19 November 2019

Digital Strategy Consultation
The Department of Premier and Cabinet
Email: digital@dpac.tas.gov.au

To whom it may concern,

Please find enclosed Amazon Web Services's (AWS) submission on the draft Tasmanian Government Cloud Policy (the Policy) and the DRAFT Tasmanian Government Cloud Policy Risk Assessment Guide (the Guide).

We welcome the important step the Policy sets out in no longer mandating the use of 'on-island' cloud for the public sector, but rather taking a cloud-first, value-for-money and risk-based approach to the implementation of ICT services and solutions, where cloud service and solution options may be located off-island. We also support the Guide as it set out a measurable risk-based approach.

The Government's move towards a cloud-first policy, which allows for the use of hyperscale cloud service providers under the appropriate risk assessment, is a positive step forward and should give the Tasmanian people and the broader ICT industry comfort in the Tasmanian Government's approach to cyber security and ICT modernisation.

We look forward to continuing to work with you on the implementation of this important policy.

Yours sincerely,

Jessika Loefstedt
Senior Manager Public Policy, Australia and New Zealand
Amazon Web Services

Introduction

Amazon Web Services, Inc. (AWS) is a leading global provider of public cloud services and provides information technology (IT) building blocks for customers of all types, from governments to commercial enterprises, not-for-profits to universities. Hyperscale cloud services enable customers to become more secure, innovative, and responsive to the needs of their end-users. AWS provides standardized services and makes them available to all customers. These services range from core infrastructure, such as compute, storage, database, and networking, to specific purpose services, such as video management and streaming, Internet of Things services, and artificial intelligence/machine learning.

AWS launched its Asia-Pacific (Sydney) Region in 2012, and has since then invested several billion dollars in physical infrastructure and the skilling of the local technology sector in Australia. Across all services, security is our top priority at AWS.

AWS welcomes the Tasmanian Government's new Cloud Policy, which advocates a risk assessment-based cloud-first approach and removes the mandatory need for the public sector and its agencies to use 'on-island' cloud providers only. This policy change opens up significant opportunities for the State, including:

- Improved digital Government services for all Tasmanians – allowing technology to facilitate more digital citizen-centric services;
- The development of the skills Tasmanians will need for the future – helping Tasmanians upskill for a modern workplace and global online economy; and
- More efficient allocation of Tasmania's IT budget – the opportunity to replace large, upfront capital expenditures and high ongoing maintenance costs with the cost effective pay-as-you-go expenditures of hyper scale cloud service providers associated with the use of modern technology resources that help deliver citizen-centric services.

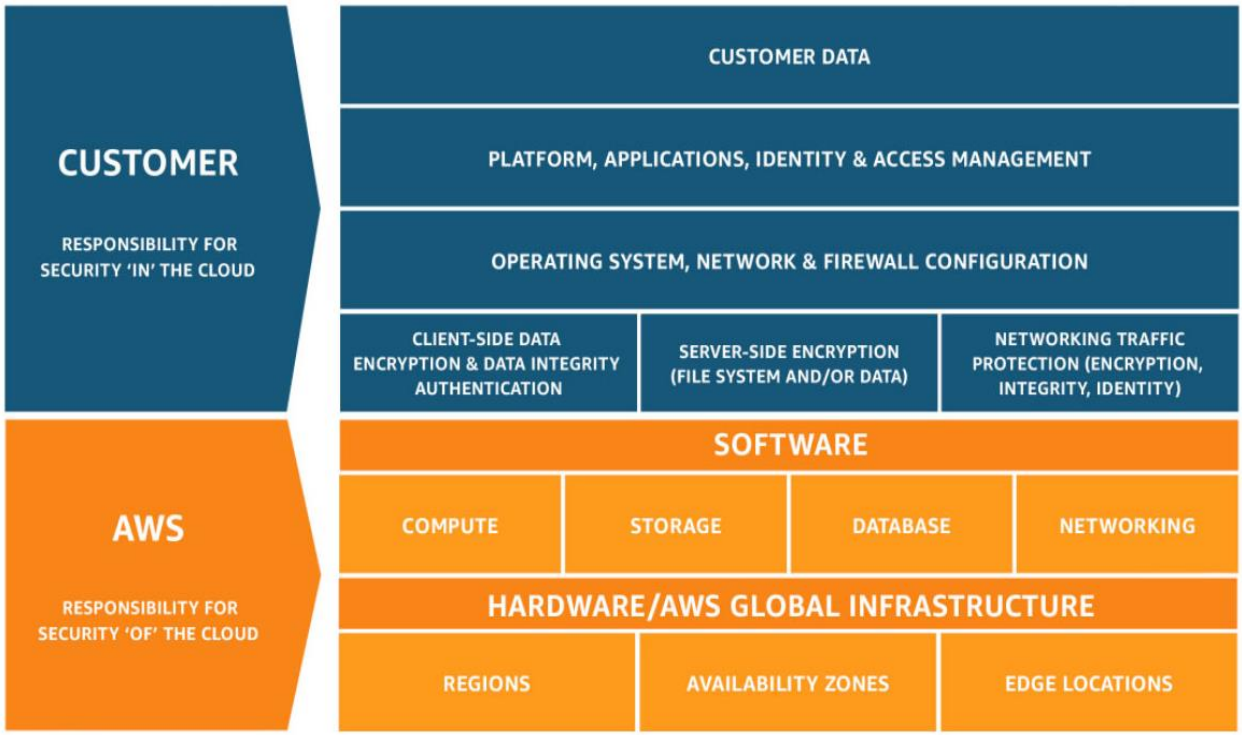
AWS shared responsibility model

AWS operates on a 'shared responsibility model' where security and compliance is a shared responsibility between AWS and its customer, as illustrated in image 1.0 below. AWS is responsible for the security and compliance 'of' the cloud, and implements security controls to secure the underlying infrastructure that runs the AWS services and hosts and connects customer resources. AWS customers are responsible for security 'in' the cloud and should determine, design and implement the security controls needed based on their security and compliance needs and AWS services they select.

AWS provides customers with best practices on how to secure their resources within the AWS service's documentation at https://docs.aws.amazon.com/.

Clear delineation of responsibilities ensures that identifying, assessing, and mitigating cyber risks is undertaken by the party best able to address the threat in any given technology environment or scenario.

1.0 AWS Shared Responsibility Model



AWS global infrastructure, international standards and risk-based approach

AWS has 22 Regions globally, a Region being a stand-alone separate geographic area, one of which is located in Sydney, Australia. In January 2019, the Australian Cyber Security Centre (ACSC) declared that AWS had been award PROTECTED status for 42 services in its Asia-Pacific (Sydney) Region under the Information Security Registered Assessors Program (IRAP).

This will enable Australian public and private sector organisations to store and process highly sensitive data at the PROTECTED security classification level. This means Government agencies and affiliates are able to innovate faster while they manage cyber risk, compliance and cost in an efficient way.

The customers using the AWS cloud choose what data they migrate to the cloud, where this data resides and how they use the cloud to improve citizen centric service provisions. For example, if a public sector customer chose to, it could store all its data and draw upon associated processing/value adding products using only the Asia-Pacific (Sydney) region.

Every AWS customer benefits from a data centre and network architecture built to meet the requirements of the most security-sensitive organizations. Customers that use the AWS Cloud

do not have to manage physical servers or storage devices. Instead, they use software-based security tools to monitor and protect the flow of information into and of out of their cloud resources.

AWS provides IT infrastructure to its customers designed and managed in accordance with best security practices and embracing a variety of IT security standards. The following is a partial list of assurance programs with which AWS complies:

- SOC 1/ISAE 3402, SOC 2, SOC 3
- FISMA, DIACAP, FedRAMP, and IRAP
- PCI DSS Level 1
- ISO 9001, ISO 27001, ISO 27017, ISO 27018

A full list of all compliance program AWS complies with can be found on:
https://aws.amazon.com/compliance/programs/

Tasmanian Draft Policy and Guide

AWS supports the baseline principles underlying the Policy and welcomes its consistency with the Australian Government principles-based approach for the adoption of cloud services. We note the draft Guide seeks to manage risk in accordance with AS/NZS ISO 31000 Risk management principles. AWS is in principle supportive of this approach.

We welcome the Policy's statement that cloud services and solutions can be located off-island. We do however question the Policy's stated preference for on-island cloud. The security and privacy of an ICT environment is not a function of location, is a function of the secure nature of the ICT infrastructure and ICT environment. Hyperscale cloud service providers, like AWS, help customers improve their security posture. An outcomes driven policy approach, with cyber security and innovation at its core, should put the emphasis on the need for the safety of the ICT infrastructure and the ICT environment and a risk assessment against that, not on physical location.

Finally, we welcome the review the Department of Treasury and Finance (Treasury) is undertaking in the context of the Tasmanian Government's Digital Strategy Consultation, to streamline procurement processes for technology services. AWS will engage in this process to ensure its view on ICT procurement processes are considered as part of this.