Fujitsu Secure Government Cloud Services on Azure & Vault

Governments in Australia and New Zealand rise to the data protection challenge in the age of the cloud

Governments have not been immune to the impacts of technology. Citizen expectation around service delivery have been transformed as the computing power they can access from their computers, tablets and smartphones means they can access government services from anywhere at any time. Local, state and federal government agencies and departments have all had to adapt to this rapidly changing world.

Challenges such as digital identity, modernising older applications, a rising wave of new security challenges, a shift towards 'as a Service' delivery models and increased need to connect services across departments mean governments in the region need to rethink how technology and service delivery are executed in the 21st century. Secure cloud services give governments the opportunity to address these concerns without compromising security and integrity.

While citizens have embraced new technologies, so has every level of government. Initial forays into cloud computing were taken cautiously in order to ensure services were reliable and that citizen data was protected. Those steps forward have given governments valuable experience and a deepened understanding of how best to take advantage of cloud technologies. But what happens with more complex workloads that require different levels of security?

The Australian federal government uses a six-level system to classify data. Data that is deemed to be Unofficial, Official and Official: Sensitive is considered to have either no impact or limited impact if it should become public. But Protected, Secret and Top-Secret data are subject to significantly heightened controls to ensure their security and integrity.

New Zealand uses a similar system with four levels described as Restricted, Confidential, Secret and Top Secret. The systems and processes required to ensure the most sensitive data is kept safe are different and, thus far, have been largely maintained using traditional systems.

It is now possible for governments to use cloud services that retain all data on shore, are subject only to local laws and deliver the level of security needed to support the needs of citizens and governments in the 21st century.

VAULT Australia's Secure Cloud Specialist

Gold Microsoft Partner | Azure Expert MSP

FUJITSU

What do governments need?

With demands from citizens for better integrated and easier to access services, governments have been hit with significant challenges. As more data is being collected and used, governments need to ensure they have strong protection and controls in place. As well as considering the different classification levels for access, they need to ensure information is stored and sent using appropriate tools and standards.

With data sovereignty rules paramount in the consciousness of governments, on-shore data storage is critical. This is the reason why Fujitsu has expert security and cloud advisory services, professional services and managed services to ensure that cloud adoption is highly secure. Fujitsu brokers and integrates secure government cloud services with the flexibility of over 100 Azure services which have been IRAP assessed along with the Australian Cloud Infrastructure and Secure Internet Gateway capabilities from Vault.

Fujitsu's secure government cloud services gives government assurance that the chosen cloud services are designed for rigorous security requirements with an understanding of the unique needs of government departments and agencies. In New Zealand, similar assurances are provided by ISPC to ensure its citizens are well protected.

However, it is important to understand some services have more caveats on those assessments than compliances. Government departments and agencies need to ensure that they recognise these compliances and caveats for the cloud services they choose.

As well as working with trusted partners, governments want to ensure they are focussed on delivering value as citizens and taxpayers are increasingly concerned with government spending. This is why transformative cloud services, which can deliver digital citizen services, are so important. They allow governments to not only change the way they invest in infrastructure, shifting from a predictive and capital expenditure intensive model to a responsive and operational expense focussed model, to platforms that allow them to develop vastly improved experiences for citizens that take advantage of software technologies that can fully leverage the cloud.

What are the challenges?

Political shifts and economic changes are common for governments and create cycles of regular change. Systems need to be flexible and support the easy transition as departments and agencies are merged, split and realigned. Governments need systems, technology, people, and processes that can quickly adapt. And with new government initiatives in constant development, the ability to leverage a stable and secure cloud foundation.

Over the last two decades, the expectations of citizens have changed. Armed with always-on smartphones and tablets, there is an expectation that governments at every level provide access to government services that work across all platforms. However, many government services are delivered through older legacy systems and the required pace of change is faster than how government typically operates.

Many of those systems are operated by different agencies and departments with the ability to share data or interoperate often ignored during design. This creates increased security boundary design effort. When a service from one agency touches with a service from another agency, there can be significant design and risk assessment effort.

Many government systems are monolithic, and not composable. But by shifting to a "microservice" style architecture, data from different departments and systems can be integrated more easily. For example, data from one system can be easily interrogated and used across systems. This means integration of agency systems often do not follow standard and reusable patterns leading to rework and increased complexity due to a lack of plug and play architectures. Often systems and support are duplicated as this is easier than integration.

With government departments looking at moving complex applications and services to the cloud, access to well trained and experienced experts with appropriate security clearances can be challenging.

Governments handle some extremely sensitive information. And this, coupled with perceptions about how secure the cloud is, means that they are often risk averse which can make them change averse.

This is why many government departments and agencies have taken the DIY approach to systems. But that has introduced new risks. For example, they can struggle to scale during periods of peak demand and updating systems can be challenging when key people move on. This is why it is critical that they find local service providers that understand that satisfy data sovereignty requirements, the need for strong security and are on approved selection panels.

There's no one size fits all

The cloud is not a single, monolithic system. There are thousands of different services and service providers available. The choice of services and providers means there's no single cloud or on prem solution that works for everyone in every context. And when you throw in the need to maintain some systems and applications running on local infrastructure, it becomes apparent that multi-cloud systems that take advantage of SaaS-based services, hybrid IT and public cloud infrastructure working together make sense.

Hybrid cloud solutions enable government departments and agencies to manage data sovereignty concerns while enabling better connectivity between people and data on whatever devices they choose. The cloud is not just about infrastructure – it is about software that is built to be reliable with security built in and not bolted on.

Successfully delivering cloud services may mean consuming different cloud services from a variety of providers including hyperscalers, sovereign cloud providers and SaaS providers. Once the best services for a given use-case are chosen, the challenge then becomes integrating, along with integrations back into the on-premise landscape, to successfully fulfil the needs of governments and their citizens.

What does government need?

With the need for speed and agility, it is not surprising that the government has enthusiastically pursued its secure cloud strategy. The cloud provides government agencies with a platform that will enable the application of AI. Machine learning, advanced analytics and other new and evolving technologies that will allow governments to adapt and innovate faster than ever before. And this can be achieved while removing complexity, technical debt and risk.

While many private sector organisations have "cloud strategies" the Digital Transformation Agency's secure cloud strategy emphasises the inherent security which is obligatory for all government agencies in their adoption of cloud. Regardless of the system information security classification, from Unofficial, through Protected and up to Top Secret, security is essential.

One of the biggest barriers to overcome for agencies and organisations who are adopting Protected cloud is the risk assessment which is necessary to confirm that a cloud service can gain authority to operate. This assessment process can be long and arduous and has potential to delay and derail a government program, which can have far reaching consequences to citizen services and national security.

The answer is not to shirk this but to devote effort to understanding the risks and addressing them. In many cases, existing systems had their own risks, but these went unrecognised as the systems had been in place for so long that they were not designed to consider the current risks. Fortunately, there is significant guidance to assist government agencies and departments.

In 2020, the Australian Signals Directorate ended the Cloud Services Certification Programme, which effectively ended the certification of cloud services. This was superseded by the Cloud Security Guidance, which has been published by Australian Cyber Security Centre in collaboration with the Digital Transformation Agency and the wider industry. The result is a comprehensive set of guidelines and control objectives which are designed to assess the risk of adopting cloud for specific use cases.

This new guidance provides government with a set of even principles and assessment framework to facilitate assessing cloud services. It also provides certification, support with contracts and platforms for information sharing so agencies and departments can share information and collaborate when assessing and choosing cloud platforms.

Dealing with Protected data

Governments have been digitising services for many years. But challenging projects involving protected data have been avoided because of security concerns. That meant the 'low hanging fruit' has been picked, leaving more complex projects dealing with more sensitive data.

In 2017, Microsoft partnered with Canberra Data Centres to establish capability to operate Microsoft Azure services with assurance that the data centres are certified for TOP SECRET. That has enabled the ASD to certify many Azure services as secure.

Vault Cloud was first to the cloud for government and has built its technology to the highest security standards with TOP SECRET controls for government, defence, and intelligence workloads. And there are many other protected services delivered though this platform to a number of government departments and agencies.

In addition to platform specific services, Fujitsu provides government agencies with access to PROTECTED cloud and Enterprise Applications as a Service with the rigorous security controls that are required for PROTECTED data. This has been delivered to numerous departments dealing with highly sensitive data and has continuously exceeded expected service levels since it was first deployed in 2017.

The federal and state governments now have options for securely hosting data, with local providers that have been certified and accredited by ASD and assessed by IRAP. It is now possible to address workloads that have been previously considered too difficult to move to the cloud as the secure infrastructure to support these specific needs is now available.

Security is not just about technology. People are a critical factor. Governments need to work with trusted service providers who have security cleared personnel with NV-1 or above. Fujitsu Secure Government Cloud Services with both Microsoft Azure and Vault give governments the assurance they need that their data and workloads are protected to the highest levels

The path forward

Protected cloud services can help government departments and agencies, at local, state and federal levels meet their strategic needs for today and the future. But that transformation requires a plan.

Business Priorities:
Document the priorities, stakeholders and user needs for your agency.

Cloud Strategy:
define the cloud strategy for your agency which underpins your priorities and is in support of the DTA's Secure cloud strategy that allows you to securely integrate all the applications and services.

Data Classification:
Review your data security requirements and choose a cloud service to support your TOP SECRET, PROTECTED and UNCLASSIFIED workloads.

Application Portfolio Discovery:
Undertake a thorough investigation of all the applications the department or agency is using and the data they handle.

Prioritise Your Applications:
Map the applications you have to your business services and the strategic priorities which they underpin.

Define the migration/transformation strategy:
Make a plan for each application and service. In some cases, that may mean either retaining the application in the current state, retiring it, rebuilding or rehosting it - moving from on-prem to cloud hosting. In other cases, it may be wiser to rearchitect applications to leverage new cloud technologies to make them more flexible, resilient and secure or replace legacy or bespoke applications with tools that can be better supported and more efficiently managed and maintained.

Define your rapid business case:
A cloud economics accelerator can be used to create a rapid business case for your future TCO, the cost of change and the return on investment.

Plan:
Create your agile sprint plan for your cloud adoption and application transformation or migration.

Pilot:
prove the concept and value of your selected plan with a small scale minimum viable product, to assure your technical and business stakeholders of the viability of the proposed approach, whilst also delivering early value.

Execute:
Implement your migration and transformation plan to adopt secure government cloud, in harmony with any workloads moving to SaaS or staying on premise.

Working with a trusted partner who can provide valuable information and counsel, such as Fujitsu, will greatly assist with the decisions you need to make at each step of the plan.

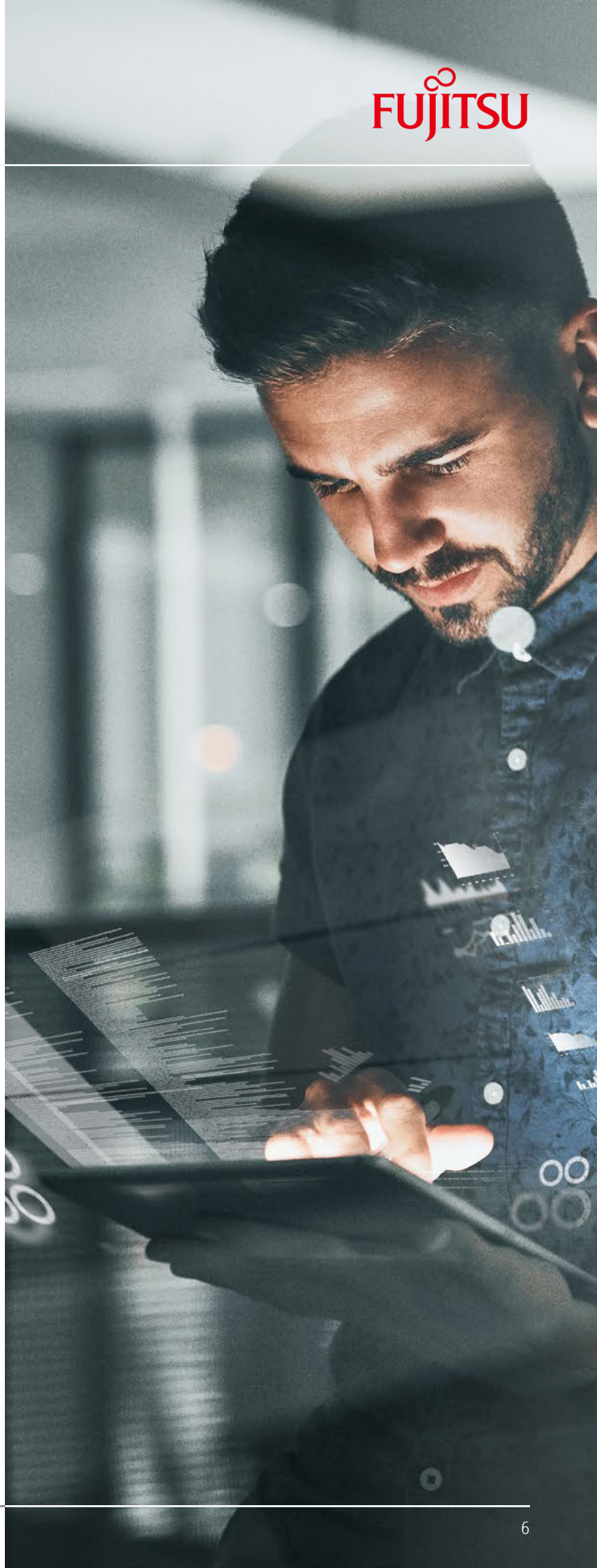
It is important to start with a vision of what you want the end state to look like. To determine what applications and services you need to achieve that end state. It is critical to remember that your end state is not just about platforms and applications. Your data is critical. Ensure focus is given to how data will support your end state. How will you bring together multiple data sets to provide a single view of citizen services, allowing for enhanced analytics and AI models to provide more value?

Governments in the 21st century need to be responsive to citizen needs as well as ensuring all data and workloads are securely managed and operated. This requires partnerships between government agencies and departments and service providers that understand these unique needs.

Cloud services are critical to delivering what citizens and governments need. Cloud service providers like Vault and Microsoft have listened to the market and can offer service that meet the need for strong security to protect the most sensitive data. And they do that while keeping the data on shore and subject to Australian laws. They have been assessed and certified by ASD.

But the right cloud platform service partner is just part of the equation. Working with a team of experts that have appropriate security clearances and deep experience and understanding is also critical. Fujitsu understands the needs of governments and how the technology offered by partners like Vault and Microsoft can guide success in achieving strategic objectives.

Fujitsu has a heritage of service excellence in managing massively complex services across multiple geographies and industries over many decades. This mission critical expertise is coupled with its more recent experience in transformative applications, customer experiential and digital services with technologies such as cloud and AI.



TO TALK ABOUT YOUR SECURE CLOUD NEEDS

> Get in touch with us today

enquire@fujitsu.com

fujitsu.com/au/services/multi-cloud/secure-government-cloud-services

FUJITSU AUSTRALIA LIMITED