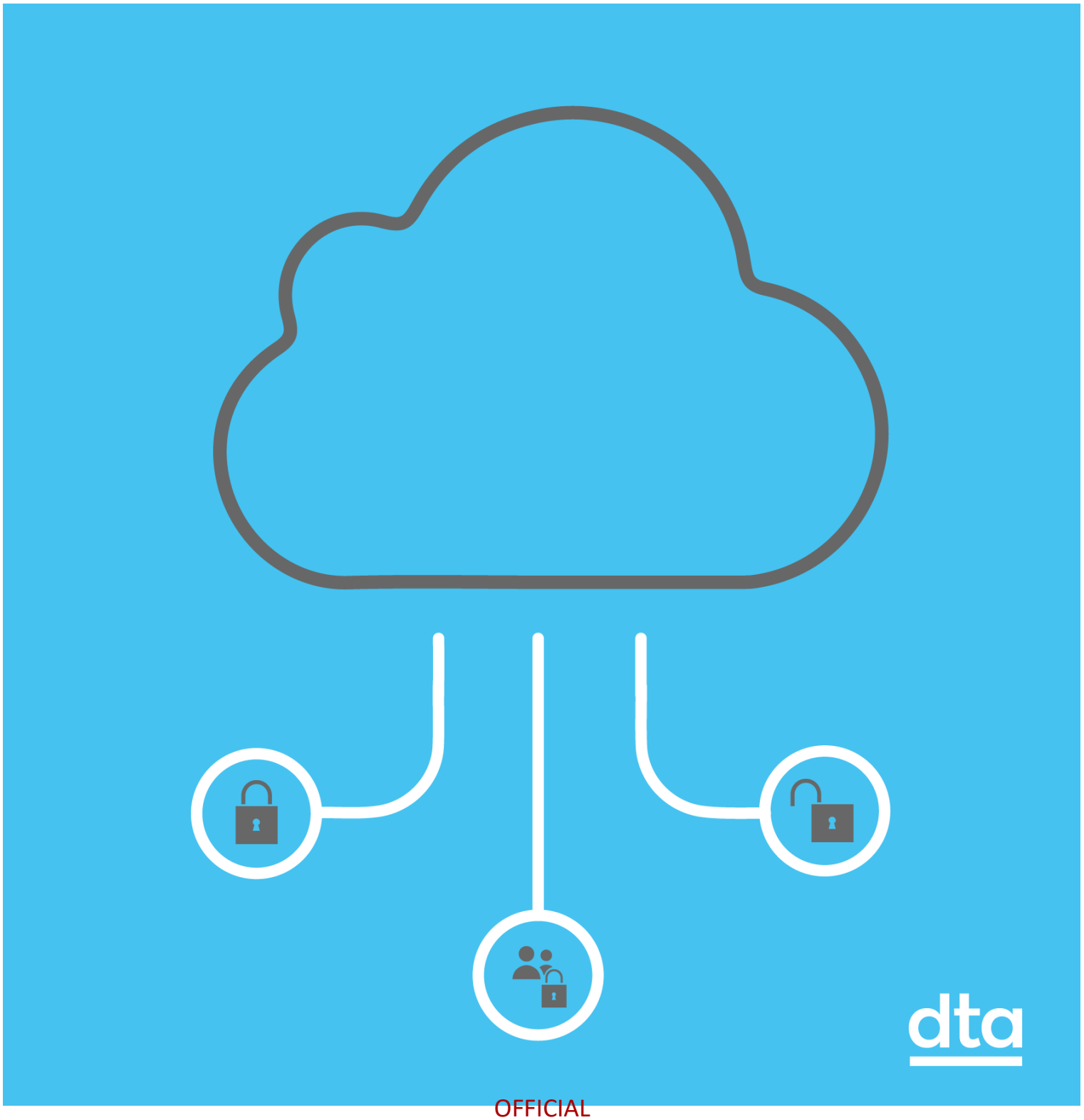
Australian Government
Digital Transformation Agency

Secure Cloud Strategy



dta

Digital Transformation Agency

Version: 2110

Contents

1 Executive summary

The case for cloud is no secret to industry or government. A move to cloud computing - away from on premise owned and operated infrastructure - can generate a faster pace of delivery, continuous improvement cycles and broad access to services. It can reduce the amount of maintenance effort required to ‘keep the lights on’ and refocus that effort into improving service delivery.

Cloud, however, is a way of sourcing Information Communication and Technology (ICT) services and many agencies will have to change the way they operate to make the most of this new model. In the Australian Government, a number of factors can get in the way of agencies realising their cloud aspirations, from a shortage of knowledge and experience, decades old, stubborn operating models and a struggle to sell the case for cloud across the business.

The Secure Cloud Strategy has been developed to guide agencies past these obstacles and make sure everyone has the opportunity to make the most of what cloud has to offer. This is not a simplistic ‘lift and shift’ view of the transition. Instead, the strategy aims to lay the foundations for sustainable change, seizing opportunities to reduce duplication, enhance collaboration, improve responsiveness and increase innovation across the Australian Public Service.

Some agencies have already embraced a cloud model. A coordinated approach for further adoption will make sure government derives the maximum value from this shift. The strategy will ensure experience and expertise is not locked-up and create opportunities to reuse and share capabilities through increased collaboration.

The strategy is based around a number of key initiatives designed to prepare agencies for the shift to cloud and support them through the transition:

- Agencies will develop their own **cloud strategies**. There is no one-size-fits-all approach to implementing cloud. Agencies will use the Secure Cloud Strategy as a starting point to produce their own value case, workforce plan, best-fit cloud model and service readiness assessment.

- Cloud implementation need to be guided by **seven key Cloud Principles**:
  - make risk-based decisions when applying cloud security
  - design services for the cloud
  - use public cloud services by default
  - use as much of the cloud as possible
  - avoid customisation and use cloud services as they come
  - take full advantage of cloud automation practices,
  - monitor the health and usage of cloud services in real time.
- **A layered Cloud Certification Model** will be created. The certification model creates greater opportunity for agency-led certifications, where agencies can certify using the practices already in place for certification of ICT systems.
- **Service procurement** will be aligned with the ICT Procurement Review Recommendations. As cloud services move more rapidly than services available through panels traditionally do, the recommendations in the ICT Procurement Review align well with creating a better pathway for cloud procurement.
- **A cloud qualities baseline and assessment framework** will be introduced to clarify cloud requirements. The cloud qualities baseline capability and assessment framework will enable reuse of assessments.
- **A Cloud Responsibility Model** will be developed to clarify responsibilities and accountabilities. Traditional head agreements cannot cover all cloud services and their frequent variations. A shared capability for understanding responsibilities, supported by contracts, will address unique cloud risks, follow best practice and maintain provider accountability.
- **A cloud knowledge collaboration platform** will be built. The platform will enable secure sharing of cloud service assessments, technical blueprints and other agency cloud expertise, to iterate on work already done rather than duplicating it.

- **Cloud skills uplift programs** will be designed. Increase government skills and competencies for cloud aligned with the Australian Public Service Commission Digital Skills Capability Program and create the pathways to leverage industry programs to enhance cloud-specific skills in the Australian Public Service.
- **Common shared platforms** and capabilities could be explored including:
  - Federated identity for government to enable better collaboration in the cloud.
  - A platform for PROTECTED information management to reduce enclaves in agencies, and continue to iterate cloud.gov.au as an exemplar platform.

    The cloud.gov.au platform has been decommissioned by the DTA no longer provides whole-of-government certified cloud services.

  - Service Management Integrations services to enable agencies to manage multi provider services.

These platforms will include the integration toolkits that enable agencies to seamlessly transition between the cloud services.

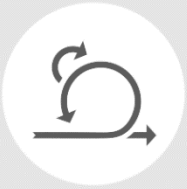
These initiatives will be supported through a Digital Transformation Agency-led community of practice that will support agencies to plan and transition their environments for cloud. It will include delivering training and advice to agencies to build confidence in their ability to manage cloud services.

The Australian Government has an ambitious agenda to transform its digital service delivery. Cloud offers reusable digital platforms at a lower cost, and shifts service delivery to a faster, more reliable digital channel. Cloud services have the opportunity to make government more responsive, convenient, available and user-focused.

2 The case for cloud

Cloud has increasingly become the new industry standard for how technology is delivered to support digital service delivery. Cloud computing provides a commodity service for government, underpinned by a dynamically growing marketplace, which can increase the agility, flexibility and speed of delivery for digital services. It removes the big upfront investments in technology to enable scaling up or down quickly. This provides much needed flexibility and the ability to respond to changing demands. It has the potential to enhance collaboration, limiting the duplication of solutions and reducing the amount of maintenance effort required to 'keep the lights on'. This allows agencies to refocus that effort into improving digital service delivery.

Cloud is not a new concept for government - many agencies are already embracing the cloud to drive better business outcomes. Cloud delivers value to agencies through increased business agility, operational effectiveness and improve visibility across business services and ICT investments. The use of cloud technologies and techniques in ICT delivery provides the agility, flexibility, scalability and robustness required to operate in a digital environment. Understanding how the shift to cloud will deliver the most value for the government and its citizens is important so the right investments in cloud are made.



Agility

Cloud allows business areas to rapidly tune their resource usage based on demand, and eliminate the lead times that delay delivery.

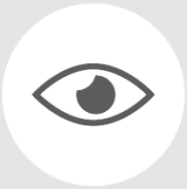
Businesses using cloud can leverage the latest technology innovations in the market as soon as they become available, enabling experimentation without big upfront investments.

Operational effectiveness

Cloud services improve operational effectiveness through increasing availability and freeing up resources to focus on business delivery rather than maintenance.

Right sized infrastructure reduces costs for maintaining idle resources.

Cloud automation allows services to quickly restore after a failure and scale capacity up or down to meet demand.



Visibility

Real-time monitoring of cloud services provides a clear picture of the health and status of the environments, and can be used to drive behaviour accordingly.

Running services in the cloud makes our services more visible. It increases options for the delivery services with low risk profiles, and applies greater focus and assurances around higher value information.

2.1 The opportunity

The government has the opportunity to harness the investment and transformational potential of cloud to enable:

- Whole-of-government efficiencies: Reduce the cost of developing and maintaining technology and reduce the duplication of capabilities across government.
- Interoperability: Efficiently manage information across agencies and classifications including between the PROTECTED and OFFICIAL:DLM domains where appropriate.
- A capability uplift: Enable agencies to share and collaborate to reduce unnecessary duplication of ICT investment, or repetition of procurement and development processes.
- Competition: Drive efficiencies through competition in a wide marketplace that enables government to easily move services between competitive and innovative offerings.

Figure 1—Cloud Appetite Opportunities

In order to build capability, agencies should begin their cloud journeys with low complexity services, and progressively mature their approach.

Low complexity services are already being moved to the cloud. These services often do not contain any sensitive data, making rapid transition to cloud more straightforward.

Medium complexity services will require some additional planning and migration effort for agencies but are often common services offered by the market (not bespoke).

High complexity services are often legacy services and can be the most difficult and expensive to move to cloud. These are often bespoke, and can hold significant volumes of sensitive data.

2.2 Where we want to be

The government has identified digital transformation and innovation as crucial to Australia's economic prosperity. Australians are strong adopters of technology and digital channels offer access to services in a manner that is easier, faster and cheaper. At the same time, government needs to make the most effective and efficient use of its resources. Cloud has the opportunity to provide:

- Technology, skills and support that enables the digital transformation of agencies.
- Cross agency collaboration and knowledge sharing to avoid reinventing the wheel.
- Robust, secure, resilient and agile technologies that are easier to consume than to create.
- Access to innovations from a broad range of commercial providers.

2.3 What is stopping us?

Many Australian government agencies are adopting cloud services to facilitate digital transformation. However, feedback from agencies highlights that this is not a quick or simple task. There are a number of barriers to agencies realising their cloud aspirations, such as a lack of knowledge and skills, or decades old operating models that are difficult to change.

Discovery research (2017) revealed:

- There isn't a common understanding of cloud for government.
- Government's approach to cloud is siloed rather than collaborative.
- There is no confidence in how to meet compliance obligations.
- Government approaches don't fit cloud models.

- Cloud adoption may increase short term costs.
- The skills needed to harness the cloud opportunity are not wide-spread.
- Government applications and services are not ready for cloud.

These barriers highlight a significant knowledge and capability gap that must be addressed to realise the government's cloud aspirations.

2.4 Industry barriers

The cloud market is growing at a rapid pace. A viable marketplace of services, equipped to meet the needs of government, is critical to enable government to become more agile and innovative, and to keep technologies and business processes up to date. Therefore the strategy must also address the barriers confronting industry. It also must ensure the Australian Government’s security and accountability posture is maintained, while also providing incentives for investment in the Australian cloud market.

During Discovery (2017), industry raised a number of issues including:

- Australian Government certification practices require significant investment, both in time and dollars, with a significant gap between the initial investment and any return being realised.
- The Cloud Services Panel fails to keep up with the rapid release of cloud offerings.
- Cumbersome ICT contract head agreements that do not align well with the features, flexibility or nuance of cloud.
- There is no standardised way for agencies to compare services for both functionality and cost.
- Funding models that drive agencies to consider purchasing cloud using Capital Expenditure (CapEX) which do not align with the service model of the cloud.

The secure cloud capability seeks to address some of these concerns. Whilst certifications will always be important for maintaining the integrity and confidentiality of government and citizen information, clarification of certification and accreditation accountabilities is needed. The development of a streamlined, transparent process to

reduce bottlenecks will increase government responsiveness. The introduction of frameworks in the strategy will provide greater clarity for industry, about not only the government's appetite for cloud, but also how government wants to use cloud.

Initiatives in the strategy will support agencies by building capability and reducing the duplication through shared assessments. They will enable faster implementations through collaboration and reuse which will reduce the siloed and sometimes fragmented approaches of government. The creation of new procurement approaches will enable a better pathway for cloud procurement and increase the opportunity for new markets with innovative and small-scale cloud services to be available to government.

3 The strategy

Assurance for citizens and agencies that their information and data stored in the cloud is secure, accurate and reliable is fundamental. Effective government cannot operate without such an assurance.

The cloud marketplace continually grows with rapid innovation cycles of high value, high volume services. This pace is new for government and requires different approaches to choosing, assessing, transitioning, comparing and collaborating on ICT services. Confidence of government and citizens in the ability of cloud services to protect and manage government information must also be maintained. This can be achieved through the development of a secure and compliant cloud capability.

This secure cloud capability for government is not a whole-of-government cloud platform. Instead, it is the competency government needs to use cloud in a way that maintains confidentiality, integrity and availability for critical government systems across all cloud deployment and service models.

The Secure Cloud Strategy identifies the building blocks that will enable agencies to adopt cloud-based services, while continuing to meet the government's security and assurance needs. It sets a pathway for government use of cloud services in a secure way through:

- The development of practical guidance to help agencies develop the knowledge, skills and ability to choose, secure, adopt and manage cloud-based services
- The creation of frameworks that enable a better understanding of, and ability to apply, appropriate risk and information management practices to services in a cloud environment
- Identifying ways to reduce duplication across government.

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.

3.1 Setting the cloud context for government

To ensure the right opportunities for cloud are harnessed across government a common understanding of the offerings, capabilities and benefits of cloud are needed. This can be achieved through defining the common principles for cloud adoption in government and creating individual agency visions that align with the principles.

3.1.1 Guidance community

Agencies require access to practical, implementable guidance to support the development of their cloud strategies. Leading agencies have developed guidance material that can be reused by other entities. A community of practice, led by the Digital Transformation Agency, will establish a culture of collaboration and facilitate the sharing of this sort of advice. This guidance material will support agencies to prepare their ICT environments for cloud. It will include training and advice to agencies to build confidence and capability, additionally assisting in addressing organisational barriers to a cloud operating model such as funding and governance.

This capability will support the implementation of the initiatives outlined in this strategy and provide guidance support for agencies in their adoption.

3.1.2 Principles based approach

A principles-based approach will enable agencies to align their cloud adoption with best practices.

Principle: Make risk-based decisions when applying cloud security

Risk based decisions, rather than just checking off compliance, are required to understand the security needs of a cloud service and apply the appropriate security controls.

a. Use threat modelling to evaluate and monitor risks.

b. Consider separating high and low value information into different environments to increase flexibility and focus resources.

c. Apply relevant security policy and guidance to make risk-based decisions. Make cloud specific considerations for individual services to set the right controls, mitigations, and accepted risk.

d. Apply appropriate controls for the workload don't restrict services with controls that are not required.

Principle: Design services for the cloud

When designing applications and services, consider cloud native and modern application architecture design patterns. Modern applications should be secure, resilient, elastic, modular, automated, and interoperable. Cloud deployment models such as serverless or containers enable automation and allow applications and services to be run independent of the infrastructure, enabling more opportunities for provision and expansion of services.

a. All agencies must use cloud services for new services or modernisation of services whenever the cloud services are fit for purpose, provide value for money, and demonstrate appropriate risk management.

b. Agencies must design all new or modernised ICT services as cloud native, or cloud enabled[1], consistent with the National Institute of Standards and Technology (NIST) essential characteristics for cloud.

[1] https://www.techopedia.com/definition/347/cloud-enablement

c. Where no suitable commercially provided cloud service is appropriate, agencies must design applications to be cloud-ready, maximising automation, portability, and resilience.

Principle: Use public cloud services as the default

NIST defines public cloud as being available to the public or a large industry group and owned by a cloud service provider. The public cloud market offers a broad range of services and providers that enable agencies to keep their technologies and business processes up to date. Public cloud can provide fast and competitive options for agencies and should be used as the preferential default before exploring hybrid and multi cloud options.

a. When choosing cloud models agencies should consider public cloud first and in preference to any other cloud deployment model.

b. Agencies should ensure the public cloud service has the appropriate security implementation for the information being handled.

Principle: Use as much of the cloud as possible

Agility comes from models that leverage standardised cloud technologies. This enables agencies to keep pace with industry disruptions and innovation cycles as well as maintaining business process and technology currency.

a. Agencies must source as much of the service through cloud as is practical and feasible for any new or emerging business capability or modernisation of existing services.

b. Where the cloud cannot be sourced to meet the capability, agencies must approach their own developments to be cloud enabled.

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

Agility comes from using the service ‘as it comes’ without bespoke processes being introduced which erode the business agility of the service by adding complexity and requiring intervention during change cycles. Rather than developing bespoke processes and technology to have cloud services suit business processes, business processes should change to greater adopt cloud and realise the benefits of being a cloud centric organisation.

a. Agencies should configure services and not customise them.

b. Agencies should change business functions/processes in preference to changing service functions.

Principle: Take full advantage of cloud automation practices

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

a. Agencies should use automation to manage demand and availability to meet user expectations of performance, reliability and security.

b. When developing or procuring services agencies should ensure application, data and messaging services can take advantage of cloud automation characteristics.

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

Monitoring allows agencies to have visibility of their cloud usage, cloud health and enable them to control costs.

a. Ensure that your Cloud Service Provider (CSP) can provide metrics that support the forecasting and analytics needs of your agency.

b. Ensure you can control costs of cloud use through provisioning and scaling on demand.

c. Ensure you proactively monitor the health and status of your cloud services.

d. Implement a resource tagging strategy to enable the above points in a cohesive manner.

3.1.3 Agency vision

Agencies can maximise the value of cloud to their business by using the cloud principles as a starting point to set their own vision and strategy for cloud adoption. The value opportunity, portfolios of applications and systems, investment cycles and maturity of each agency is unique and cannot be covered under a whole-of-government cloud strategy. It is therefore important that agencies articulate how they will obtain benefits from cloud in their own strategies, underpinned by initiatives in this strategy.

Agencies will also need to plan the modernisation, migration, network, skilling and service management capabilities needed to integrate cloud services into their environments.

There should be early consideration for how agency budgets and appropriation cycles will align with their cloud investments. This will enable agencies to transition their funding for cloud with minimal disruption. Whilst the secure cloud strategy looks at ways agencies can take advantage of cloud, it cannot drive changes to budget rules and therefore, agencies need to incorporate timeframes for budget planning purposes into their own strategies.

Cloud adoption will be influenced by agencies' technical and business readiness to transform existing business practices to align with cloud offerings. Business readiness for cloud will ensure agencies can completely use the agility of cloud to meet their business outcomes. Agencies will need to consider their current business models and identify where targeted change programs are required.

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.

3.2 Frameworks and practices

3.2.1 Cloud security considerations

The Australian Government has a strong risk based management posture that is maintained through the Protective Security Policy Framework (PSPF) and Information Security Manual (ISM). These frameworks provide the mandatory guidance and obligations for agencies to ensure cloud is suitable for handling government data. The frameworks also define accountabilities and outline who within agencies has the authority to accept risk. The PSPF and ISM outline security obligations and guidance for Government agencies to use in response to risks and threats to government services, and proposes mandatory and optional treatments to reduce risk to an acceptable level. This includes the people, technology and process aspects of a service. All technology services are risk assessed and authorised for government use through these frameworks.

The risks of using outsourced ICT services is inherently more complex than traditional in-house ICT implementations. Physical and information security considerations across data centres, networks, operating systems, gateways and applications are significantly complex when a range of providers are responsible for developing and/or supporting the environment. Cloud services are similar to outsourced ICT services. However, they are subject to regular configuration changes, can be multi-tenanted, and hosted offshore, which creates additional complexity.

Typically, cloud providers and their cloud services are assessed by an IRAP Assessor and the subsequent report provided to the CSP for sharing with agencies interested in using their services. Agencies use this report as the basis for their risk assessment to determine if the CSP and its cloud services meet their security needs and is suitable for handling Government data. For most Government information systems, the authorising officer is within the owning agency. Authority To Operate (ATO) occurs to ensure that sufficient security mitigations have been put in place, and that residual risks have been accepted by an appropriate authority. This is usually undertaken by a senior executive within the owning agency who has an appropriate level of understanding of the risks and the authority to accept risk on behalf of the agency. These practices enable agencies to maintain accountability for their risk posture and provide them autonomy in making decisions for their organisations.

Commonwealth agencies are responsible for their own assurance and risk management activities through self-assessment, leveraging the following guidance from the ACSC. This includes:

The Anatomy of a Cloud Assessment and Authorisation

Cloud Security Assessment Report Template

Cloud Security Controls Matrix

It is recommended that risk assessments clearly address security controls listed within the ISM, as well as the additional cloud security guidance listed below:

Cloud Computing Security Considerations

Cloud Computing Security for Tenants

3.2.2 Hosting and Data Considerations

The Hosting Certification Framework has been developed to operationalise the principles outlined in the whole-of-government Hosting Strategy, and to support the secure management of government systems and data.

The Framework will assist agencies to mitigate against supply chain and data centre ownership risks, and enable them to identify and source appropriate hosting and related services.

Initiative 2: Implement a layered certification model

Cloud services self-assessed by agencies, following the IRAP process, do not have a reduced security posture. Where cloud specific risks exist, ASD can provide further advice. Sharing information and assessments through a Common Assessment Framework will help to improve security practices while at the same time reducing the burden on agencies to recreate material.

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.

3.2.3 Cloud service procurement

The Cloud Services Panel (CSP) is a whole-of-government panel established to support agencies in procuring cloud services. The panel has been in operation since January 2015 with a refresh of panellists undertaken in mid-2016. The CSP enables agencies to request quotes for services and provides transparency of the certification and accreditation status of cloud services. It is non-compulsory, however its intention is to streamline the procurement for cloud services and increase value for money from cloud procurements.

The ICT Procurement Review[2] (May 2017) found some suppliers and agencies believe there are too many panels that are not refreshed often enough, limiting access to newer and more innovative suppliers (including SMEs and start-ups). The report also noted that panels would benefit from the introduction of a new procurement pathway that better supports purchases through a catalogue-based e-procurement approach. This approach would include the ability to undertake comparisons between services, click-to-buy and dynamic pricing and create opportunities for small scale experimentation and innovation. The CSP was considered in this review.

The rapid iteration and release cycle of cloud services makes them well suited for a streamlined procurement pathway. The current CSP infrequent refresh cycle for new panellists limits the opportunity to procure innovative new products and, in some cases, benefit from price reductions through improved competition. Additionally, standardisation and transparency of cost models, taking into account differences of pricing in the deployment and provider models will provide a comparative baseline for agencies to understand and control their cloud costs and drive competition.

[2] http://ict-procurement.digital.gov.au/assets/documents/ICT-procurement-taskforce-report_WCAG.pdf

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.

The Cloud Services Panel expired on 31 March 2021 and was replaced the Cloud Marketplace. Further details about the Cloud Marketplace can be found at: https://www.dta.gov.au/news/dta-launches-new-cloud-marketplace

3.2.4 Dashboard

Increased transparency of the use, cost and certification status of cloud services will help inform decision making. There is currently limited visibility for agencies and industry of what cloud services are being adopted, used, the certification status of the services and associated service pricing. Improving visibility will help government make risk based decisions improve agency decision making, drive increased competition through transparent pricing and provide clarity of the services that have been certified and their progress to help government make risk based decisions.

Publishing a dashboard of government cloud services will provide clarity about when a service may be available for use and the cost of the service. Whilst commercial considerations need to be taken into account, a transparent approach that is sensitive can provide great benefit, including driving competition.

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.

3.2.5 Cloud Common Assessment Framework

The Cloud Common Assessment Framework seeks to address barriers to cloud adoption resulting from agencies being unsure if they can meet the government compliance needs. The approach will increase collaboration and reuse to avoid duplication and drive best practice approaches.

To build confidence, the capability within government needs to improve to identify the compliance needs of government cloud, not just in security, but across the broad range of compliance obligations including information management, privacy, audit, accessibility and so on.

This can be achieved by creating a more standardised approach that enables agencies to assess, measure and compare the service's ability to meet the government need and share this for reuse. The Cloud Common Assessment Framework will identify the qualities that make cloud useable for government and how to measure this usability. This approach will build the capability to better understand cloud compliance needs in the government context. The framework will provide a clear and consistent approach to cloud assessments that articulates, to both agencies and cloud service providers, the measures used to determine usability in a government context. It will foster reusability of assessments.

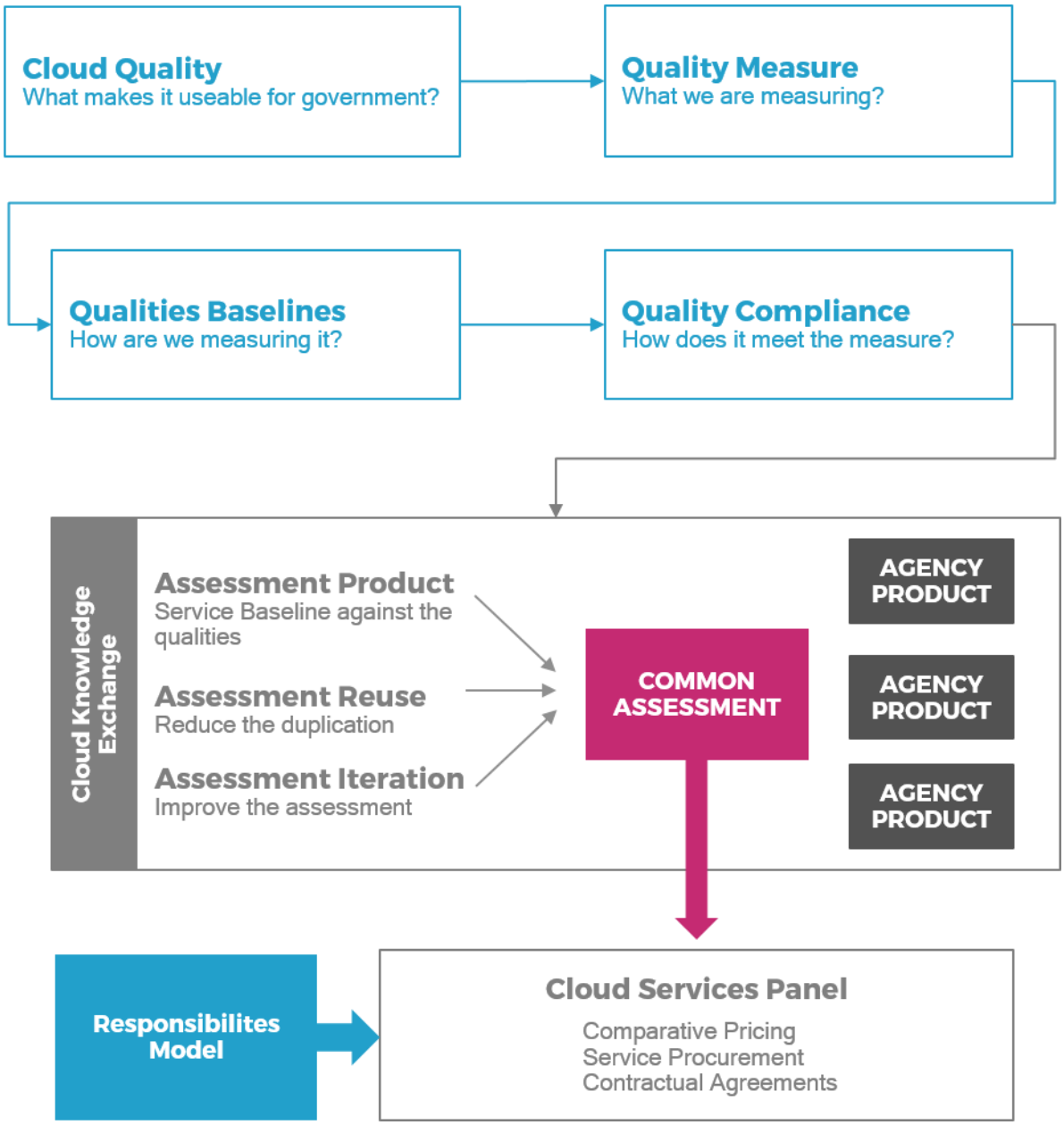


Figure 2—Cloud Common Assessment Framework

Sharing Cloud Common Assessments

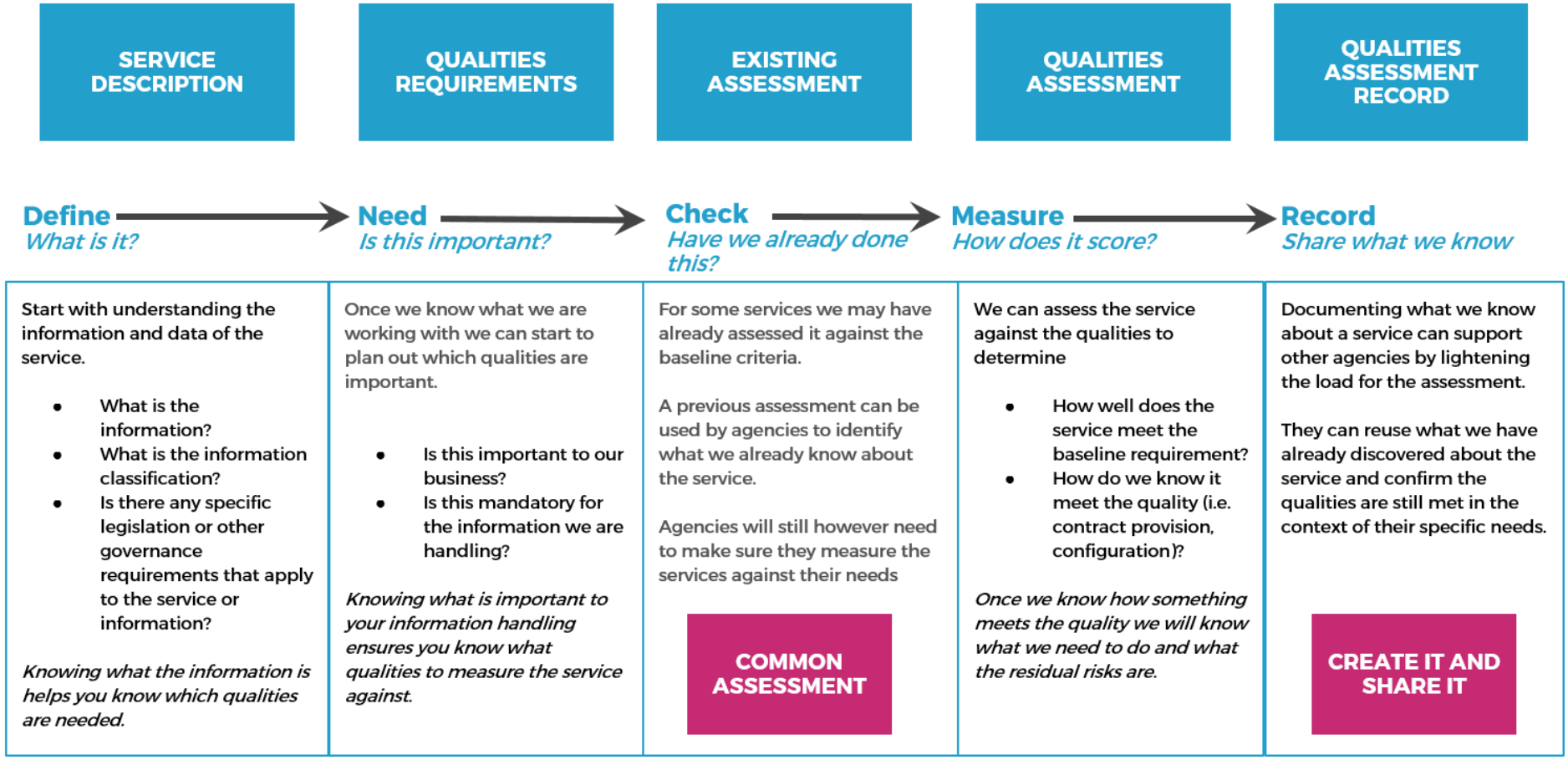


Figure 3—Sharing Cloud Common Assessments

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.

3.2.6 Responsibilities model

Clarity around responsibilities for cloud services is critical to managing risks and maintaining security confidence within agencies. The cloud introduces operational \practices that are different to those for traditional infrastructure. This doesn't mean it is less secure, but it does mean the risks and assurances need to be understood in this environment and appropriate governance and accountabilities put in place.

In using cloud, agencies need to identify the risks, the mitigations and the accountability for management, security and integrity. Uncertainty about what the provider is responsible for and what the agency is responsible for must be addressed early. Whilst some providers have comprehensive guidance, agencies will still need to be clear on what is managed on their behalf by a provider.

A responsibilities model can provide a platform for clearly understanding accountabilities and operating expectations in the cloud and create a shared capability for agencies to use best practices for monitoring and managing their cloud services.

Refer to ACSC guidance The Anatomy of a Cloud Assessment and Authorisation for up to date guidance on shared responsibilities with CSPs.

For cloud services much of the provider accountability is managed through contract provisions. Accountabilities between agencies and providers vary with which service model is used.

Cloud services are also consumed through an ‘as a service’ approach which means they are bought with pre-defined terms and conditions and service levels. Current ICT contracts are not flexible and don’t always cover the variations in cloud services responsibilities. Modular contracts which are based on a responsibilities can make it clearer for agencies.

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.

3.3 Sharing the knowledge

Sharing knowledge, capabilities and expertise in cloud across government will enable agencies to transition to cloud with improved insight. Shared products that can be reused, lessons learnt and common technology creates a capability uplift for agencies that iterates and shares good practices and reduces duplication or the same product across a number of agencies.

As part of this strategy, the Digital Transformation Agency will develop a Cloud Knowledge Exchange to support the sharing of common products. It will connect agencies and provide access to resources and information to support cloud adoption.

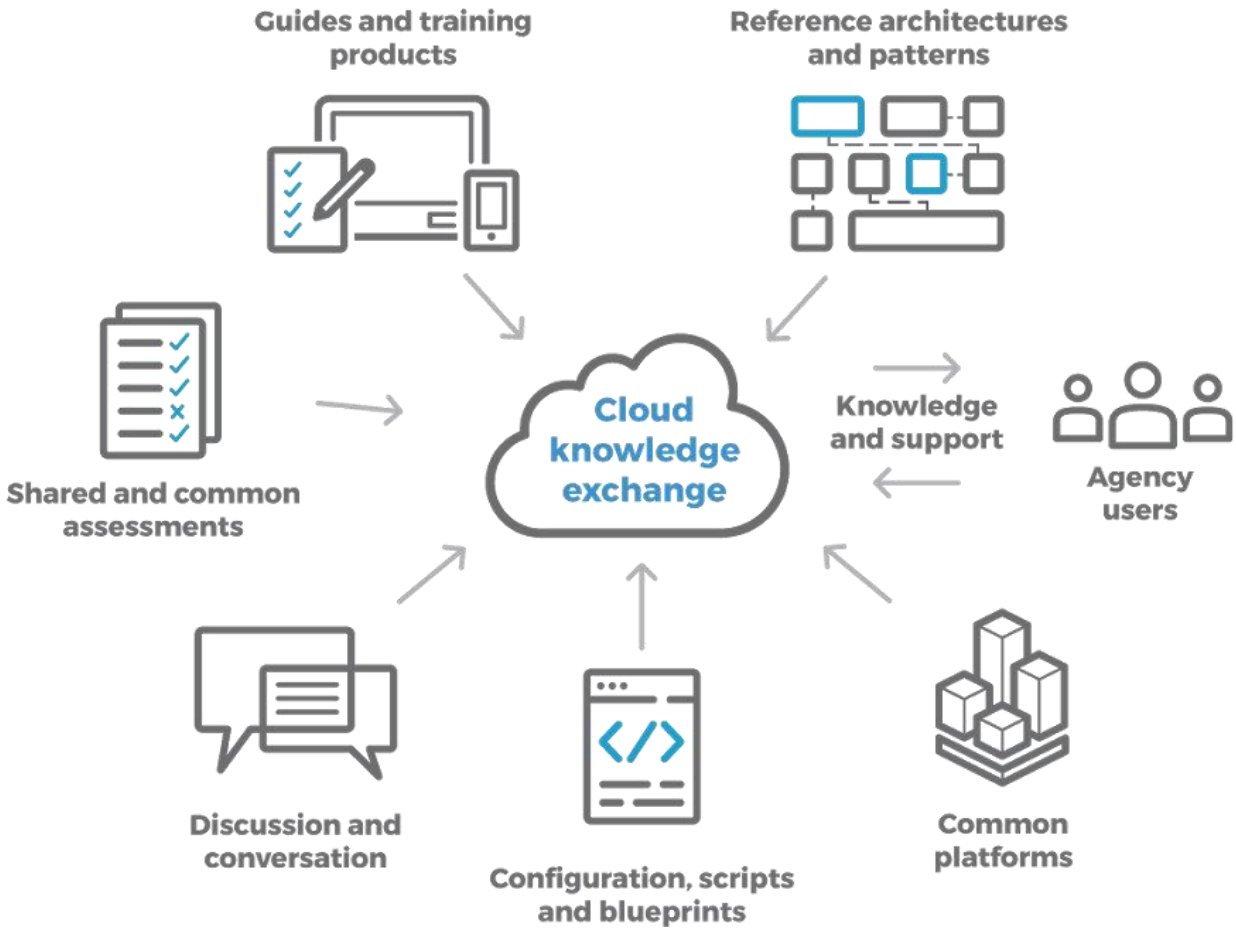


Figure 4—Cloud Knowledge Exchange

The knowledge exchange will provide an opportunity to iterate and improve products for the benefit of all. As more agencies use the exchange, their knowledge and experience will create better whole-of-government products rather than many individual products. This will be particularly beneficial for agencies with limited resources or capabilities as they will be able to leverage the experiences of agencies with more maturity or with access to cloud skills.

Figure 5—Identifying Common Products

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.

3.4 Shared capabilities

3.4.1 Building skills

Building the digital skills to support cloud use is a key need for government to successfully adopt cloud services. The public sector workforce needs the skills to build, modernise, implement, manage, monitor, procure and govern cloud services, across providers and across environments. These skills specific to cloud are not currently recognised in the Australian Public Service Commission job family model, nor is there a general or more universal description of the various cloud roles and job descriptions. This new cloud job capability will sit within the same framework as the Digital Transformation Agency's Building Digital Capability program.

Industry can also help build competency as providers of training programs specific to cloud services. These programs will build skills and competencies needed in addition to other frameworks being developed across government.

Government will need to leverage existing expertise while also embracing new business and technology skill sets. The new skills required may mean the disruption of careers, and it is important to note that the knowledge and expertise of staff familiar with the current environment continue to be valuable following the adoption of cloud.

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.

3.4.2 Cloud.gov.au

The cloud.gov.au platform provides a capability to educate and enable agencies to develop cloud native applications. It supports agencies to use standard approaches to cloud development and allows for agency experimentation in the cloud with a fully supported environment. The cloud.gov.au platform fosters knowledge and capability of cloud in government and will continue to play a role in developing capability and maturity within agencies but is not a single cloud platform for all government cloud use. The strategy does not advocate a single whole-of-government cloud platform be developed. Instead cloud.gov.au will assist with developing agencies skills in using cloud.

The cloud.gov.au platform has been decommissioned by the DTA and no longer provides whole-of-government hosting services.

For further details or if you have any questions, please contact the support team at support@cloud.gov.au.

To source a Cloud platform and cloud services for government, please visit the Cloud Marketplace.

3.4.3 Common platforms

A platform provides reusable services that can range from commercial applications to a complete set of business services, such as a common service management practices. The government's adoption of cloud provides opportunity for the development of services for agencies that can be reused by other agencies.

There are a number of cloud platforms that will provide benefit across agencies and create more opportunities for collaboration and standardisation. These are different to other initiatives for common platforms across government, such as Tell us Once and Digital Identity as they focus on providing capabilities to support government use of cloud, rather than delivering a whole-of-government service offering.

Platforms that will initially be explored include:

- **Federated access management** - Federated access management is a key capability required for seamless interaction with cloud services for agency staff and users, including system users. Cloud services require the management of role-based access and authorisations. Managing these in a central location that also enables single sign on (SSO) ensures agencies can control their user management and access and associated internal policies and enable trust across multiple identify services. Being able to audit these services is also fundamental. Extending government federation to build a trust relationship amongst government entities creates a core capability to reduce the effort in provisioning users for shared and collaborative activities across government.
- **Integrated Service Management** - Moving to cloud is likely to see agencies use services across multiple cloud providers. Understanding the overall health of systems and services across multiple providers becomes a challenge. Agencies need to build best practices for reporting and monitoring across. An opportunity exists to deliver shared service integration practices, including toolkits, reporting and integration capabilities to build this best practice and reduce duplication.

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.