What does the new Australian government DTA Secure Cloud Strategy mean for Office 365?

Office 365 and the Secure Cloud Strategy

- Published on February 27, 2018
  https://www.linkedin.com/pulse/office-365-secure-cloud-strategy-aaron-dinnage/

On the 1st of February, 2018, the Australian government Digital Transformation Agency released their Secure Cloud Strategy. In this article I'll be analysing this new strategy from the perspective of Microsoft's Office 365 software as a service platform. I'll also provide my opinion on a number of the principles and initiatives outlined within the strategy.

The Secure Cloud Strategy has a clear intent, to accelerate the adoption of cloud services within Australian government. It makes the case for why that is a worthy goal, and it establishes seven cloud principles to guide that process.

Further, the new strategy details eight initiatives the DTA is undertaking in support of this goal, and busts three common cloud myths along the way.

We'll take a look at all of those elements of the strategy and try to give an *actionable* Office 365 perspective on each one. So let's start with the seven cloud principles…

Cloud Principles

Principle 1: Make risk-based decisions when applying cloud security

Risk-based decision making is not only a hallmark of this new secure cloud strategy, but is a long standing principle of the Australian government Information Security Manual (ISM). I believe the reason we keep hearing so much reiteration of this concept lately is that there is a perception agencies are taking a *box ticking* approach to security and compliance.

Tick the box, move on / don't tick the box, don't move on.

However, it should come as no surprise that agencies are keen to defer to an authority like the ASD when making security and compliance decisions around cloud platforms. The technology is evolving faster than at any time in the past, so making a risk-based determination can be difficult.

How do you perform a risk assessment when you're still trying to **understand** the technology?

Many of the other areas of the Secure Cloud Strategy go towards answering this challenge. For example, knowledge exchange between agencies, building in-house cloud skills, and implementing a layered certification model can all help to address this. But Microsoft customers shouldn't hesitate to reach out to their account team for assistance in performing a risk assessment and getting on with the job.

However, that said, I believe there is another concept that needs to be spoken about in this context:

Trust

Agencies should align themselves with vendors that have demonstrated trustworthiness through a commitment to privacy, transparency, partnership, security, and compliance. There is no public cloud provider in the world that has done more in this space than Microsoft. This is demonstrated through local data centres in Sydney, Melbourne, and Canberra, through investing time and engineering effort in achieving international and local compliance standards, and through fighting for the rights of their customers on the global stage.

Microsoft has built a cloud business on a foundation of trust.

If a service provider isn't displaying these characteristics, isn't fighting for your rights, isn't putting your privacy, your compliance, and your security first, then I would I argue that they cannot be a service provider for Australian government, no matter how big or small they are. Australian government needs a contractual **and** cultural commitment to these ideals, in their absence it is my contention that government should not engage.

For more information on how Microsoft fits this requirement, I'd recommend starting with the Office 365 Trust Center and then take a look at the reports and whitepapers on the Microsoft Service Trust Portal. But don't hesitate to reach out to your Microsoft account team and ask for more information.

Principle 2: Design services for the cloud

In this principle, things get very prescriptive. There are a lot of "must" statements made.

> "… agencies **must** use cloud services for new services or modernisation…"
>
> "Agencies **must** design all new or modernised ICT services as cloud native, or cloud enabled…"
>
> "… agencies **must** design applications to be cloud-ready…"

How should we read this in the context of Office 365? I would say it's conclusive, government agencies cannot continue to incur legacy technology debt, and must move to cloud services, period.

If you're looking at upgrading Exchange server, move to Office 365. If you're looking at deploying a new SharePoint server environment, start in Office 365. And if you feel like an on-premises Skype for Business server farm is needed, you should be building a cloud hybrid at a *minimum*.

Of course, the Office 365 services must be fit for purpose. They need to be appropriate for the sensitivity of your material, and also be appropriate from a functionality level. From a sensitivity perspective, the service is already certified for Unclassified DLM and it's no secret (pun intended) that Microsoft is continuously seeking to improve the certification standing of Office 365.

If you run an Unclassified environment today there is no reason you can't be moving services onto Office 365. If you run a PROTECTED environment today, you should start evaluating Office 365. By performing a threat & risk assessment you may be able to start using the service now. Again, Microsoft can help you with that.

When it comes to functionality, there are a number of situations where a hybrid configuration (some on-premises infrastructure with a balance of load being taken up by the cloud service) is appropriate. In most cases a hybrid implementation is deployed to facilitate migrations, maintain legacy systems, or to enable more exotic configurations. In some cases it is to accommodate a feature that is, to date, missing in the cloud service.

Hybrid is often the first step in a journey to the cloud. The long term plan may be 100% cloud, but in the short term, hybrid means less on-premises infrastructure to maintain. If you're not sure you can move to Office 365 and you'd like to discuss hybrid options talk to a Microsoft Gold Partner or contact your Microsoft account team.

Principle 3: Use public cloud services as the default

Put simply, private clouds don't offer the same value as public clouds, and should be used only if public cloud options can't meet your particular needs.

If you're not moving to public cloud services, you need to be able to explain why.

If you're getting advice that you need a private cloud, it would be worth getting a second opinion to be sure. A private cloud alternative to Office 365 is simply not Office 365. You can host Exchange Server, but you can't deploy a private cloud version of Office 365. Nothing has the same scale, value, integration, or feature richness of Office 365.

What's more, many new Microsoft products are *public cloud only.* Like Teams, Flow, PowerApps, Stream, Yammer, Planner, Sway, MyAnalytics, and StaffHub. These are all Office 365 apps that exist only in Microsoft's *public* cloud.

However, Office 365 is not a perfect fit for every situation, there are a small number of scenarios where Office 365 is the not best option on balance, but you should at least want to be clear on why you're going with private cloud, what it's giving you that Office 365 isn't, and what you're consciously choosing to miss out on.

DTA now expects agencies to have good reasons when they choose not to take up public cloud services.

If you're choosing a private cloud implementation to facilitate customization then take a look at Principle 5.

Principle 4: Use as much of the cloud as possible

The highest return on investment comes from placing as much of a workload, and as many workloads, in Office 365 as possible. There is a lot of capability on offer, so taking advantage of that should be a goal for any agency on this journey.

If you're going to deploy a hybrid with Office 365 then try to put as many users or as much content online as you can. If you're only planning on taking up one Office 365 service, take a look at what else you have access to and plan for more. For example, if you're taking up OneDrive for Business, then consider the amplifying effect on employee productivity of that being integrated with Microsoft Teams and Office 365 ProPlus.

Consider how some features of Office 365 get better or add more value with each component of the service you add, for example:

- Intelligent search and discovery allows users to find data across the entire Office 365 suite, simplifying the end user enterprise search experience.
- Delve surfaces useful content personalised to the individual. The more content and signals that are available to Delve to draw on, the more fine tuned the experience.
- MyAnalytics provides personal productivity analytics to give employees insights into how they are spending their time. This is only useful if sufficient data is sourced from the interactions users are having across the Microsoft ecosystem.
- eDiscovery enables an organization to leverage the same data as the search system to perform investigations and Freedom of Information data gathering with ease.
- Teams just gets better when combined with Exchange Online, Planner, Power BI, and OneDrive for Business. Each of these builds on the user experience within Teams to help users save time and be more productive without leaving the Teams client.

Through integration across the suite, Office 365 is truly greater than the sum of its parts.

Principle 5: Avoid customisation and use services ‘as they come’

Anyone who's been an IT consultant for a good length of time will remember a customer engagement or two that went something like this:

The customer asks for 10 requirements, they can get 8 met straight out of the box, leaving 2 to be custom developed. At the end of the project the two custom requirements took 50% of the project time to deliver and the customer turns around and says "if we knew it would be that hard we would have dropped those requirements, we didn't really need them!"

All requirements should be evaluated on the balance of **total** cost of ownership against the benefit.

In my experience it's very rare for Office 365 to be honestly evaluated and found to have a limitation that breaks the overall value of the proposition.

However, public cloud platforms are generally less flexible than doing it yourself on-premises. Private cloud providers will also often give customers more scope to customize the environment.

The freedom of on-premises and private cloud hosting is a double-edged sword.

Just because you *can* customize an on-premises application doesn't mean you *should*. And just because you did customize that on-premises application in the past doesn't mean customization is a *requirement* of any new platform. I've seen over-customization too many times to count, heck, I've been guilty of it myself! It's very tempting to say yes to every ask when you have a platform that lets you do anything.

Through my journey from being a software developer into IT operations, and subsequently into the vendor side, I've seen first hand the value of sticking with using services 'as they come'. It's one of the main things that first drew me to Office 365.

An 'as it comes' attitude typically delivers platforms that are cheaper and faster to provision, cost less to maintain, are more easily upgraded, are more stable, more secure, and work like people expect them to.

With Office 365 you also get a platform that is always current version, so you're avoiding creating another soon-to-be-legacy application.

Principle 6: Take full advantage of cloud automation practices

The DTA put's this principle very well when they say:

"Automation enables support teams to focus on the more complex requirements that are unique to their business by minimising the effort need to provision, configure, backup, restore, patch, update and deploy services."

It's hard to build on that, except to point out a few opportunities for automation that are available in Office 365 that you may not be aware of:

- Automate tasks and business processes with Microsoft Flow.
- Self-service group management takes the load off IT managing group memberships.
- Self-service password reset makes employees productive again sooner and saves help desk time and money.
- Automatic group based license assignment makes cloud software asset management a breeze.
- Automate user identity security with Azure Identity Protection to keep your users safe (Microsoft 365 feature).
- Automate security operations with Microsoft Cloud App Security and Windows Defender Advanced Threat Protection (Microsoft 365 features).
- Automate eDiscovery drudgery with the technology assisted review features of Advanced eDiscovery.
- Automate report generation and data refreshes with Power BI Pro.
- Automatically create video transcripts and captions with Microsoft Stream.

Principle 7: Monitor the health and usage of cloud services in real time

Like the automation principle above, the principle of monitoring your cloud services is also readily achieved with Office 365. There are a number of monitoring options you may not have considered, so it's worth referring to this handy article on Office 365 tools for security investigations.

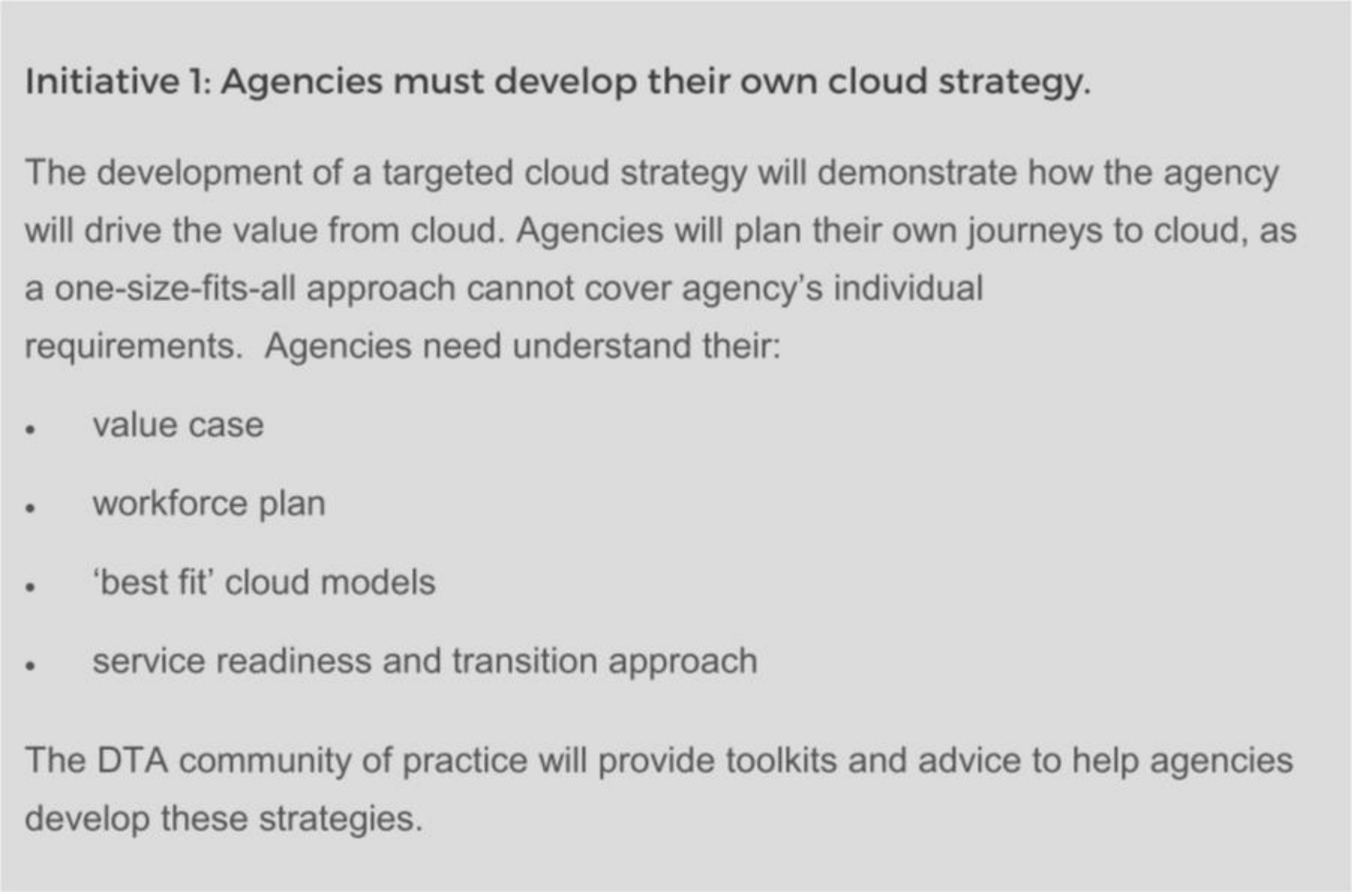
As above, I'd again suggest looking at how you can enhance your security operations with Microsoft Cloud App Security and Windows Defender Advanced Threat Protection (Microsoft 365 features).

This principle is also nicely aligned with the updated ISM controls from November, 2017, which calls out the need to *actively* monitor. I've written a walkthrough of the recent changes to the ISM controls from a Microsoft 365 perspective.

Initiatives

In addition to the cloud principles, DTA has outlined eight initiatives it is undertaking to help government agencies in their cloud journey. Let's now take a look at how these initiatives might relate to Office 365…

Initiative 1: Agencies must develop their own cloud strategy



Initiative 1: Agencies must develop their own cloud strategy.

The development of a targeted cloud strategy will demonstrate how the agency will drive the value from cloud. Agencies will plan their own journeys to cloud, as a one-size-fits-all approach cannot cover agency’s individual requirements. Agencies need understand their:

- value case
- workforce plan
- ‘best fit’ cloud models
- service readiness and transition approach

The DTA community of practice will provide toolkits and advice to help agencies develop these strategies.

It has been my experience, and that of my colleagues, that when an agency starts on the journey to cloud services without a cohesive cloud strategy they find internal forces pulling in different and occasionally opposing directions.

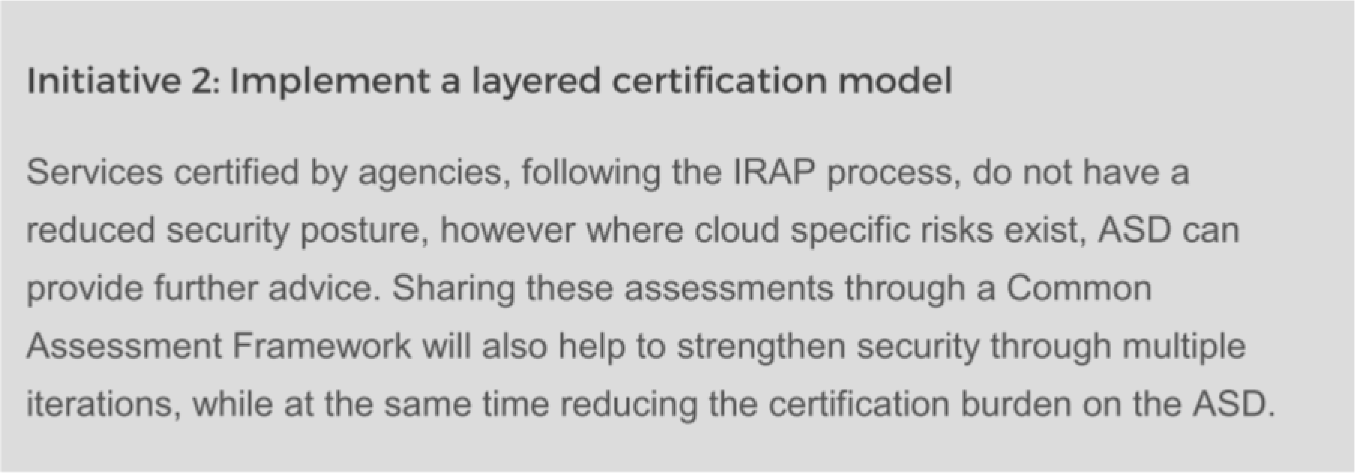
A cloud strategy aligns the organisation around a common vision and understanding.

This is in no way specific or peculiar to Office 365, but Office 365 by it's nature as a collection of various products and services does require different parts of an organization to collaborate on the journey. For example, to successfully implement Exchange Online you must address identity, networking, desktop and mobile devices, security, compliance, retention, and archiving requirements. It's hard to do that without a strategy to rally and align around.

Office 365 will require collaboration and consultation across the breadth of an organization. A cloud strategy helps enable this through the definition of common goals, common language, and common interest. Without a cloud strategy every one of those collaborations and consultations is open to objections, dissenting views, and delays.

A meaningful cloud strategy is now a critical policy that every agency must have.

Initiative 2: Implement a layered certification model



Initiative 2: Implement a layered certification model

Services certified by agencies, following the IRAP process, do not have a reduced security posture, however where cloud specific risks exist, ASD can provide further advice. Sharing these assessments through a Common Assessment Framework will also help to strengthen security through multiple iterations, while at the same time reducing the certification burden on the ASD.

This initiative is founded on the idea that agencies could be performing their own assessments and then using cloud services ahead of a formal certification by ASD. The DTA is encouraging agencies to share those findings across government to make it easier for others to take up cloud services too.

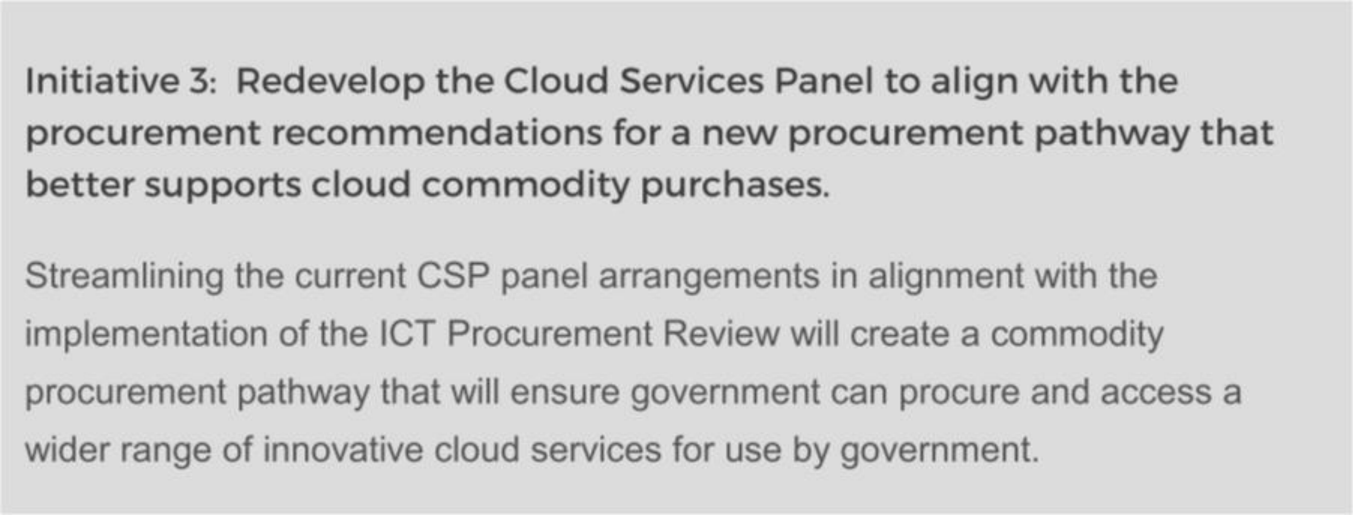
Whilst it's been the case for some time now that an agency can act independently of ASD to accept the risks of taking up a particular cloud service, most agencies are reluctant to do so. This speaks to the first of the Cloud Principles, that of making risk-based decisions in cloud security. It's difficult.

I believe that a common assessment framework, like the one being proposed by DTA would help agencies with a less risk averse culture to take up cloud services not currently on the ASD Certified Cloud Services List (CCSL).

However, I personally doubt this would be sufficient to encourage an agency to use an Unclassified DLM certified service, like Office 365, for PROTECTED classified workloads. I believe that will still need ASD certification to get the majority of government organizations over the line.

The possible downside to this approach is that agencies might share flawed assessments of unsecure and non-compliant cloud services and their usage increases as well. We could see currently uncertified cloud services deemed acceptable when in fact they don't make the grade. There will be a role here for the group to check each-others homework, so to speak.

Initiative 3: Redevelop the Cloud Services Panel to align with the procurement recommendations for a new procurement pathway that better supports cloud commodity purchases



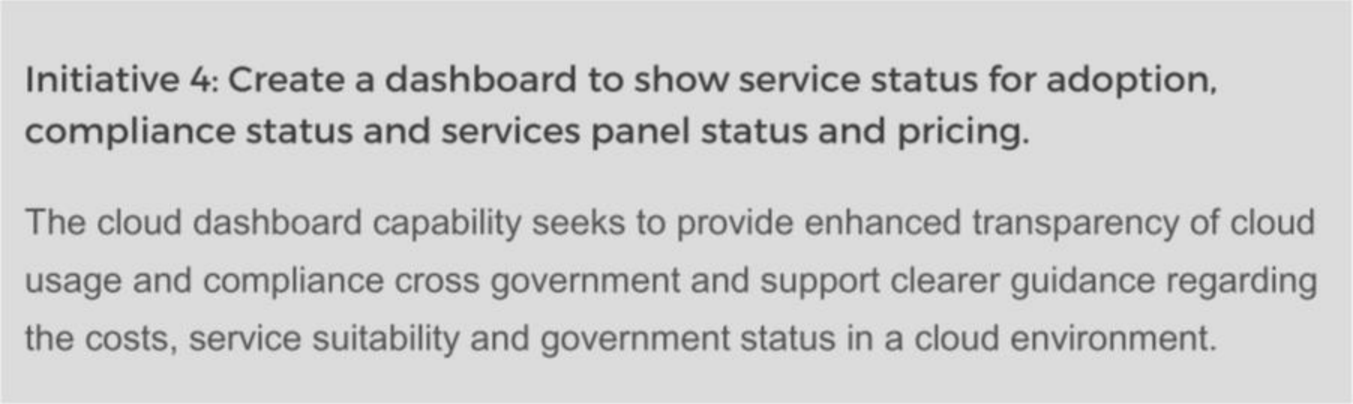
Initiative 3: Redevelop the Cloud Services Panel to align with the procurement recommendations for a new procurement pathway that better supports cloud commodity purchases.

Streamlining the current CSP panel arrangements in alignment with the implementation of the ICT Procurement Review will create a commodity procurement pathway that will ensure government can procure and access a wider range of innovative cloud services for use by government.

Microsoft software as a service offerings, such as Office 365, are already well catered for under the Volume Sourcing Agreement between Microsoft and Australian government, this agreement is controlled today by the DTA themselves.

I can't speak to the experience of other vendors or from the perspective of agencies, so I won't comment any further on this initiative.

Initiative 4: Create a dashboard to show service status for adoption, compliance status and services panel status and pricing

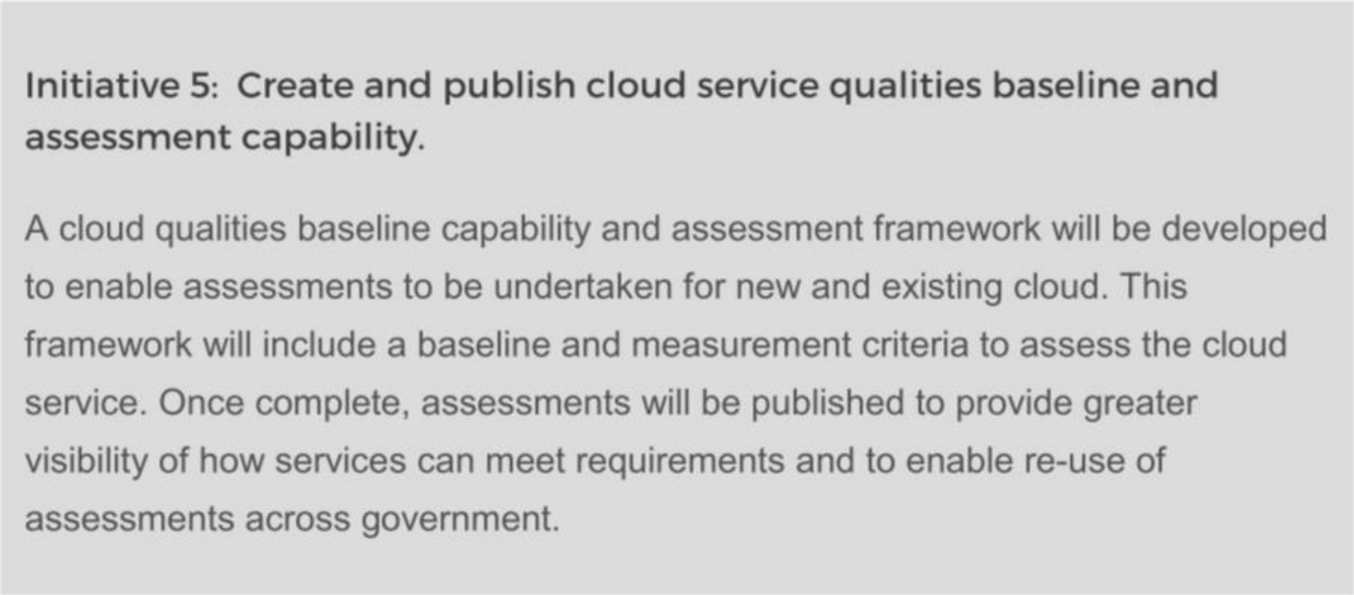


Initiative 4: Create a dashboard to show service status for adoption, compliance status and services panel status and pricing.

The cloud dashboard capability seeks to provide enhanced transparency of cloud usage and compliance cross government and support clearer guidance regarding the costs, service suitability and government status in a cloud environment.

Microsoft cloud services compliance is already represented on the ASD CCSL, and panel status and pricing for Office 365 are already accessible across government. So for the same reason that I can't comment any further on Initiative 3, I've got nothing to add on Initiative 4.

Initiative 5: Create and publish cloud service qualities baseline and assessment capability



Initiative 5: Create and publish cloud service qualities baseline and assessment capability.

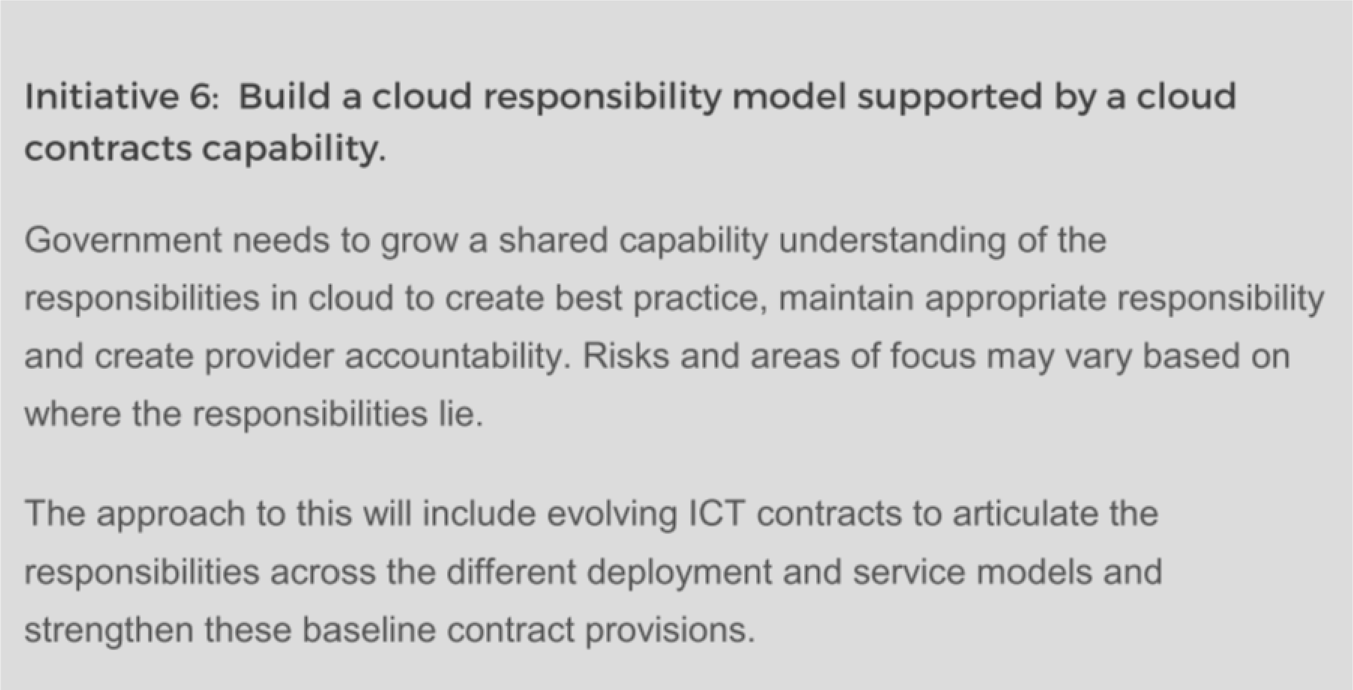
A cloud qualities baseline capability and assessment framework will be developed to enable assessments to be undertaken for new and existing cloud. This framework will include a baseline and measurement criteria to assess the cloud service. Once complete, assessments will be published to provide greater visibility of how services can meet requirements and to enable re-use of assessments across government.

Sharing threat and risk assessments across government could lead to greater take-up of cloud services by government. However, I believe there will be a chicken-and-egg dilemma as agencies wait for other agencies to generate and share assessments.

Perhaps there is a role for DTA to play in sourcing, performing, or funding those assessments? However, at that point it would seem like a *de facto* IRAP / CCSL alternative, with all of the same challenges.

I'm keen to learn more about how this initiative would operate. So please do sound off in the comments if you have a view on this one.

Initiative 6: Build a cloud responsibility model supported by a cloud contracts capability



Initiative 6: Build a cloud responsibility model supported by a cloud contracts capability.

Government needs to grow a shared capability understanding of the responsibilities in cloud to create best practice, maintain appropriate responsibility and create provider accountability. Risks and areas of focus may vary based on where the responsibilities lie.

The approach to this will include evolving ICT contracts to articulate the responsibilities across the different deployment and service models and strengthen these baseline contract provisions.

This initiative certainly seeks to clarify, and perhaps to standardize, the responsibility matrix across cloud vendors. But cloud is a complex, moving feast of rapid innovation and providers always seeking to differentiate themselves from their competition.

If kept to the more modest ambition of developing a responsibilities matrix for common services, like Office 365, then this could have real benefit. Beyond that I believe it's quite ambitious.

Initiative 7: Establish a whole-of-government cloud knowledge exchange

Initiative 7: Establish a whole-of-government cloud knowledge exchange

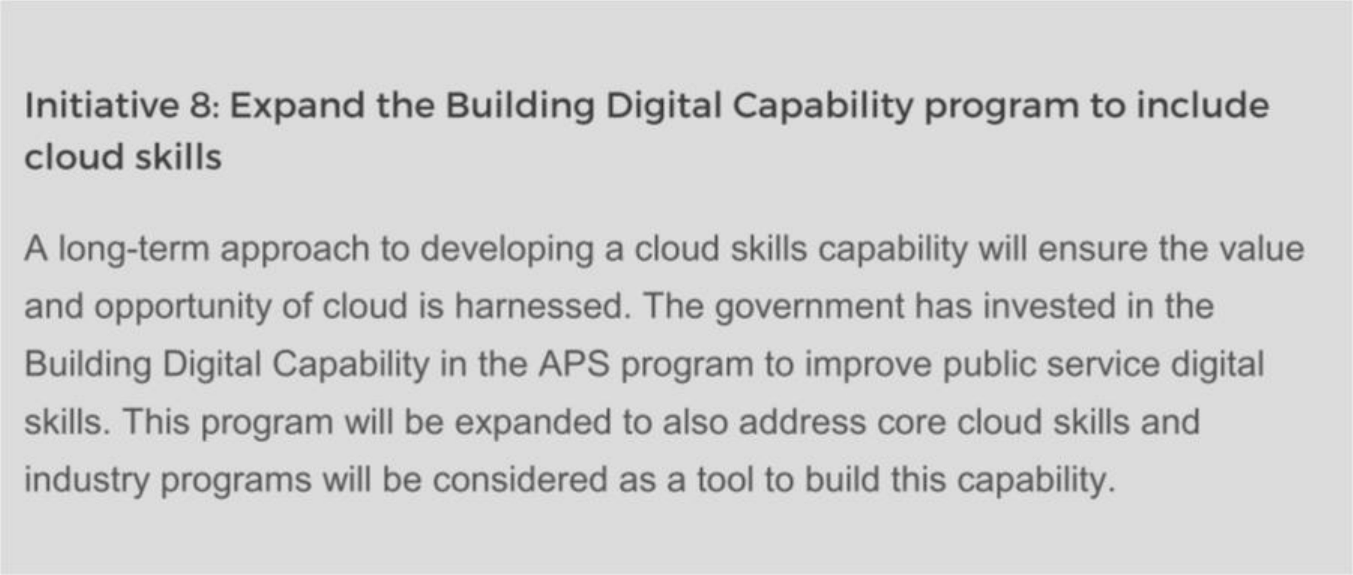
Deliver a platform for agencies to better collaborate and reuse common capabilities for their cloud adoption and use. Development of the platform will consider how users will interact with the service, accessibility, governance, operations and technology.

As agencies learn and upskill around cloud technologies I believe government agencies will need to share knowledge, intellectual property, and learnings to help their fellow agencies accelerate their success in cloud adoption.

From my own work with Australian Government, I believe this is already starting to happen organically. So DTA support can only be of benefit here.

I think a knowledge sharing *forum* would be a fantastic start. Keeping in mind that cloud knowledge goes stale faster than traditional IT knowledge, so it will be important not to put too much value in curating a collection of aging information.

Initiative 8: Expand the Building Digital Capability program to include cloud skills



Initiative 8: Expand the Building Digital Capability program to include cloud skills

A long-term approach to developing a cloud skills capability will ensure the value and opportunity of cloud is harnessed. The government has invested in the Building Digital Capability in the APS program to improve public service digital skills. This program will be expanded to also address core cloud skills and industry programs will be considered as a tool to build this capability.

This aligns well with Microsoft's National Skills Program recently launched in Adelaide. And in the UK, Microsoft is providing free digital skills training for public sector workers. I don't speak for Microsoft on this, but a collaboration between Australian Government and Microsoft seems like a good fit for APS.

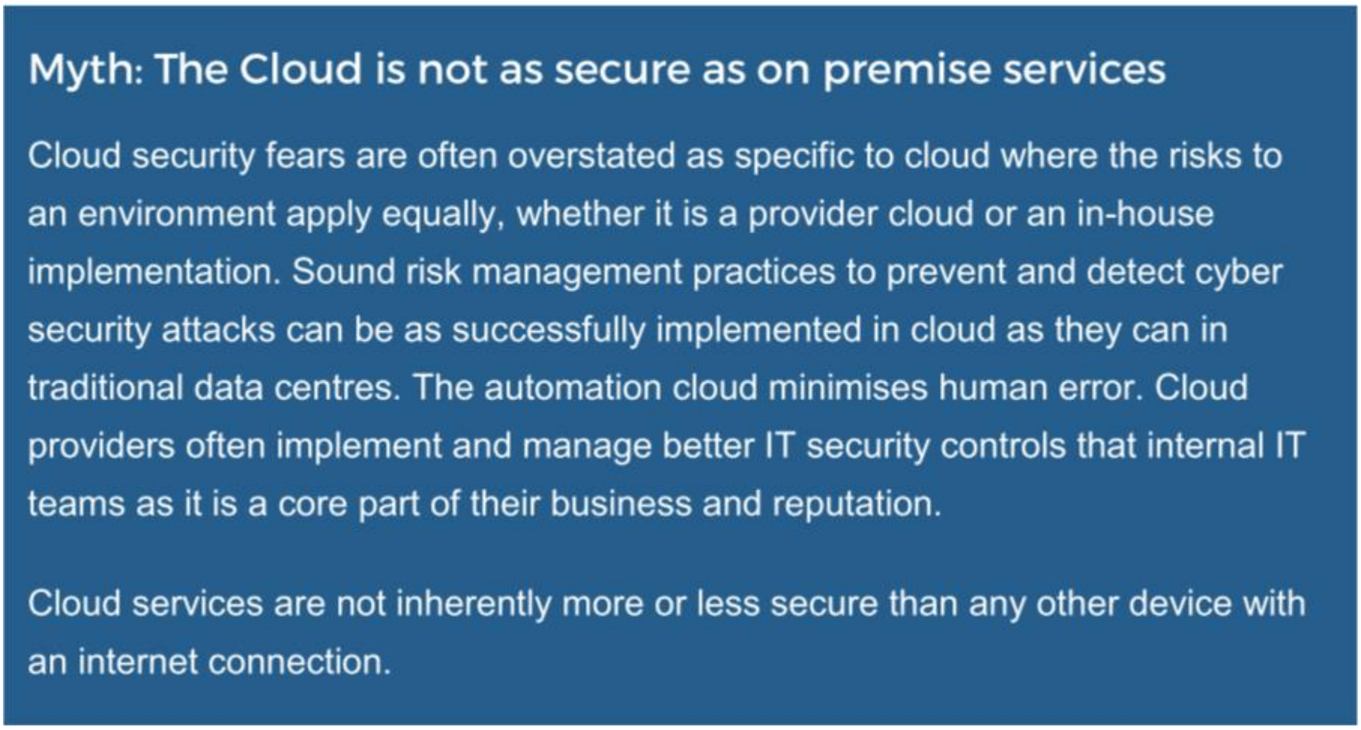
More immediately, Microsoft has a large amount of online training available on Office 365 which can be accessed 24/7 on the following platforms:

- Office 365 Training Center
- Microsoft Virtual Academy

There are certainly cloud skills that APS staff would benefit from. Additionally, a cultural shift to continuous learning will be needed to ensure ongoing success.

Myths

Myth 1: The Cloud is not as secure as on premise services



Myth: The Cloud is not as secure as on premise services

Cloud security fears are often overstated as specific to cloud where the risks to an environment apply equally, whether it is a provider cloud or an in-house implementation. Sound risk management practices to prevent and detect cyber security attacks can be as successfully implemented in cloud as they can in traditional data centres. The automation cloud minimises human error. Cloud providers often implement and manage better IT security controls that internal IT teams as it is a core part of their business and reputation.

Cloud services are not inherently more or less secure than any other device with an internet connection.

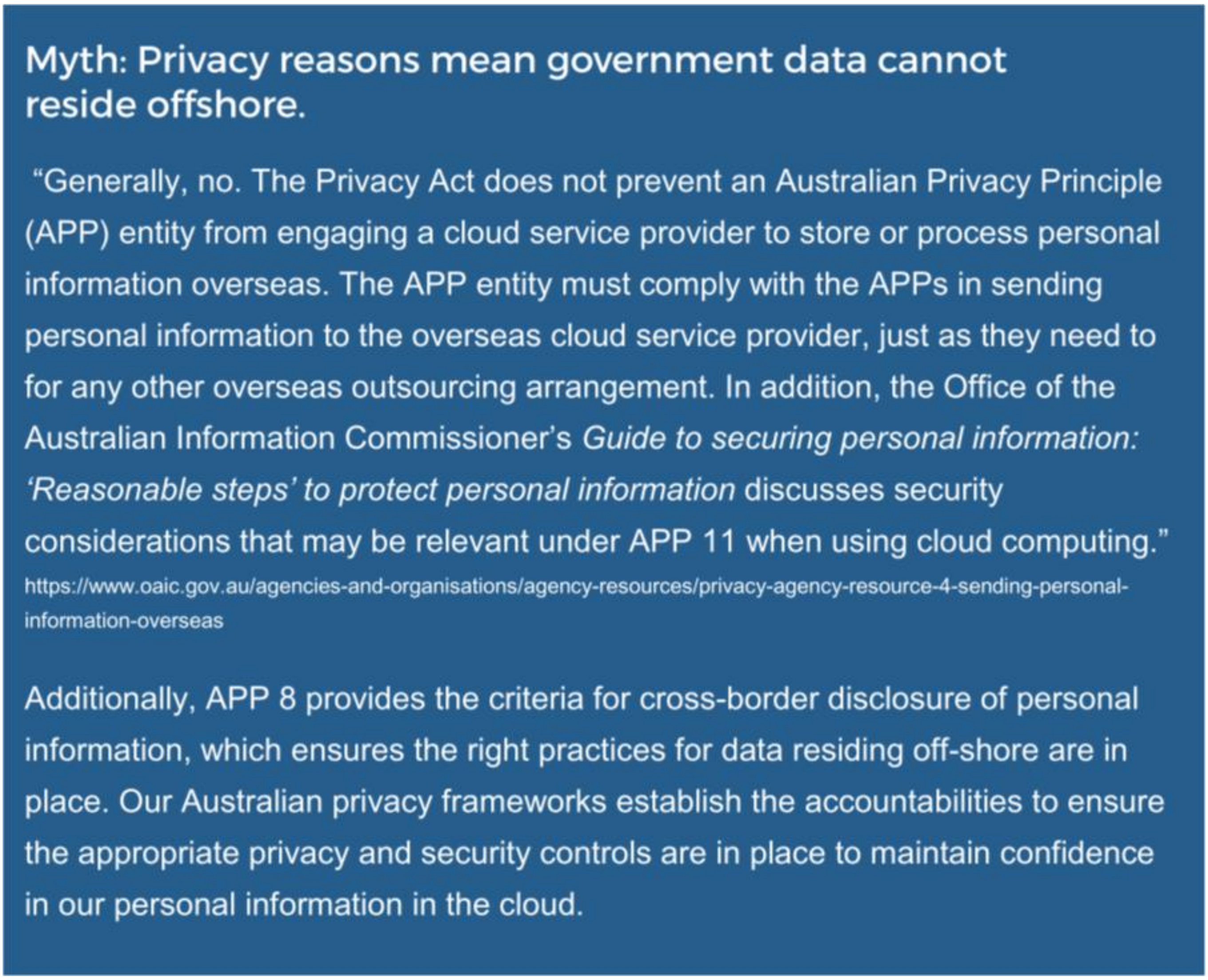
The problem is that the term 'cloud' is almost meaningless when used to describe anything other than a pool of resources being provided by a third party. When we address a specific cloud provider we can start to make more interesting statements. For example, the Microsoft cloud is a more secure platform than most on-premises or hosted alternatives.

No customer moves to a cloud service they think is **less** secure

It takes time to demonstrate and describe the depth of security features present in Office 365, but over time customers develop a greater understanding and trust in the platform.

Part of that understanding is around how to configure Office 365 to be more secure. It's not enough to simply turn it on and use it, an organization must configure the service to meet their particular needs. When they do this, they have a service that will be at least as secure, and often more secure, than they have had before.

Myth 2: Privacy reasons mean government data cannot reside offshore.



Myth: Privacy reasons mean government data cannot reside offshore.

"Generally, no. The Privacy Act does not prevent an Australian Privacy Principle (APP) entity from engaging a cloud service provider to store or process personal information overseas. The APP entity must comply with the APPs in sending personal information to the overseas cloud service provider, just as they need to for any other overseas outsourcing arrangement. In addition, the Office of the Australian Information Commissioner's *Guide to securing personal information: 'Reasonable steps' to protect personal information* discusses security considerations that may be relevant under APP 11 when using cloud computing."

https://www.oaic.gov.au/agencies-and-organisations/agency-resources/privacy-agency-resource-4-sending-personal-information-overseas

Additionally, APP 8 provides the criteria for cross-border disclosure of personal information, which ensures the right practices for data residing off-shore are in place. Our Australian privacy frameworks establish the accountabilities to ensure the appropriate privacy and security controls are in place to maintain confidence in our personal information in the cloud.

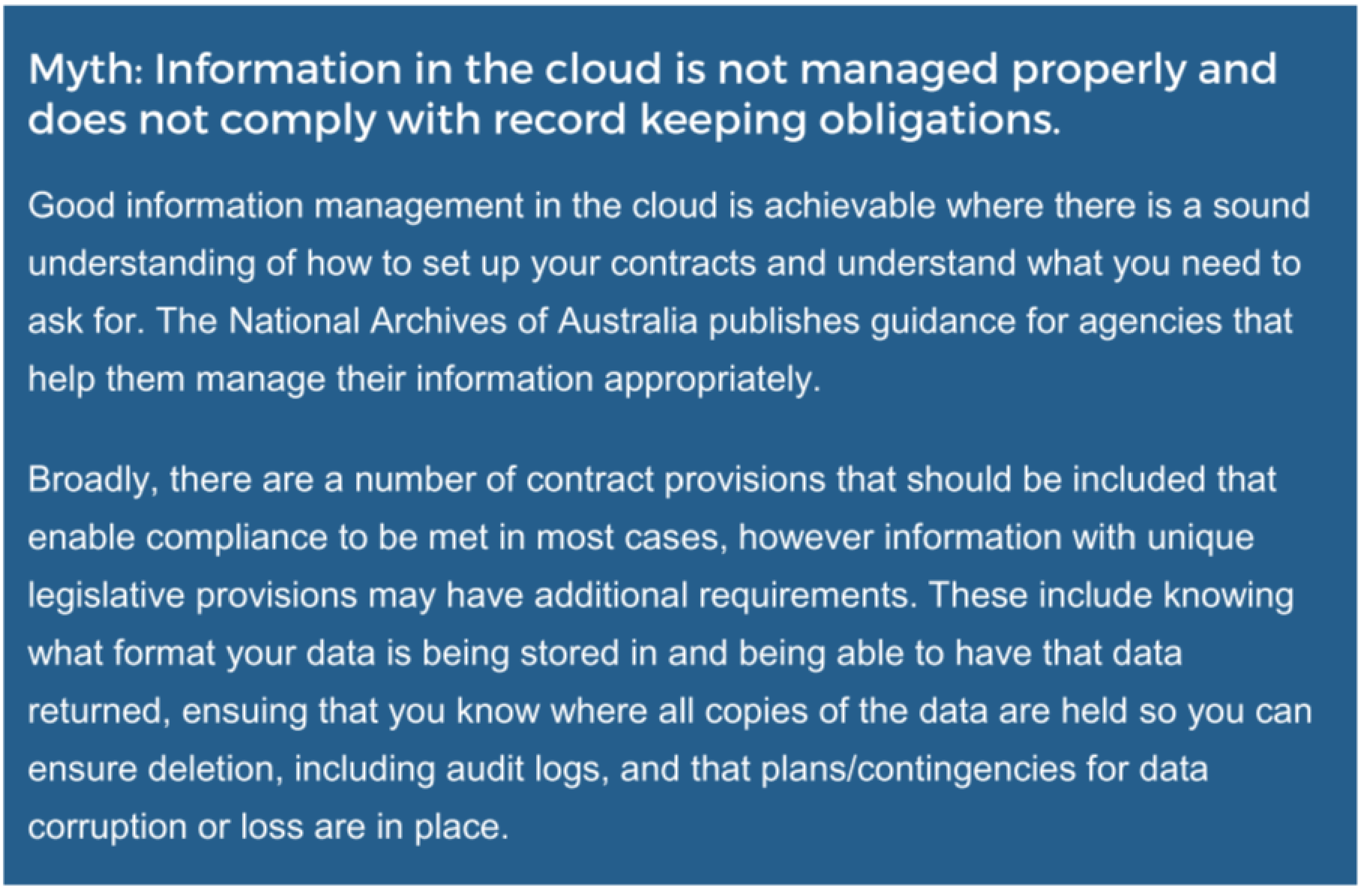
This is perhaps one of the most persistent myths in government today. And unfortunately, because there are a small number of legitimate circumstances where data cannot leave the country most agencies seem to assume their data can't.

The important thing here is for government agencies to get advice they can rely on about their particular regulatory and legislative requirements.

It's worth considering also that simply being on-shore doesn't guarantee security and compliance. There are other vendor's cloud services delivered on-shore in Australia that have lesser security & compliance than Microsoft cloud services delivered out of the United States, Singapore, or Hong Kong. More importantly, Microsoft will protect and fight for the privacy of their customers regardless of where the customers data is stored.

Microsoft customers should familiarise themselves with the Office 365 service locations, and consider using tools like Microsoft Cloud App Discovery to evaluate 3rd party services for security, risk, and compliance, and with Microsoft Cloud App Security, take control of them.

Myth 3: Information in the cloud is not managed properly and does not comply with record keeping obligations



Myth: Information in the cloud is not managed properly and does not comply with record keeping obligations.

Good information management in the cloud is achievable where there is a sound understanding of how to set up your contracts and understand what you need to ask for. The National Archives of Australia publishes guidance for agencies that help them manage their information appropriately.

Broadly, there are a number of contract provisions that should be included that enable compliance to be met in most cases, however information with unique legislative provisions may have additional requirements. These include knowing what format your data is being stored in and being able to have that data returned, ensuing that you know where all copies of the data are held so you can ensure deletion, including audit logs, and that plans/contingencies for data corruption or loss are in place.

Office 365 can be configured to broadly meet the requirements for records management in Australian government. In fact, 3rd party and customer assessments have shown that SharePoint, for example, can meet the vast majority of the ISO 16175 standard.

There are a number of case studies on the National Archives website that highlight government organisations that have successfully implemented records management solutions on top of SharePoint:

- Department of Industry, Innovation & Science
- Federal Court of Australia
- Australian Trade and Investment Commission

Additionally, many of the 3rd party records management solutions in the market today integrate with Office 365. Which is to say that a government agency can meet their record keeping obligations and use Office 365, whether they want to take on the configuration of the service to their needs, or rely on a specialised 3rd party tool to assist.

Records management is a specialised topic, you can get appreciation for this by perusing the relevant legislation, so it's worth engaging with a specialist in the space. However, you can certainly be confident that records management obligations are no reason to avoid Office 365.

Conclusion

The Secure Cloud Strategy is great step in the right direction. The Cloud Principles in particular are very solid. In my opinion, this is **good work**. And calling out some of the myths is also a valuable contribution to the conversation. Whilst I believe there is value in a number of the initiatives, particularly around cloud strategies and digital skills, I worry that some of the other initiatives are very ambitious. But the DTA is not their to be unambitious, so kudos to them for getting on the front foot.

I'm quite keen to see how some of these initiatives play out, the layered certification model in particular is something I'll be eager to get more detail on. But if the initiatives spark more thoughtful cloud conversations across government then that in itself will be a positive outcome.

At the end of the day if just the Cloud Principles are taken seriously by government agencies, the Secure Cloud Strategy will have made a substantial impact.

All in all, Office 365 has once again fared very well. In light of the principles, the myth busting, and the initiatives under way, it is clear why Office 365 remains a strategically sound and compelling choice for government agencies in their cloud journey.

You may have noticed a number of references to Microsoft 365 throughout this article, which I've written up a detailed explanation of in Unpacking Microsoft 365. In the context of Office 365, Microsoft 365 adds Enterprise Mobility + Security which is a broad package of solutions that can assist government to meet their security and compliance requirements. EM+S is not only applicable for Office 365 but also for other SaaS solutions, and even PC and Mobile Device Management. Microsoft 365 also includes Windows Enterprise licensing.

Given the complementary nature of Office 365, Windows, and EM+S, Microsoft decided to create a suite that included them all, hence Microsoft 365. For any organisation that has deployed Windows on the desktop and is looking to move to Office 365, Microsoft 365 is worth considering.