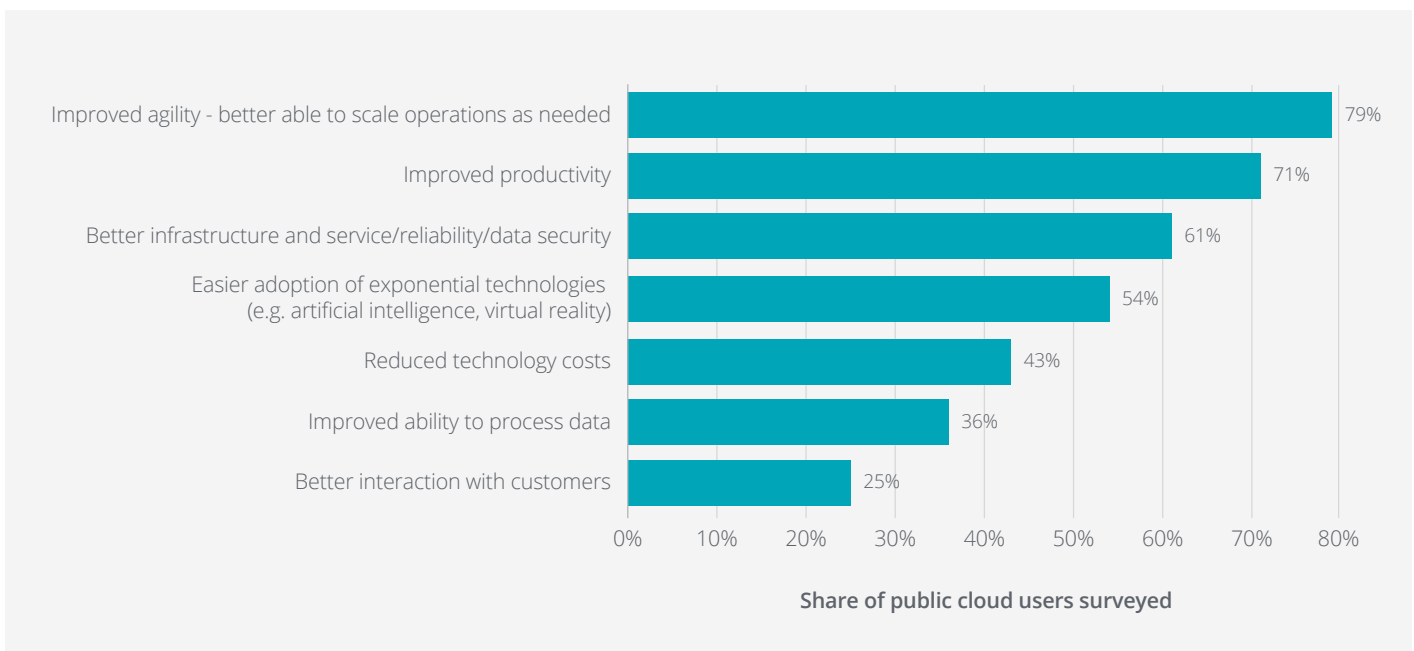Public cloud is transforming the whole Australian economy. As part of a larger research project, Deloitte Access Economics has estimated that over the last 5 years, public cloud has delivered cumulative productivity benefits of $9.4 billion despite less than one third of businesses using paid public cloud services.

There are a range of ways that agencies can experience productivity benefits; for example, IP Australia, an agency within the Department of Industry, Innovation and Science which administers intellectual property rights, uses public cloud to process data, obtain insights, and make decisions faster compared to operating on its legacy systems.[5]

Based on government sector expenditure on public cloud, which is around 23% of total public cloud spending in Australia (IDC, 2018a) it can be estimated that the cumulative productivity benefits of public cloud to the government sector could be in the order of $2.2 billion over the last five years.

However, it is important to note that this is a rough estimate only, as traditional measures of productivity are not as applicable to the government sector, where measuring the value of 'service' is not as

Chart 2.2 Main benefits of cloud experienced by agencies surveyed

Share of public cloud users surveyed

Benefit	Share
Improved agility - better able to scale operations as needed	79%
Improved productivity	71%
Better infrastructure and service/reliability/data security	61%
Easier adoption of exponential technologies (e.g. artificial intelligence, virtual reality)	54%
Reduced technology costs	43%
Improved ability to process data	36%
Better interaction with customers	25%

Source: Deloitte Access Economics, 2019

4. AWS customer story
5. AWS customer story

straightforward as measuring businesses' inputs and outputs via costs and revenues.

That said, there is significant potential for the benefits of public cloud in Australia to be even greater. As shown in Chart 2.3, public cloud expenditure in Australia in 2018 was $4.1 billion, expected to grow to $8.1 billion by 2022, with the government sector share of this valued at $1.9 billion in 2022.

Public cloud is also uniquely placed to enable next-wave technologies. Over time, advances in technology will increase the ability to collect data, leading to exponential increases in the volume of data available for processing.

Public cloud's ability to process large and variable volumes of data is foundational to enabling technologies such as machine learning, drones, robotics, blockchain and the internet of things. For the government

sector, the ability to utilise these next wave technologies will unlock innovation in citizen insights and the way the sector is able to deliver services, resulting in potential efficiency benefits and a growing economic impact.

Chart 2.3 Public and private public cloud services spending
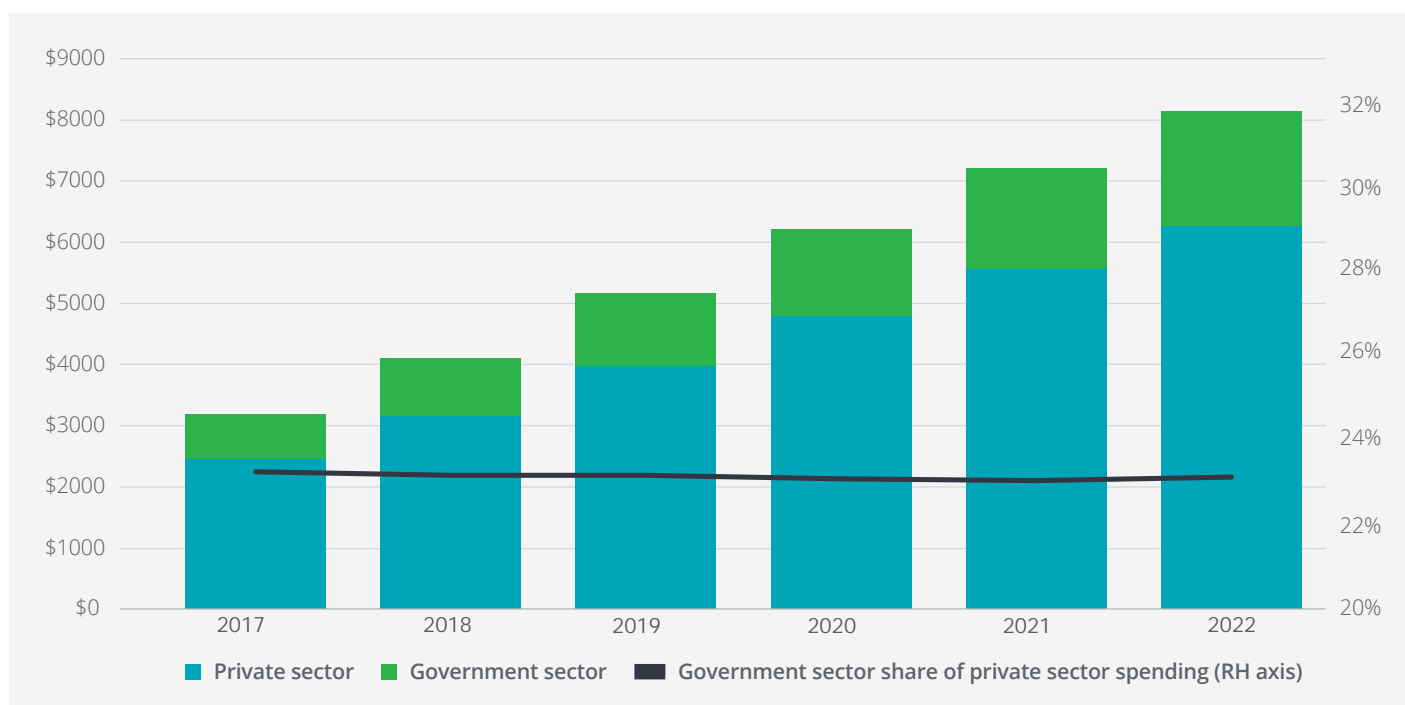
Source: IDC, 2018a. IDC definition of 'government sector' includes federal/central government, state/local government, education and healthcare sectors.

3 Government sector use of public cloud

3.1 Current use

For the government sector across Australia, public cloud represents new opportunities. Through moving away from traditional IT infrastructure towards a more flexible and adaptable operating environment, this new way of sourcing IT services provides the government sector with the ability to better serve the needs of its citizens.

Government sector use of public cloud reflects an amplified version of the Australian public cloud situation overall; the benefits of public cloud are potentially greater, and the barriers are more complex.

The government sector is a significant user of public cloud, spending around $950 million on public cloud in 2018 (IDC, 2018a). When compared with business use of public cloud, government sector expenditure represents 23% of Australia's total public cloud spending (IDC, 2018a)[6] and is proportional to its share of the Australian economy (24%) (ABS, 2018). Given that government sector agencies tend to be large organisations with significant legacy systems, this suggests their investment levels may be better than expected based on these barriers.

Federal government accounts for a significant share of public cloud expenditure in Australia. It is the third largest user of public cloud ($372 million in 2018), behind the banking sector ($633 million) and the telecommunications sector ($392 million) (IDC, 2018a).

Across the government sector, take-up of public cloud varies. As shown through the case studies in Chapter 5, some agencies, such as the Australian Bureau of Statistics, have started to experiment with public cloud and use it for specific applications. Many are operating in a hybrid cloud environment, with a mix of on-premises, private cloud and public cloud services. And others, such as the Queensland Building and Construction Commission, have migrated major core services to public cloud providers, or gone 'all-in'.

Chart 3.1 Average surveyed agency's IT structure
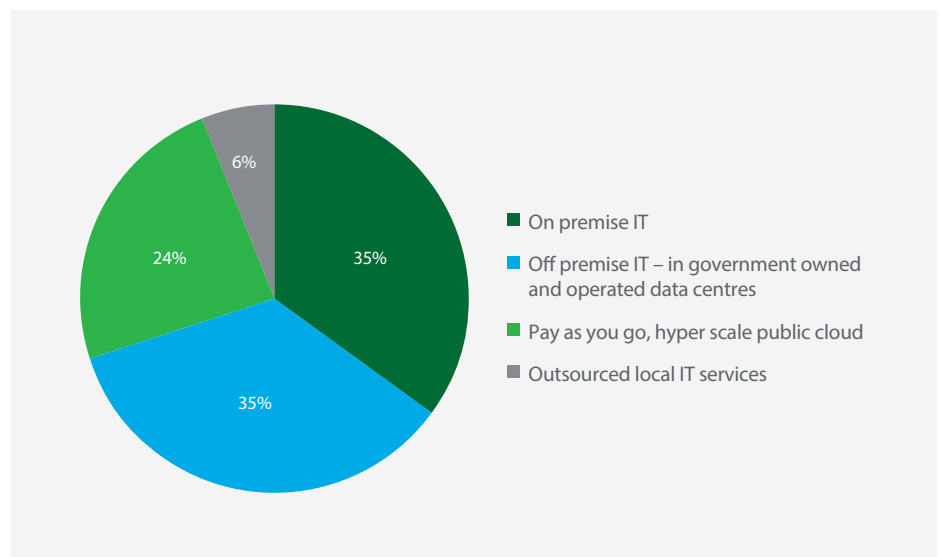
Source: Deloitte Access Economics, 2019

Deloitte Access Economics' survey of government sector decision makers found that, on average, public cloud accounts for one quarter of an agency's IT structure (Chart 3.1). Government data centres (35%) and on premise IT (35%) account for the largest shares of agencies' IT structures.

Agency size has a significant influence on its likelihood of using public cloud. As Table 3.1 shows, as the size of the agency increases, the share of its IT infrastructure using public cloud decreases. The smallest agencies surveyed (those with between 100 and 499 employees) used public cloud, on average, for over half of their IT systems, while this declined to just 9% for agencies with over 10,000 staff. This may reflect the flexibility of smaller agencies in adopting new approaches, relative to larger agencies having more complex legacy systems or organisational structures that may be a barrier to change. These findings correspond with the experiences canvassed in our consultations with government sector stakeholders (see Chapter 5) which indicated that smaller agencies are more agile and open to making a transition to public cloud.

Federal government accounts for a significant share of public cloud expenditure in Australia.

6. This includes expenditure on IaaS, PaaS and SaaS. By some definitions, SaaS may not reflect a proactive decision by leadership to move to public cloud as the underlying hosting platform may not be obvious. If this category were excluded, government sector expenditure on public could be around half of the total.

Table 3.1 Agency size and average public cloud's share of IT structure

Agency size (number of employees)	Average share of IT systems in public cloud
100 to 499	51%
500 to 999	45%
1,000 to 2,999	21%
3,000 to 4,999	18%
5,000 to 9,999	12%
10,000 or more	9%
All respondents	**24%**

Source: Deloitte Access Economics, 2019

Reflecting the early stages of government sector use of public cloud use, the majority of agencies surveyed reported using cloud for basic tasks. For example, over 80% of respondents were using public cloud for data storage and were less likely to be using the more advanced capabilities of machine learning (21%) or personalised user interfaces (11%).

This is mirrored in the private sector, where the most common uses of cloud are software applications (such as customer relationship management, invoicing and marketing) and data storage (Deloitte Access Economics, 2019).

However, this is expected to change over time as businesses invest more in cloud and begin to utilise its more advanced offerings such as hosting bespoke applications, enterprise resource planning and next-wave technologies. Some of these functions may be less applicable for the government sector relative to the private sector (e.g. blockchain and robotics), though potential use cases may increase over time.

An international survey of government sector decision makers found that in Australia, around 40% of government sector agencies were currently using Iaas, PaaS and SaaS, while internationally, there was a stronger trend towards SaaS use (IDC, 2018b).

Chart 3.2 Reported uses of public cloud by agencies surveyed
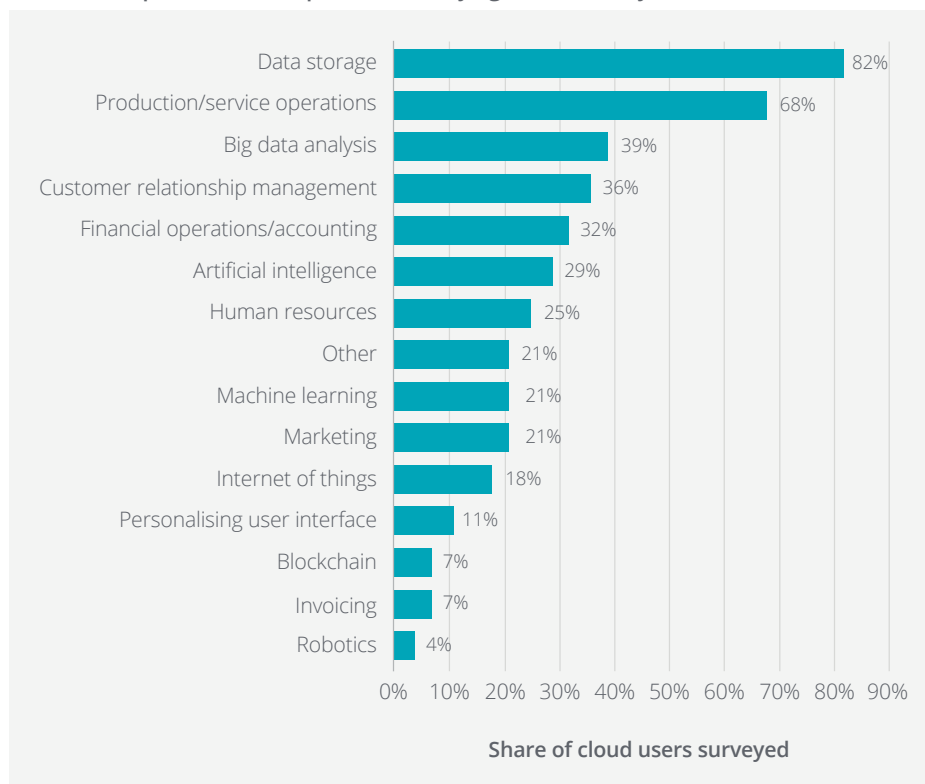
Source: Deloitte Access Economics, 2019

Chart 3.3 Current or near term plans for cloud deployment options
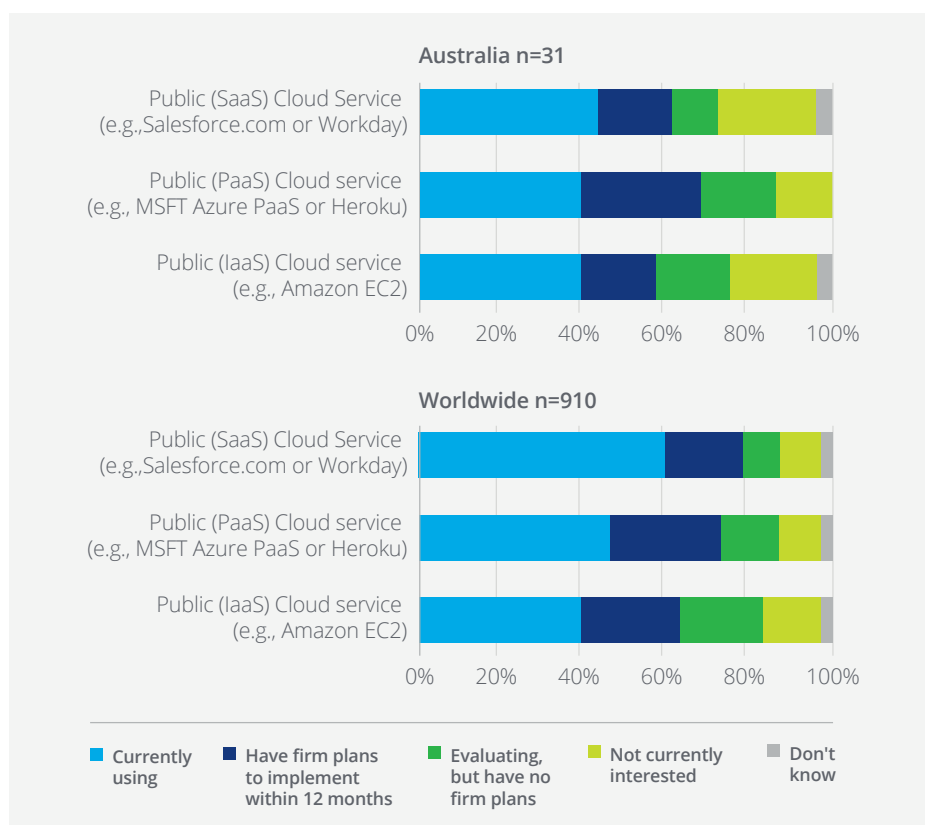
Source: IDC, 2018b

3.2 Government cloud policies

Government policy supports the transition to cloud where possible. The federal government, states and territories have existing cloud policies or strategies. These strategies, summarised in Table 3.2, outline agency responsibilities when using public cloud and provide guidelines on considering when cloud may be appropriate, as well as procurement, risk and other considerations.

These strategies tend to be broad in their scope and direction. While they generally emphasise a strategy to migrate current functions to public cloud where appropriate, they leave much discretion to individual agencies. In some cases, implementation can be unclear or the policy narrows the provider options (Table 3.2).

The strategies also commonly reference data security considerations; it is noted that Australian Cyber Security Centre (ACSC) Protected Certification, now granted to a range of public cloud providers, enables greater certainty around the security of certified entities, meaning that data can now be stored and processed at the protected security classification level, overcoming this barrier to public cloud use. This is discussed further in section 4.3.

Australian government sector decision makers are positive about the maturity of their cloud strategies (see Chart 3.4). Globally, government sector decision makers in Australia and overseas are most likely to consider their current strategy as 'managed'. However, when considering their strategy in the next two years, Australian government sector decision makers are more likely to perceive their strategy as 'optimised', relative to their global counterparts (46% compared with 39%) (IDC, 2018b).[7]

IDC (2018b) research also finds that government decision makers in Australia are in fact most likely to describe their approach to cloud as 'cloud also', where cloud is considered among the options but not necessarily as the first option, while internationally, cloud approaches are most likely to be described as 'best fit', with decisions on a case by case basis (see Chart 3.5). This suggests that the Australian government sector's posture towards using cloud for net new IT services is ahead of international comparators.

Australian government sector decision makers are positive about the maturity of their cloud strategies.

7. **Managed:** Description: Widespread use of cloud is supported by proactive business and IT leadership driving decisions about cloud use, operational policies, IT architectures, and contract negotiation and monitoring. Mission-critical workloads and applications are increasingly implemented using cloud platforms and services. Workload portability increases while end users enjoy consistent experiences across applications. Business Outcome: Infrastructure and development resources are more scalable, available, and cost effective.

    Optimised: Description: Company has broadly implemented a cloud-native strategy that is proactively managed and is clearly driving business innovation while improving IT operational efficiency. Organizations' cloud strategies and policies are consistently defined and implemented, resulting in more robust and flexible IT availability and lower costs and risks. Business Outcome: Business innovation and digital transformation exist throughout the organization and partners, with a clear understanding of true cost and value (IDC, 2018b).

Table 3.2 Cloud policies by jurisdiction

Jurisdiction	Policy	Agency led aspects of cloud policies	Government directives of cloud policies
Commonwealth	Secure Cloud Strategy (2017)	Agencies are responsible for their cloud migration strategies and security certifications of public cloud providers. Procurement of cloud services to be based on review recommendations decided by agency specific panels.	Government has produced frameworks for agencies to follow: a provider assessment framework, responsibility and accountability framework, collaboration platform, skills program and common shared platforms. Whole of government panels are to be used for government wide projects.
NSW	NSW Government cloud policy (2018)	Agencies are responsible for their cloud migration strategies and they bear the majority of security risk and responsibility when procuring public cloud solutions.	The government has devised a procurement framework using The *GovDC Marketplace* for agencies to purchase services. The government has produced a Registered Supplier List for public cloud providers that have met overarching security certifications. Government stipulates that health information must not be transferred out of state.
Victoria	Cloud Computing Policy (2013)	Agencies are responsible for their cloud migration strategies as well as procurement processes.	The government has produced guidelines on risk assessment for public cloud procurement. Agencies must adhere to cloud Victorian government computing checklists, public record acts, security policies and privacy policies.
Queensland	Cloud Computing Strategy and Implementation Model (2014)	Agencies are responsible for their cloud migration strategies and the rate at which they transition from service provider to service broker. Agencies are responsible for securing their data and must produce a local supplier benefits test when procuring cloud services.	Agencies must follow a 'cloud first' deployment model, where cloud solutions must be considered first for any new IT procurements. The government maintains a marketplace for ICT and cloud services for agencies using an authorised supplier panel. Whole of government cloud community skill share to enable knowledge transfers between agencies.
South Australia	Cloud Services Policy (2015)	Agencies are accountable for the security of their data.	'Cloud first' policy unless it does not deliver the best value for money or does not meet government obligations.
Western Australia	Cloud Policy (2016)	Agencies are responsible for their cloud migration strategies and how ICT is managed and delivered. Agencies are to evaluate cloud and pay as you go option for all new or redeveloped services and projects.	Government has directed agencies that their first preference for procurement should be to reuse or adapt existing systems if suitable. The Government has developed *GovNext*, a common use agreement to relocate 60 physical data centres into a pay-as-you-go secure private cloud.
Tasmania	Tasmanian Cloud Policy (2015)	Agencies may have residual small local ICT servers.	Agencies must locate most of their information and services in the on-island *Tasmanian Cloud*. All agencies are to have closed their existing data centres and be progressively moving away from owning ICT server and storage equipment.
Northern Territory	Cloud computing policy (2017)	Agencies bear almost all the responsibility for cloud related use, from migration strategies, to procurement and securing agency data.	Government procurement policies stipulate that a minimum 30% weighting to local content and agencies are required to prepare an Industry participation plan inviting at least one Territory enterprise.
Australian Capital Territory	ACT Government Digital Strategy (2016)	Agencies acquire approval from the ACT Digital Service Governance Committee if a non-cloud based solution is selected. Agencies are responsible for securing their data and ensuring cloud providers meet business, regulatory and policy requirements.	The ACT government has directed agencies to follow a 'Cloud first' deployment model, with the aim of migrating current assets and services into the cloud. Agencies are not to undertake bespoke builds unless when a unique core capability must be satisfied.

3.3 International experience

Globally, government sector use of public cloud is still relatively low, though internationally a greater share of IT budgets are being spent on cloud. An IDC survey of 78 European government agencies indicates that only 9% of respondent's IT budgets are currently being used on public cloud services, expected to increase to 13% in the next two years (IDC, 2018c). The higher use may reflect better compliance of agencies to governments that have 'cloud first' policies, such as the UK in where public cloud is specifically stated as the pre-ferred cloud deployment model (Govern ment
Digital Service, UK Government, 2017).

Private cloud[8] use is twice as prevalent as public cloud use, mostly due to perceptions on security, data privacy and the ability to easily exit solution providers. In fact, 77% of respondents reported that data centres being located in-country was important or very important when considering potential cloud service providers (IDC, 2018c).

The IDC survey also found that internal cloud strategies in European government agencies have been viewed as lacking direction, with almost 40% of respondents stating their current cloud strategy is either ad hoc or opportunistic. Only 13% of respondents reported their current cloud strategy as optimized (IDC, 2018c).

Yet governments are starting to value the benefits that a transition to public cloud can bring, with 52% of respondents expecting to see improvements in agility in 2018, up from 22% in 2017 (IDC, 2018c).

The latest available information on US Federal spending on cloud services highlights that it is comparable to European expenditure, accounting for roughly 8.5% of the total ICT budget (IDC, 2016). The US Federal government started a 'Cloud First' policy in 2010, yet saw slow up-take as most agencies lacked an implementation plan or strategy. The replacement, 'Cloud Smart' strategy aims to address adoption issues that agencies faced under the previous policy (Office of the US Federal Chief Information Officer, 2018).
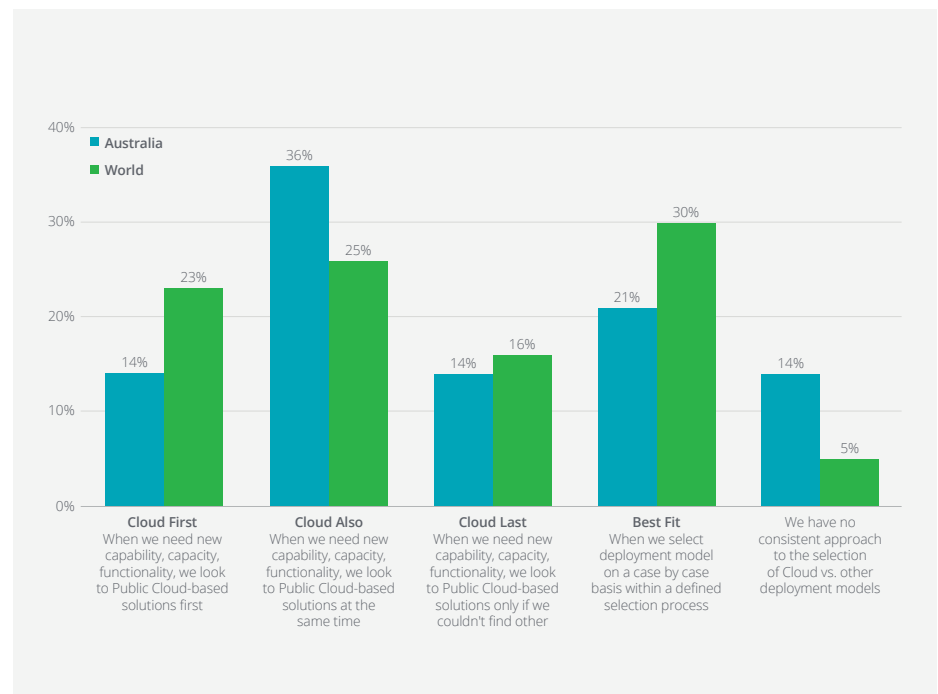
It is hard to make direct comparisons of public cloud use across countries, but by world standards, Australia is a fast adopter of public cloud[9] and in fact, is

Chart 3.4 Perspectives on maturity of current and expected cloud strategies
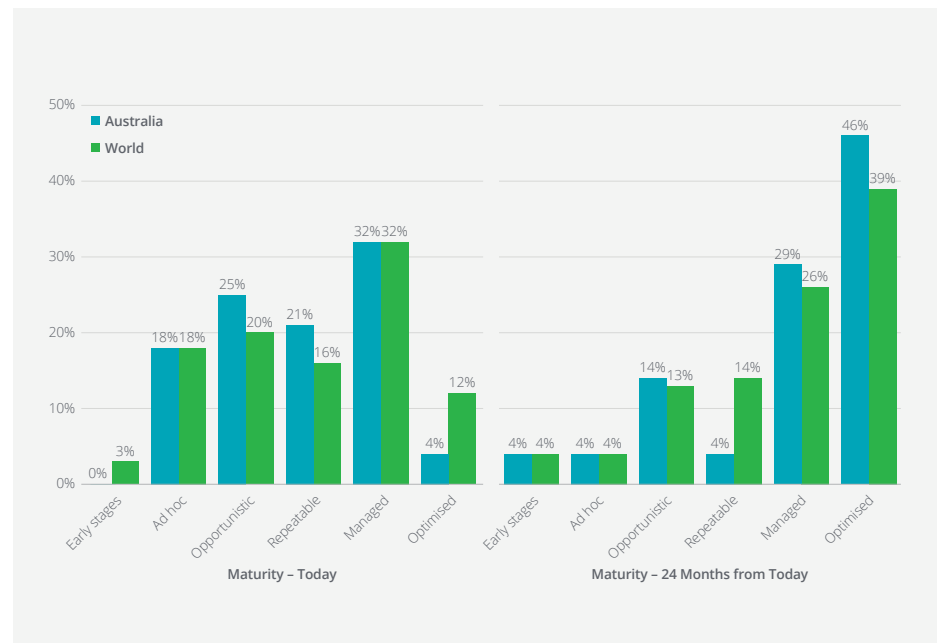
Source: IDC, 2018b

Chart 3.5 Public sector posture towards using the cloud for net new IT services

Source: IDC, 2018b

not far behind the top five countries' total expenditure on public cloud. For example, while the US spent more than

double what was spent in Australia on public cloud, its economy is around ten times the size of Australia's.

---

8. Private cloud refers to services and infrastructure which are maintained on a private network and dedicated to use by a certain group of users.

9. US was the largest market for public cloud services in 2018 (US$97 billion), followed by UK (US$7.9 billion), Germany (US$7.4 billion), Japan (US$5.8 billion) and China (US$5.4 billion) (IDC data cited in Technology Record (2018). IDC (2018a) estimates Australian expenditure on public cloud in 2018 to be US$3.0 billion.

4 What's holding the government sector back?

4.1 Barriers to adoption and expansion of public cloud

The government sector is facing implementation challenges for public cloud, resulting in missed opportunities. Over time, if the government sector does not keep up with the pace of business use of public cloud, it may struggle to meet the evolving needs of its citizens. The move to public cloud has been likened to the digital transformation process for government, with progress lagging behind the private sector. Particularly in an election year, 'big decision inertia' can limit the appetite for change, however, it is in making the strategic decision to move to cloud that uncertainty can be reduced in the future.

Firstly, the 'burning platform' for change is not evident for many agencies. While some high-profile moves to cloud have been the result of large scale issues with existing systems, as experienced by the myTax system and 2016 Census, these examples have not influenced other agencies to follow suit.

Deloitte Access Economics' survey found that for government agencies, the most reported barriers to adopting or expanding the use of public cloud were policy related – namely data privacy concerns and data sovereignty concerns, cited by 79% of respondents. This can reflect a disconnect between overarching policy and enabling policy, or perceptions of risks which can be managed (see section 4.3).
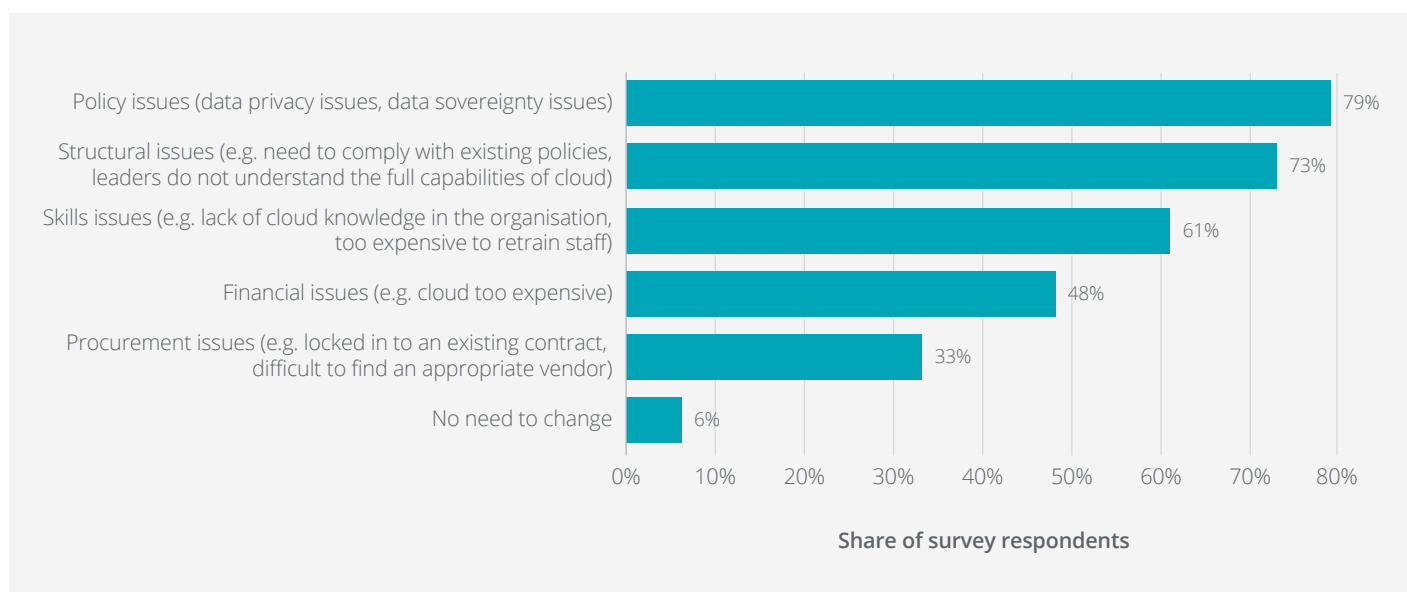
Further, it was noted that leaders do not understand the full capabilities that cloud offers. The lack of provision for additional operational expenditure in place of capital expenditure in an agency's budget was also identified as a challenge in adopting cloud. These barriers are similar to those experienced by the private sector, namely inadequate skills, legacy systems and costs of adoption.

> **This chapter explores the key barriers to government sector use of public cloud. Namely:**
>
> - understanding and skills gap
> - risks – data privacy and sovereignty
> - procurement policies
> - budgeting
> - organisational culture.

Chart 4.1 Barriers of adopting or expanding use of public cloud by government agencies

Barrier	Share
Policy issues (data privacy issues, data sovereignty issues)	79%
Structural issues (e.g. need to comply with existing policies, leaders do not understand the full capabilities of cloud)	73%
Skills issues (e.g. lack of cloud knowledge in the organisation, too expensive to retrain staff)	61%
Financial issues (e.g. cloud too expensive)	48%
Procurement issues (e.g. locked in to an existing contract, difficult to find an appropriate vendor)	33%
No need to change	6%

Share of survey respondents

Source: Deloitte Access Economics, 2019

4.2 Understanding and skills gap

A common theme discovered through both consultations and the survey of government sector decision makers is that insufficient knowledge of or understanding about using public cloud is holding agencies back. In fact, 73% of agencies reported that leaders do not understand the extent of capabilities that public cloud offers.

There is a perception in the government sector that government data centres or 'government cloud' is the same as public cloud, when in fact this is a private cloud. It should be acknowledged that government cloud can be a good first resource consolidation step. Indeed, government cloud allowed government to tackle many of the data, governance and cultural challenges in an environment that gave a level of comfort. However, in order to unlock the full benefits of technology and cost savings over time, the government sector is now on the verge of needing to make the next step to public cloud.

Skills gaps in the IT sector are a problem for Australia more broadly. There are fewer than 5,000 ICT graduates each year in Australia, and Australia's ICT performance ranks seventh out of 16 countries on measures relating to consumers, businesses, and workforce skills. In 2017 there were just over 50,000 IT workers in the public sector, but this will need to grow significantly if cloud services are to be better implemented (Deloitte Access Economics, 2018). Further, there will be a need to upskill non-IT workers in the use of cloud, so that systems can be used by all.

AWS initiative: cloud skills

Organisations looking to accelerate cloud adoption need employees with cloud IT skills, and research from IDC (2017) shows trained organisations are 80% faster to adopt cloud. However, a study by TEKsystems (2016) indicates 68% of IT leaders do not believe their organisations have the required IT skills in house to address their needs. In response to the need for highly skilled cloud IT professionals, AWS offers free access to over 340 online courses and through strategic partnerships with select digital training providers, and over 40 classroom courses are being delivered by AWS trainers. To further address the cloud IT skills gap, AWS offers nine AWS Certifications to validate technical skills and expertise, providing employers a way to identify talent.

In order to develop the next generation of cloud IT skills, AWS offers two global programs, AWS Educate and AWS Academy, and a variety of local initiatives in Australia, like Kids in Tech and the Young Women Leaders in AI program.
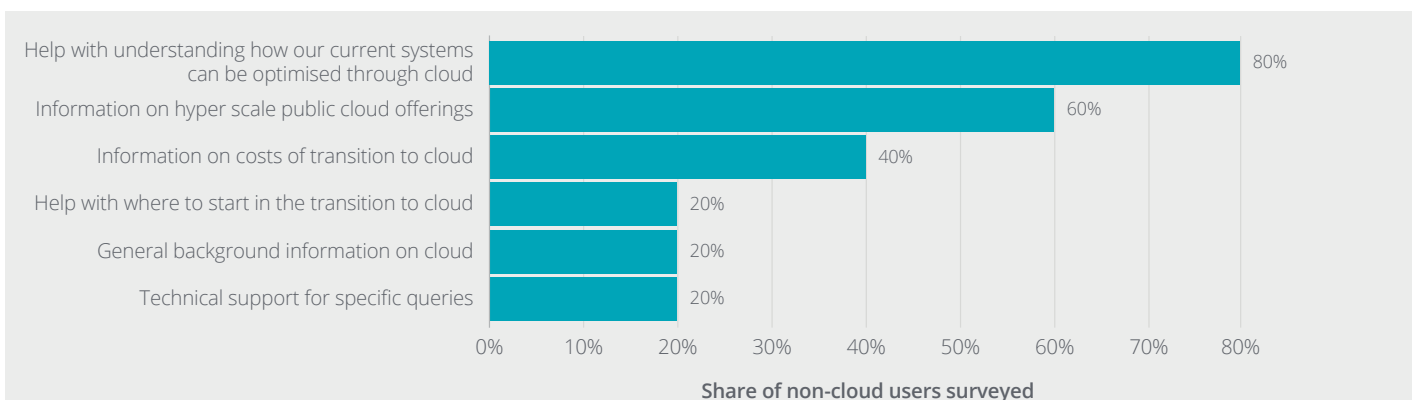
AWS Educate is an online portal with content developed by AWS and other leading educational institutions for the purpose of upskilling students and academics on cloud technology. The learning content is broken into micro credentials and in-depth career pathways including basics topics like "Cloud 101" through to advanced topics including "Machine Learning Scientist", "Cybersecurity Specialist" and "Data Scientist". Educate is designed to support either self-paced learning or integration into other learning delivery mechanisms, and includes yearly free cloud credits to support the practical implementation of learning.

The foundational purpose of the Educate Program is upskilling students and academics across the K-12, VET and Higher Education sector. However, AWS also recognises the value of the Educate content portal for upskilling personnel within public sector departments and is happy to work with relevant agencies to integrate the content into any existing professional development ecosystems.

AWS Academy provides higher education institutions with access to formalised AWS authorised curriculum which aligns to and helps students achieve AWS Certification. AWS launched this program in 2017 and currently have more than twenty enrolled institutions in Australia. The program focuses on driving educator enablement to deliver this curriculum, with the ultimate aim to ensure student employment.

Source: AWS

Chart 4.2 Types of support non-cloud agencies need to start using public cloud services

Type of support	Share
Help with understanding how our current systems can be optimised through cloud	80%
Information on hyper scale public cloud offerings	60%
Information on costs of transition to cloud	40%
Help with where to start in the transition to cloud	20%
General background information on cloud	20%
Technical support for specific queries	20%

Share of non-cloud users surveyed

Source: Deloitte Access Economics, 2019

AWS initiative: enterprise support

Agencies and businesses may subscribe to AWS Enterprise Support as they adopt and run cloud services and solutions. AWS Enterprise Support is designed to help customers better understand how to reliably use the cloud, adopt best practices in operations, security and governance and assist with skilled experts for support related questions.

AWS Enterprise Support customers receive a designated Technical Account Manager who works closely with the agency technical staff and customer leadership teams on an ongoing basis to coach the agency staff through the various phases of cloud adoption. Early in the cloud adoption lifecycle the Technical Account Manager focuses on safe adoption and technical coaching. Later in the adoption lifecycle this focus moves to help customers scale their solutions and improve cloud operational maturity in cost control, security and governance.

AWS Enterprise Support also includes features to help customers prepare, plan and support application and product launches, deliver self-paced technical training and API connectivity to 3rd party development pipeline or support/help desk tooling. In the event of a support problem occurring, customers are able to raise support requests 24x7 to AWS Cloud Support Engineers with a 15 minute response for critical cases.

Source: AWS

It is possible that this lack of understanding could also be affecting the basic use cases of public cloud, with over 80% of respondents using data storage, but little use of more complex capabilities such as machine learning and blockchain.

This suggests an opportunity for increased government sector education on cloud use and capabilities. The survey found that the majority of agencies not using public cloud stated that help with understanding how their system could be optimised through public cloud would lead to adoption, as would more information on public cloud offerings. The majority also indicated that in person support would be the most useful in helping make the move the public cloud.

4.3 Risks – data privacy and data sovereignty

Real and/or perceived risks of public cloud pose a significant barrier for both current public cloud users and non-users. Although some agencies may have already moved non-sensitive information to public cloud, perceptions and policies regarding the storage of sensitive information has meant that much is still stored in government data centres rather than on public cloud.

As noted in the case studies (see Chapter 5), public cloud providers achieving Australian Cyber Security Centre (ACSC) Protected Certification may assist in reducing this barrier. ACSC Protected Certification enables public and private sector organisations to store and process highly sensitive data at the protected security classification level, supporting the Digital Transformation Agency's Secure

Cloud Strategy and reducing barriers to the government sector making the most of public cloud.

The survey findings also highlight that 79% of agencies identified data privacy and data sovereignty issues in the top barriers to expanding use. These findings are similar to those found by Gartner (2018), which predict that found that security and privacy issues are some of the top objections to adopting public cloud.

As we move to a more interconnected world, the government sector will need to tackle a range of challenges including data moving across international boundaries. Where public cloud providers have data centre infrastructure in Australia, this can present a solution; by enabling the use of public cloud domestically and providing the option to prevent it from being processed overseas. The government sector will need to look at regulations and guidelines to ensure that public cloud decisions are based on real obligations (rather than perceived and preferred) to make informed decisions to ensure critical datasets and algorithms trigger the appropriate restrictions from being processed overseas.

4.4 Procurement policies

Public sector procurement policies include a number of considerations for engaging external suppliers, ranging from overarching and general rules regarding value for money and threshold arrangements, to security, data protection, records, audit and confidentiality considerations.

One of the major challenges for government sector procurement is the different procurement process for public cloud compared with traditional IT procurement or procurement of other services. In particular, the government sector historically has had discretion over the terms of any agreement they enter in to, but customisation of contracts is not compatible with the public cloud business model because the platform is available in the same way for all users.

Public cloud providers supply an infrastructure network with security measures for agencies to design their own solutions. This means that agencies are responsible for managing access to third parties' products and services hosted by cloud providers. This shared responsibility model can be a new approach for government, where responsibility has traditionally been borne by its suppliers.

An AWS analogy of this situation is going to a hardware store to purchase plumbing materials and asking the store if this has been installed correctly, rather than asking a plumber. An improved understanding of the public cloud model will assist in overcoming procurement challenges.

Other countries have already incorporated responsibility sharing into how they approach cloud solutions. For example, the Canadian Government noted in their cloud strategy that security control profiles are to be tailored to public cloud environments and recognise that both the provider and consumer should share responsibility for security (Government of Canada, 2018).

4.5 Budgeting

Managing the costs of a move to public cloud can also be a challenge. For some agencies, where there are designated annual IT capital budgets, but operational budgets are shared throughout the agency, it is unclear where the budget for such an IT transformation would come from.

While a move to cloud can be marketed as reducing costs, an optimised cloud strategy is needed to manage the transition and ensure that capital costs are reduced as operational costs increase. When there is uncertainty around the management of costs, this can hinder government sector decision making.

Switching expenditure models has also been a concern brought up in consultations. Some agencies perceive operating expenditure models as more uncertain in the long term compared to capital expenditure models. To optimise an operating expenditure model, consultations have suggested the need for appropriate training and problem solving skills of IT staff to manage the pay-as-you-go nature of public cloud. Finance departments may also need training to understand the nature of the transition and implications for the agency's budgeting.

The Digital Transformation Office recently proposed changes to funding models to help overcome this barrier, noting that "Future budgeting processes could help government make more frequent, smaller-scale decisions, helping to adapt to new technologies sooner".

4.6 Organisational culture

Organisational culture underpins all the other challenges of moving to public cloud. A culture of risk aversion and decision inertia across the government sector, particularly in larger agencies with significant legacy systems in place, can be a significant barrier to adopting new technologies and new ways of working. However, with a desire for change and visionary agency leadership, action plans can be implemented to increase knowledge and skills, manage risks and procurement challenges, and restructure agency budgets.
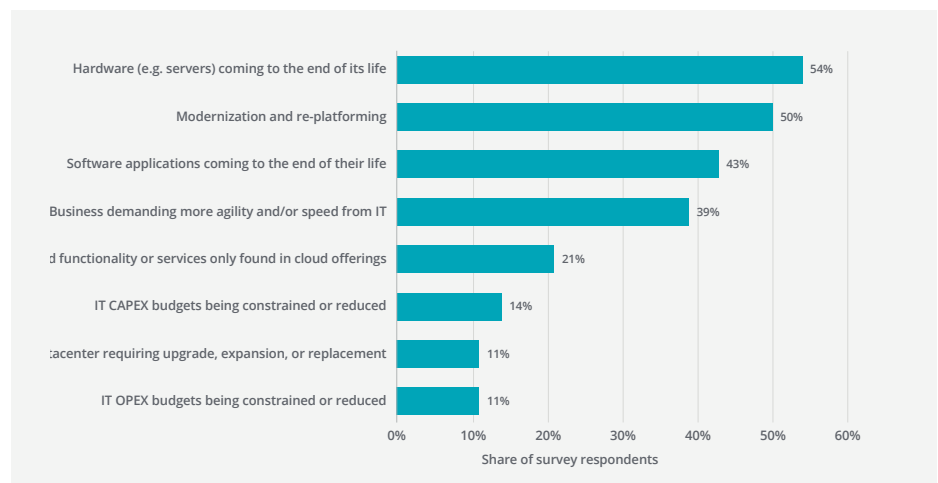
5 The public cloud transition journey

There are several factors to consider in a cloud transition. The following lessons are based on five case studies of successful government sector transitions to public cloud and nine consultations with subject matter experts from AWS, Deloitte and public sector leaders.

To support a successful transition to public cloud, government sector considerations should include:

- **Finding the opportunity:** Prepare for a move to public cloud – while contracts renewals are an opportunity to consider future use of public cloud, prior preparation may enable an earlier or smoother transition.

- **Managing risks:** Public cloud has been used successfully in high profile and sensitive situations such as by the Australian Bureau of Statistics for the Australian Marriage Law Survey, and the Australian Taxation Office for logging tax returns. A considered risk management approach is required to mitigate the residual risks of running sensitive workloads in public cloud. There is a need to understand data rules in an agency's jurisdiction and the management of preventable, strategic and external risks to the agency.

- **Financial considerations:** There is a need to consider the implications of a move to a consumption based pricing model and a need to educate the relevant staff managing these changes to government sector budgets.

- **Upskilling staff:** An understanding of the organisational staff capability, skills gaps and the change management required.

- **Governance:** Agency leadership is critical for driving change. There is a need to align skills and processes to IT strategy and the agency's operating strategy.

Chart 5.1 Most important trigger factors leading to use or serious consideration of use of cloud services

Hardware (e.g. servers) coming to the end of its life	54%
Modernization and re-platforming	50%
Software applications coming to the end of their life	43%
Business demanding more agility and/or speed from IT	39%
...d functionality or services only found in cloud offerings	21%
IT CAPEX budgets being constrained or reduced	14%
...acenter requiring upgrade, expansion, or replacement	11%
IT OPEX budgets being constrained or reduced	11%

Share of survey respondents

Source: IDC, 2018b

- **Supporting others:** The transition to cloud can be harder for larger agencies and those with more complex legacy systems. Agencies can learn from success in other agencies, and lessons and skills learnt can be shared across the government sector.

IDC (2018b) research has also considered the 'trigger factors' for a move to cloud. As shown in Chart 5.1, the top three factors identified by the government sector are hardware coming to the end of its life (54% of respondents), modernisation and re-platforming (50%) or software applications coming to the end of their life (43%).

These factors correspond with the following case study experiences illustrating different public cloud transition journeys.

- For the **Queensland Department of Transport and Main Roads**, using public cloud was a natural choice for the Cooperative and Automated Vehicle Initiative (CAVI), involving the largest

Cooperative Intelligent Transport Systems (C-ITS) pilot in Australia to date.

- **The Australian Bureau of Statistics** (ABS) successfully demonstrated the application of public cloud in the implementation of the online component of the Australian Marriage Law Postal Survey.

- For the **Australian Taxation Office**, public cloud offered the ability to boost their capacity and enhance customer experiences.

- **The Queensland Building and Construction Commission** experienced a 'burning platform' for change, and now operates entirely through cloud.

- **The South Australian Department of Planning, Transport and Infrastructure** moved their geographic information and traffic management systems to cloud when faced with ageing infrastructure that no longer meets their processing needs.

Queensland Department of Transport and Main Roads

The Cooperative and Automated Vehicle Initiative (CAVI) is a project being delivered by the Queensland Department of Transport and Main Roads (TMR). Its purpose is to help prepare for the arrival of new vehicle technologies with safety, mobility and environmental benefits on Queensland roads.

Due to the nature of the program, a hyper-scale cloud solution was an obvious choice for the main component of the program, the Ipswich Connected Vehicle Pilot, which will use roads in and around Ipswich, from late 2019.

The pilot will include up to 500 vehicles retrofitted with Cooperative Intelligent Transport Systems (C-ITS) technologies and is the largest C-ITS pilot in Australia to date.

These vehicles are to be retrofitted with C-ITS enabled devices that meet current European standards, and support interoperability – meaning regardless of brand, all devices will be able to communicate with each other.

These devices will enable many safety use-case applications, including vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), to operate in the participating vehicles.

This will allow the participating vehicles to 'talk' with each other (V2V), roadside infrastructure (V2I) and with a central station (V2I).

Director-General of TMR Neil Scales, said the central station was always going to be cloud-based, giving access to a wider set of solutions.

"The use of a public cloud-based system allows customers to share data back to the central station in a highly efficient way.

"For us, the decision to move to a cloud-based solution was easy, as it strategically aligned with wider departmental approaches, emphasising that for areas such as Intelligent Transport Systems (ITS), and the future of vehicle safety, partnerships between Government and industry are vital."

Case study 2

Australian Bureau of Statistics

In 2017, the Australian Bureau of Statistics (ABS) successfully utilised AWS hyper-scale public cloud to deliver services for the Australian Marriage Law Postal Survey, including an online return form and interactive voice (IVR) recognition, and a platform for publishing the result.

"The use of public cloud services provided a resilient and contemporary experience for those participating in the Marriage Law Survey" said ABS CIO Steve Hamilton.

Drawing on lessons learnt from the 2016 Census as well as insights gained from his experience with the ATO's shift to digital service delivery, ABS CIO Steve Hamilton commented that "for the Marriage Law Survey, a cloud solution where we could build a native cloud application on serverless technology with all the contemporary security features available to us and have the ability to draw on near infinite capacity architected in as a feature was a natural option. Almost the perfect use case."

"Hyper-scale cloud and our use of the agile delivery method for the survey provided a platform that addressed three key technology drivers for the survey: user experience with accessibility as a focus, resilience of service and security." Mr Hamilton also remarked that "when the result was published, the ABS website was hit with substantial valid traffic in a very short period of time and scaled perfectly" but that they also "detected and thwarted a reasonable amount of nefarious activity."

Due to time constraints to deliver the survey and the need for resilience, Mr Hamilton noted little challenge internally to using a cloud solution, stating that "from the Australian Statistician down, cloud and agile was embraced as something we wanted to use. Within an accelerated learning environment the AWS and ABS delivery team worked side by side,

and the urgency proved to be a positive in not overthinking or over-engineering the process. It proved to be a good experience for our first large scale use of public cloud".

Since then, ABS has been experimenting with cloud in a sandbox environment using multiple platform providers to test products that can enhance current IT practices and organisational capabilities. As part of an approach to market for a partner to deliver the Census 2021 Digital Service, the ABS are considering ACSC certified Protected cloud hosting services as part of the solution.

In line with the Digital Transformation Agency's (DTA) secure cloud first policy, cloud is being considered for all new opportunities at the ABS. ABS Chief Information Security Officer, Julian Doak commented that "Protected Level Certification by the Australian Cyber Security Centre is expected to go a long way to putting at ease some concerns around cloud. For us, when considering cloud security, perceptions can matter as much as reality, particularly in relation to confidential personal information."

From a financial perspective, managing the shift from capital to operating expenditure is also a significant consideration when transitioning to cloud. Instead of leveraging a dedicated capital budget, operating expenses for cloud will directly compete with the agency's other operational costs. There needs to be greater consideration of financial controls and changes to internal constructs to manage the costs relative to a business as usual scenario.

Mr Hamilton noted that "CFOs are unlikely to be convinced by a more expensive option, even if operating and delivery risks are reduced. However, from a service delivery perspective it's all about creating public value faster with cost optimisation and risk reduction key factors. A CIO's best friend in an organisation is the CFO, so when I can build a platform for a national event, use it and fully decommission it without incurring sustainment costs, that's got to keep them happy!"

Case study 3

Australian Taxation Office

The Australian Taxation Office (ATO) is the statutory agency responsible for administering the Australian federal taxation system, superannuation legislation, and other associated matters.

In recent years, the ATO has moved its mission critical applications off-premise and into public cloud. The ATO website, and myGovID digital identity are currently running in public cloud. The myTax application also runs on public cloud, allowing people to launch tax returns electronically on smartphones or smart tablets.

The decision to move to cloud was influenced by a number of factors - policies of digital by default and cloud-first, as well as an executive decision to move off-premise. The ATO was one of the first Federal Government institutions to implement these strategies, paving the way for others to follow.

The benefits of cloud for the ATO have included improved reliability of services, which has helped build public trust around its services. Further, cloud has provided the opportunity to design new public-facing systems, deliver citizen-centric services and more efficiently make the most of emerging technology.

For example, since adopting voice biometric technology in their call centre, around 4 million clients have enrolled their voiceprint with the ATO. Cloud will support use of artificial intelligence, smarter data analytics and the Internet of Things.

Source: Financial Review (2017), IDG Communications (2016)

Queensland Building and Construction Commission

QBCC is the regulatory body for the Queensland building and construction industry established in 2012. As a relatively new agency, QBCC has been able to be agile and adaptable to technology solutions.

Organisational flexibility, and the potential benefits for customers and staff, were key drivers of the move to a hybrid cloud solution. The opportunity to move to public cloud arose when traditional server hardware was approaching its end of life in 2017.

The move to public cloud has enabled QBCC to become an insights-driven regulator, making the most of data in its decision making. For example, this can include identifying companies at future risk of insolvency, or being able to identify the most common building defects in Queensland.

"Cloud enables QBCC to quickly provision new environments, scale up and down to meet demand, remain flexible, improve the resilience, availability and performance of systems to customers and staff," noted Ben Ward, QBCC Chief Operating Officer.

The successful transition to cloud was underpinned by acknowledging the organisation change required and managing this carefully. A roadmap for change, the inclusion of staff right from the beginning, and being transparent about changes all contributed to effective implementation.

Source: Telstra (2018)

Case study 5

Department of Planning, Transport and Infrastructure South Australia

The Department of Planning, Transport and Infrastructure (DPTI) South Australia started on their transition to public cloud in 2017 to address a need for greater capacity that was beyond that of their existing assets.

Greg van Gaans, Manager of Solution Services at DPTI, says the decision was driven by the need to replace ageing infrastructure that was no longer coping with peak workloads. "We were using the servers at peak processing capacity on the weekend; we could not do any processing on weekdays as this would affect our normal operations."

While there were initial concerns around the move to cloud, cloud has been a good solution for this problem. "The security of our information, whether public cloud would be prove to be more costly, whether it could manage the variable workloads, and internal knowledge gaps were all concerns potentially hindering a successful transition. But with the in-person technical support we received to support the transition, we overcame these barriers and it's been a great success."

DPTI's initial entry into public cloud was through a small workload as a pilot experiment. The chosen workload was Traffic SA, a public facing website which lists roadworks, incidents and planned events that occur across South Australia. As operational costs were only $6 a month, pilot risk was low and it allowed DPTI to explore the capabilities that cloud could offer.

"Two years down the track, the agency as a whole is making a solid effort to transition to cloud given the proven benefits. For instance, some of our workloads that require huge computing power now only take 14 hours to run, down from 56 hours before. That job used to cost us at least $2,500 a month to host onsite, but using public cloud it's only $100 per month".

For a successful migration and to achieve the intended savings, Mr van Gaans notes that a clear transition plan is needed. "Agencies should have a plan in place and retire infrastructure assets as soon as possible."

Looking back at DPTI's transition journey, Mr van Gaans notes that it would have been beneficial to view public cloud as "more than just replacing infrastructure. We should look at the native solutions that public cloud providers can offer when considering a move to cloud."

The biggest ongoing challenge in moving to an operational expenditure model is managing concerns around operational expenditure blowouts. "It can be useful to explain it like stationery procurement, where we have capped stationery budgets but we don't always spend all of it. This has increased understanding around public cloud budgeting".

Training was also a key factor for success. Investment in upskilling existing staff increases organisational engagement in cloud, supports staff retention and can be easier seeking the required skills externally.

6 Recommendations for action

In response to the barriers identified through consultations and findings from the survey, we have identified a number of recommendations that may assist the government sector in accessing the benefit of public cloud.

As Chart 6.1 shows, surveyed government sector leaders are overwhelmingly in support of greater cloud take up. For instance, 94% of government sector leaders agree that procurement process should be modernised and that government should invest in upskilling its workforce to be better prepared for public cloud.

The identified benefits of public cloud have motivated the development of cloud first policies, but barriers to transition remain. The recommendations below are enablers to address these barriers and help the government sector achieve the benefits of public cloud, and help drive better agency and citizen outcomes over time.

Chart 6.1 Opinions of what should be included in the government cloud policy

Source: Deloitte Access Economics, 2019

Recommendation 1

Central/whole of government policies to be established and implemented, setting a timeframe for the majority of systems to be in the public cloud by 2025.

Perhaps one of the most simple changes that can be made is to set a clear timeframe for transition to cloud. The approach taken by many agencies currently is to move to cloud as legacy systems expire, but this will take decades.

Central/whole of government policies should be established with a goal to have the transformation well underway by 2022 and a set transition time for the majority of systems to be in the public cloud by 2025. Only around half of public sector leaders agree that all new systems should be in the cloud (Chart 6.1), but leaders should set out a clear strategy for how all appropriate

systems can be migrated. The timeframe for the move to public cloud will align with the Digital Transformation Strategy vision for Australia as one of the top three digital governments in the world by 2025.

The policies should also address at a whole of government level concerns relating to cybersecurity, identity and commercial/contracting considerations.

Recommendation 2

Government sector leaders to bring forward approaches in which capital budgets can be shifted to operating budgets in fiscally sustainable ways.
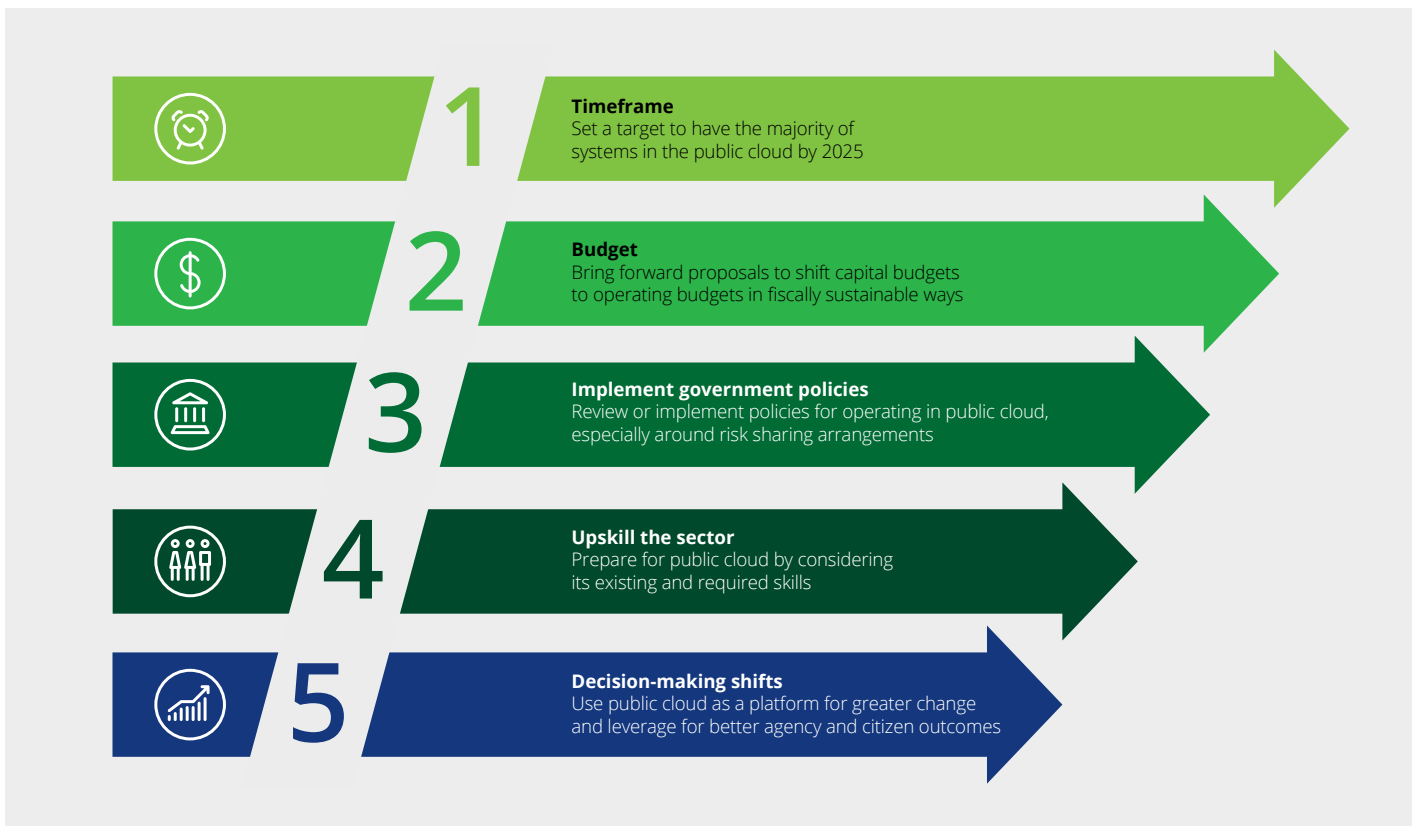

A barrier identified by the majority of survey respondents was that budgeting for IT is outdated, and cloud requires more operational expenditure than they have available. But stakeholders also said that it was not as simple as switching from a capital expenditure to an operating

expenditure model, as this makes the budget susceptible to other organisational activity and operational budget cuts.

We recommend that government sector leaders reconsider budgets, including potential trade-offs to facilitate a shift between capital and operating expenditure, so they can tailor their split between capital and operating expenditure to best meet their agency's needs.

Further, there needs to be consideration of the need to align depreciation and transition timeframes. Governance and project controls that are common for capital projects will also need to undergo change to ensure continuous improvements of the platforms over time.

Figure 6.1: Recommendations for increased government sector use of public cloud

1 **Timeframe**
Set a target to have the majority of systems in the public cloud by 2025

2 **Budget**
Bring forward proposals to shift capital budgets to operating budgets in fiscally sustainable ways

3 **Implement government policies**
Review or implement policies for operating in public cloud, especially around risk sharing arrangements

4 **Upskill the sector**
Prepare for public cloud by considering its existing and required skills

5 **Decision-making shifts**
Use public cloud as a platform for greater change and leverage for better agency and citizen outcomes

Source: Deloitte Access Economics, 2019

Recommendation 3

Review and implement government policies for operating in the public cloud, especially around risk sharing arrangements.

Policies outlining how the government sector should operate in the cloud need to be updated to reflect a contemporary procurement environment and implemented. While traditionally government contracts require all risks associated with data (such as data privacy and data sovereignty) to lie with the service provider, this is not possible for cloud services, and policies need to be updated to reflect a shared responsibility model. Some progress has already been made in this respect.

The mindset for procurement of cloud services also needs to evolve. From consideration as a capital project with a monthly charge flattened over the term of the contract, this needs to change to agencies thinking holistically. For example, this involves investing in core capabilities, making decisions for the whole of the agency, or government sector,

and preventing proliferation of solutions with similar functionality. This will prevent duplication of expensive integration costs and re-use of investment.

Recommendation 4

Government sector to prepare for public cloud by considering its existing and required skills.

Another key barrier identified was a skills gap – many government sector workers do not have the skills to use public cloud in a way that delivers the full potential benefits it can offer. Indeed, not one survey respondent was opposed to investing in the workforce to overcome this problem.

We suggest the government sector prepare for public cloud by identifying which skills are no longer required, which need to be enhanced, and what new skills need to be built in teams.

Achieving the required skills may involve hiring graduates with cloud knowledge, creating online self-paced learning modules for employees, or partnering with private sector to upskill government employees.

Recommendation 5

Use cloud as a platform for greater change in a more outcomes-focused and data-driven decision making environment, leveraging this for better agency and citizen outcomes.

The government sector should make the most of the data in the public cloud, and specific initiatives may be required to support data driven decision making.

In line with the broader trend towards an outcomes-focused government sector, agencies should be measured against outcomes (such as what will generate cost savings or deliver better service to citizens), not how they achieved them, and this should extend to public cloud procurement.

References

1. Amazon Web Services (2017) An Overview of the AWS Cloud Adoption Framework, Version 2, Available at: https://aws.amazon.com/professional-services/CAF/.Australian Bureau of Statistics (2018) 5204.0 – Australian System of National Accounts, 2017-18, Available at: http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/5204.02017-18?OpenDocument

2. Australian Public Service Commission (2018) Size of the APS, Available at: https://www.apsc.gov.au/size-aps

3. CSIRO (2016), Australia 2030, Available at: https://www.csiro.au/en/Do-business/Futures/Reports/Australia-2030

4. Deloitte Access Economics (2018) ACS Australia's Digital Pulse: Driving Aus tralia's international ICT competitiveness and digital growth, Available at: https://www.acs.org.au/content/dam/acs/acs-publications/aadp2018.pdf

5. DTA (2018), Digital Transformation Agency Submission in Response to the APS Review, Available at: https://uploadstorage.blob.core.windows.net/submission-uploads/fil03856fe4100ba4928134b.pdf

6. Edelman (2019) 2019 Edelman Trust Barometer, Available at: https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Global_Report.pdf?utm_source=website&utm_medium=global_report&utm_campaign=downloads

7. Edmonds & Bradley (2015) Mechanical boon: will automation advance Australia?, Available at: https://www.industry.gov.au/sites/g/files/net3906/f/June%202018/document/pdf/mechanical-boon_-_will_automation_advance_australia.pdf

8. Financial Review (2017), Australian Taxation Office looks to the cloud to end crashes as tech exec quits, Available at: https://www.afr.com/technology/cloud-computing/australian-taxation-office-looks-to-the-cloud-to-put-crashes-in-the-past-as-tech-exec-quits-20170907-gycnjs

9. Gartner (2018) Understanding Cloud Adoption in Government, Available at: https://www.gartner.com/smarterwithgartner/understanding-cloud-adoption-in-government/

10. Government Digital Service, UK Government. (2017). Government Cloud First policy. Available at: https://www.gov.uk/guidance/government-cloud-first-policy

11. Government of Canada, (2018), Government of Canada Cloud Adoption Strategy: 2018 update, Available at: https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/cloud-computing/government-canada-cloud-adoption-strategy.html#toc2IDC (2018), Adopting Cloud in Support of Government Digital Agendas: Cloud-Enabled Public Services, Reality Rather Than Fiction.

12. IDC (2018a) IDC Worldwide Semiannual Public Cloud Services Spending Guide, 2018H1.

13. IDC (2018b) CloudView Survey 2018 – Public Sector.

14. IDC (2018c) Adopting Cloud in Support of Government Digital Agendas: Cloud-Enabled Public Services, Reality Rather Than Fiction.

15. IDC (2017) Train to Accelerate Your Cloud Strategy, Available at: https://d1.awsstatic.com/analyst-reports/Train%20to%20Accelerate%20Your%20Cloud%20Strategy.pdf

16. IDC (2016) Federal Government to spend 8.5% of all IT spending on Cloud in FY 2016, according to IDC Government insights, accessed February 2019.

17. IDG Communications (2016) ATO goes mission critical in the public Cloud with AWS, Available at: https://www.arnnet.com.au/article/605468/ato-goes-mission-critical-public-cloud/

18. Mannheim, M (2018), Public service shrinks to smallest size in 12 years, Available at: https://www.smh.com.au/politics/federal/public-service-shrinks-to-smallest-size-in-12-years-20181019-p50ao7.html

19. Office of the US Federal Chief Information Officer, (2018), From Cloud First to Cloud Smart, Available at: https://cloud.cio.gov/strategy/

20. Scanlon Foundation (2018), Social cohesion index, Available at: https://scanlonfoundation.org.au/mapping-social-cohesion/

21. Technology Record (2018) Public cloud services spending forecast to reach US$160 billion in 2018, Available at: http://www.technologyrecord.com/ Art-icle/public-cloud-services-spending-forecast-to-reach-us160-billion-in-2018-62807

22. TEKsystems (2016) "Zombie" Training and Development Programs the Norm for Organizations, Available at: https://www.teksystems.com/en/insights/press/2016/training-and-development-programs

23. Telstra (2018) QBCC embraces the benefits of hybrid cloud, Available at: https://insight.telstra.com.au/optimise-your-it/articles/qbcc-embraces-the-benefits-of-hybrid-cloud

Our people

John O'Mahony
Partner
Deloitte Access Economics

T. +61 2 9322 7877
E. joomahony@deloitte.com.au

Kathryn Matthews
Partner
Deloitte Access Economics

T. +61 2 9322 7605
E. katmatthews@deloitte.com.au

Kevin Russo
Partner
Deloitte Consulting

T. +61 3 9671 6768
E. krusso@deloitte.com.au

Dan Newman
Partner
Deloitte Consulting

T. +61 3 9671 6768
E. dannewman@deloitte.com.au

Michelle Mountford
Associate Director
Deloitte Access Economics

T. +61 2 9322 7146
E. mmountford@deloitte.com.au

Xanthe Smith
Senior Analyst
Deloitte Access Economics

T. +61 3 9322 3792
E. xsmith@deloitte.com.au

Alex Kloeden
Research Analyst
Deloitte Access Economics

T. +61 3 8260 6441
E. akloeden@deloitte.com.au

Limitation
of our work

General use restriction

This report is prepared solely for the use of AWS. This report is not intended to and should not be used or relied upon by anyone else and we accept no duty of care to any other person or entity.

The report has been prepared for the purpose of outlining the context of public sector public cloud and explaining some of the issues to more effective public cloud use. You should not refer to or use our name or the advice for any other purpose.

Deloitte.