Vault Systems Pty Ltd, ABN 60159020127
Level 5, 2 Constitution Avenue, City ACT 2601
Level 3, 1 Bligh Street, Sydney NSW 2000
www.vaultsystems.com.au
(02) 6190 0000

Vault Systems submission to the Finance and Public Administration References Committee review of digital delivery of government services - December 2017

1. Introduction

Vault Systems appreciates the opportunity to provide feedback to the Finance and Public Administration References Committee on the digital delivery of government services.

Vault Systems is a Government Community Infrastructure as a Service Cloud Provider who enables Government agencies to deliver better services through technology while ensuring the protection of personal and national security data. Vault achieves this by providing an ASD certified, secure, data sovereign, hyper scale cloud which allows the Government to deploy services faster and more securely than previously thought possible.

Vault Systems is an Australian owned and operated company whose services are procured by a number of large Government agencies, including the Digital Transformation Agency, the Department of Human Services, the Department of Employment, the Department of Health, the Department of Social Services and Department of Defence.

Moving to the cloud provides Government agencies with immediate strategic benefits and longer term cost savings. There are significant operational cost savings, increased efficiency, enhanced flexibility and scalability, security and data storage. In the longer term, adopting cloud assists agencies to focus on their core strategic competencies by outsourcing generic IT services that can be better and more cost effectively delivered by a specialist cloud provider.

Whilst to date cloud adoption by government agencies has been modest, annual spend has doubled year on year since 2013 Cloud related infrastructure spend by the Federal Government is anticipated to be 20%+ of the total ICT budget by 2019 reaching over $1bn. With the Australian Government committed to a cloud first policy to drive a greater take up of cloud services by federal government agencies, it is inevitable that the use of cloud providers to digitally deliver government services will increase significantly over time.

2. Responses to the specific areas of focus

2.1 Whether planned and existing programs are able to digitally deliver services with due regard for: privacy, security, quality and reliability, value for money.

2.1.1 *Privacy*

With the Australian government committed to a Cloud First policy to drive a greater take up of cloud services by government agencies, establishing safeguards around managing the sensitive personal data of Australians should be a key priority of the Committee. While there are many benefits to cloud adoption, the consequences of getting it wrong are immense. The risk of irrevocably losing the public's trust in Government is almost certain if personal data is not adequately protected or handled. Data privacy continues to be a topical issue attracting continued

interest from the public and the media, particularly as 93% of Australians are concerned about organisations sending their personal information overseas [1].

When the data of Australian citizens is moved offshore it becomes difficult to apply Australian jurisdictions and laws to how that data is handled. Data held offshore is automatically subjected to the laws and general practices of the hosting country. These laws and practices may be less stringent than Australian privacy laws and regulations. It is essential that Australian citizens can rely on the Australian Government to have a physical understanding of where their personal data is stored and accessed.

Vault disagrees with the Australian Signals Directorate (ASD) security control[2] which allows agency data and computing environments to be accessed, configured or administered from outside Australian borders by a service provider if a contractual arrangement exists between the service provider and customer to do so. ASD acknowledges the risks that foreign owned vendors operating in Australia may be subject to foreign laws and may also be subject to lawful and covert collection. Allowing foreign cloud providers to access and control data does not protect the rights of Australians to have their privacy and data adequately protected.

Ensuring sensitive and personal data is stored in data centres contained within Australian borders means that data centres are certified against robust Australian security certifications, such as those developed by ASIO and ASD. Government agencies can see where their data physically resides and develop relationships with those people delivering their services and have access to local expertise within the same time zone.

In conclusion, data sovereignty and privacy can only be assured through the use of Australian Clouds based in Australian datacentres, and Australian security cleared employees. The personal, sensitive data of Australians must be managed by Australians who have the appropriate level of access, within Australian borders and in accordance with the laws of Australia. By enforcing these standards, planned and existing programs can be delivered digitally with due regard to maintaining privacy of data.

2.1.2 *Security*

The Certified Cloud Services List (CCSL) identifies cloud services that have successfully completed the Information Security Registered Assessors Program (IRAP) assessment and have been certified by the Australian Signals Directorate (ASD). Australian government agencies applying the ISM must only use outsourced cloud services listed on ASD Certified Cloud Services List (CCSL). Vault is only one of three providers globally to have been certified by ASD to store and manage data classified as PROTECTED.

Vault's security controls are assessed against the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM). Vault believes that these documents provide a clear and transparent set of requirements for providers seeking to obtain certification from ASD. Throughout the assessment process thousands of hours were spent by Vault staff working on issues with various teams within ASD and IRAP assessors. This resulted in a material uplift in Vault's security posture. It is extremely important that ASD continues to take a lead role in the certification process as the quality of IRAP assessors can vary.

[1] Australian Community Attitudes Towards Privacy Survey 2017
[2] Australian Signals Directorate, Information Security Manual Controls 2017, Control: 1073; Revision: 2; Updated: Apr-15;

Vault is aware that recently there has been a concerted effort by other large, multinational providers and the Australian Information Industry Association (AIIA)[3] for ASD to increase the number of certifications, without additional fully trained resources. The practical outcome of this action would be the reduction of the security of citizens data and a increased risk to national security. It is essential that ASD's resources are adequately maintained to manage this critical area rather than security standards being lowered in order to manage workload.

In order for planned and existing programs to be able to digitally deliver services with due regard for security, it is essential that the Australian Government Security Controls remain in place and are not diluted in any way. The integrity of the system must be maintained, otherwise trust will be eroded producing a reluctance from citizens to interact with Government services offered online and the Government's reputation will be damaged.

2.1.3 *Quality and Reliability*

Citizens expect that government services delivered digitally will be available on demand 24/7 with fast, or almost instant response times. Purpose built, cloud native applications are able to deliver the quality of services required to achieve this. Therefore, it is important that cloud providers chosen to host government services offer a choice of multiple regions and availability zones coupled with cloud load balancer options to facilitate horizontally scaling environments with resilience built into the application layer.

The choice of platform is also an important consideration. A platform such as OpenStack, the world's most widely adopted and familiar platform has been developed, supported and implemented by many global enterprises and vendors, provides a mature and trusted platform. OpenStack is used by some of the leading companies in software development and cloud computing, including Vault, IBM, Rackspace, Dell, HP and Cisco.

The capabilities of OpenStack are continually expanding due an active open source community of over 6,000 individuals and 1,000 organisations. Having a common platform across so many existing providers to Government facilitates interoperability, reliability and quality in the digital delivery of Government services.

2.1.4 *Value for Money*

Moving to the cloud provides significant savings for Government agencies. Analysis by KPMG[4] has identified that savings of 30% to 60% in ICT infrastructure costs can be achieved by moving to the cloud.

There are no large upfront capital expenses to pay when using cloud providers. For example, if Government agencies purchase Infrastructure as a Service they purchase a service, not physical servers. This means Agencies only pay for what they actually use, rather than expected utilisation. Agencies can scale up and down as in line with demand for their digital services without having to purchase additional physical infrastructure. A simple analogy is that using cloud services is the equivalent of staying at a hotel rather than buying a house in every location you visit. Moving to an operational expense model is also beneficial to agencies because there are no long term financial commitments and no significant upfront investment.

[3] Letter to Angus Taylor, Assistant Minister for Cities and Digital Transformation, from AIIA dated 13 October 2017, subject heading Certified Cloud Services List.

[4] *Cloud Economics: Making the Business Case for Cloud - An Economic Framework for Decision Making*, KPMG International 2014, https://assets.kpmg.com/content/dam/kpmg/pdf/2015/11/cloud-economics.pdf

Using cloud providers to assist in the delivery of digital services also reduces costs by eliminating ongoing cooling and power costs for heat intensive servers, reducing the leased space required for IT infrastructure and eliminating costs associated with the maintenance of IT infrastructure.

However, there are also non financial benefits in using cloud services to deliver Government services digitally, including time savings and productivity increases. For Government agencies, procuring, installing and integrating infrastructure usually takes between 3 6 months. These increases in efficiency allow employees to spend more time on other activities which underpin the core business of the agency, as well as reducing the resources and time required to deliver the project.

The use of a cloud provider dramatically reduces this cost in acquisition cost, operating cost and speed of implementation. For example, Vault typically takes as little as a day to replicate an agency's existing infrastructure in the cloud.

Productivity is also increased as ideas for new digital services can be rapidly deployed and tested rather than waiting months for infrastructure to be available for testing. This fosters innovation and provides faster delivery of digital services to citizens.

2.2 Strategies for Whole of Government Digital Transformation

There remains a general reluctance of key decision makers within some Government departments to move towards the adoption of cloud services in the digital delivery of services. This continues to be a limiting factor when it comes to Government moving services to the cloud. While there has been gains made in this area, it remains an ongoing issue. Cloud providers can play an important role in educating key decision makers on the benefits of moving to the cloud and upskilling the public service workforce in cloud technologies.

Additionally, there are benefits for Whole of Government in standardising on a platform such as OpenStack to deliver cloud services. If Government standardised on this platform to deliver cloud services, Government could start to adopt technologies like Application Blueprinting, Containerisation and Micro Services. This would allow applications to be delivered to a fully operational state. This would mean the introduction of a new Shared Services Model, where Agencies deliver the "Code" of a fully integrated service. Rather than an agency providing services on behalf of another agency, agencies could take the new application "Code" and deliver it themselves without the investment of developing the service.

Standardising on a platform such as OpenStack also avoids vendor lock in. By using OpenStack as the underlying cloud services platform, customers are using a secure open source platform built on open standards which provides greater flexibility and choice to transition applications across multiple clouds.

Open standards are another important factor in delivering government services digitally. These standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. Open Standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption. This interoperability is a boon for agencies looking for a platform that can be grown and iterated on as needs develop, without being locked into a specific vendor.

2.3 Digital project delivery, including: (i) project governance, (ii) design and build of platforms, (iii) the adequacy of available capabilities both within the public sector and externally, and (iv) procurement of digital services and equipment.

2.3.1 *Project Governance*

Vault strongly recommends establishing a Cloud Steering Committee (CSC) to manage major projects, chaired by a business senior executive and including a representative of the cloud services provider.

Governance requirements can also be lessened by agencies standardising on a platform such as OpenStack and adopting technologies like Application Blueprinting, Containerisation and Micro Services. These technologies allow applications to be delivered to a fully operational state. Once a service or application has been developed by one agency under extensive project governance, the agency could provide the new application code to another agency. This agency could then deliver the same service or application without starting a new project to develop their own application or service. Essentially, project governance in developing the new application would have already been completed by the agency who originally developed the application or service.

2.3.2 *Design and Build of Platforms*

As stated under point 2.2, having all government agencies standardising on one platform, such as OpenStack, produces many benefits including interoperability, transitioning Government applications and services across multiple clouds, and using a trusted and mature platform that is based on billions of dollars of investment in research and development.

2.3.3 *The Adequacy of Available Capabilities (Public Sector and Externally)*

There are currently three providers on the ASD Certified Cloud Services List. All of three of these companies are Australian owned. This demonstrates that there is the capacity within the Australian market to provide cloud services to facilitate digital project delivery while also providing adequate quality, reliability and security expected by citizens. Using Australian providers for cloud services also ensures the skills required to ensure effective delivery and maintenance of digital services are not moved offshore. This also means support services are provided locally and in the same timezone as the government agency delivering services digitally.

The public sector's skill set in using cloud services to deliver government services digitally could easily be upgraded through collaboration with industry to develop additional training for the public sector. This could be delivered jointly by industry and the Digital Transformation Authority.

2.3.4 *Procurement of Digital Services and Equipment*

As stated under point 2.1.4, by utilising Infrastructure as a Service, when Government agencies move to the cloud they purchase a service, not physical servers. This means agencies only pay for what they actually use, rather than expected utilisation. Agencies can scale up and down as in line with demand for their digital services without having to purchase additional physical infrastructure. Procurement costs are dramatically reduced as less infrastructure is required to deliver government services digitally.

However, currently the procurement of cloud services is hindered by a reluctance of key decision makers within Government to move services to the cloud. Continued education *and* a secure protected cloud environment will assist with digital transformation. Given the savings and benefits offered by cloud, training relating to how cloud can be adopted in the digital delivery of Government services should be a key priority across Government.

2.4. Other related matters

Aside from the risks to privacy and security, using foreign companies to store Australian data equates to the loss of Australian jobs and taxes, damaging the Australian economy. The valuable skills and expertise required to ensure effective delivery and maintenance of digital services are also moved offshore if foreign companies are providing cloud services for Australian Government agencies.

3. Concluding Comments

Thank you for the opportunity to provide feedback to the Finance and Public Administration References Committee on the review of digital delivery of government services.

If the Committee should require additional information or have any questions, please contact Vault Systems on