# Tasmanian Government Cloud Policy

VERSION 2.0
MARCH 2020

Department of Premier and Cabinet

Tasmanian Government

# Contents

GLOSSARY ..... 3

INTRODUCTION ..... 4

PURPOSE AND SCOPE ..... 5

CONTEXT ..... 5

POLICY STATEMENT ..... 7

RESPONSIBILITIES ..... 7

PRINCIPLES ..... 8

BENEFITS ..... 8

# Glossary

| | |
|---|---|
| Cloud | Cloud refers to the collective infrastructure that enables cloud computing, comprising both physical and abstraction layers: the physical layer is the supportive hardware (typically server, storage and network components); while the abstraction layer consists of software deployed across the physical layer. |
| Cloud computing | Cloud computing is a model that enables ubiquitous, convenient and on-demand network access to a shared pool of computing resources that can be rapidly provisioned with minimal management effort or service provider interaction. |
| Cybersecurity | Cybersecurity means the technologies, processes and practices designed to protect networks, computers, programs and information from cyberattack, malicious damage or unauthorised access. |
| DCaaS | Data Centre as a Service (DCaaS) refers to the provision of racks and data centre infrastructure as a service upon which consumers can deploy and manage their own infrastructure, platforms and software. |
| ICT | Information and communications technology (ICT) refers to communications and computer technologies including telephony, computer hardware, software and related services. |
| IaaS | Infrastructure as a Service (IaaS) refers to the provision of processing, storage, servers, networks and other fundamental computing infrastructure as a cloud-based service, upon which consumers can deploy and manage platforms and software. IaaS consumers do not manage or control the underlying DCaaS or IaaS, but control their own platforms (eg operating systems, database storage) and applications, and may have limited control over select networking components such as host firewalls. |
| Networking Tasmania | The Tasmanian Government's outsourced, managed data network arrangements, collectively known as Networking Tasmania (NT), comprise a number of contractual agreements with suppliers for the delivery of data network and information and communications technology (ICT) services. |
| PaaS | Platform as a Service (PaaS) refers to the provision of programming languages, libraries, databases, operating systems, services and tools as a cloud-based service, upon which consumers can deploy and manage software. PaaS consumers do not manage or control the underlying DCaas, IaaS or PaaS, but control their applications and may have limited control over configuration settings for the application-hosting environment. |
| Risk management | Risk management refers to organisational arrangements for identifying, analysing, evaluating, monitoring, reporting and mitigating risks. |
| SaaS | Software as a Service (SaaS) refers to the provision of software applications as a cloud-based service. Applications are accessible from client devices, such as a web browser or program interface. SaaS consumers do not manage of control the underlying DCaaS, IaaS, PaaS or SaaS, but may have limited control over user-specific software configuration settings. |
| Value for money | Value for money means achieving the best mix of quality, sustainability and effectiveness for the lowest whole-life cost of goods or services. |

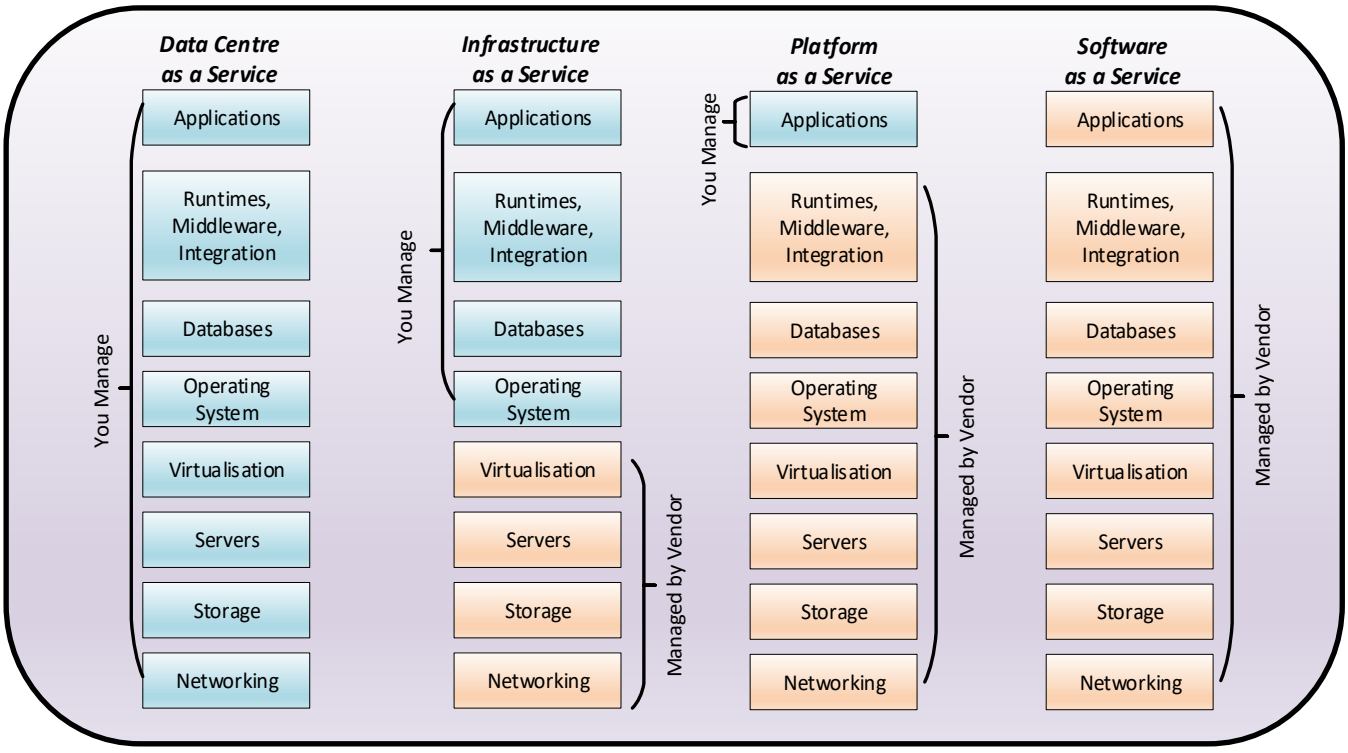
# Introduction

*Cloud computing* is a technology model that allows ubiquitous, convenient and on-demand network access to a shared pool of computing resources that can be rapidly provisioned with minimal management effort or service provider interaction. Cloud technologies continue to increase in complexity, capability and service offerings. *Hybrid cloud* is gaining popularity, being a cloud computing environment that uses a mix of on-premises private cloud and third-party public cloud services, with orchestration between the two platforms.

For contemporary organisations, the adoption of cloud services may deliver significant benefits, including:

- value for money
- technology risk mitigation
- lower key person dependencies
- greater organisational agility
- better positioning for improved service delivery
- enablement of modern work practices.

*Cloud services* are tiered, with Data Centre as a Service (DCaaS[1]) at the foundational level, through Infrastructure as a Service (Iaas) and Platform as a Service (PaaS), to Software as a Service (SaaS), as represented below.




[1] *While some definitions of cloud services do not recognise DCaaS, the context and scope of this Policy extends to and includes DCaaS*

At the lowest level (DCaaS), the customer (or a customer-appointed service broker) manages everything except data centre facilities, which are managed by the vendor. At the highest level (SaaS), the vendor manages all services.

# Purpose and scope

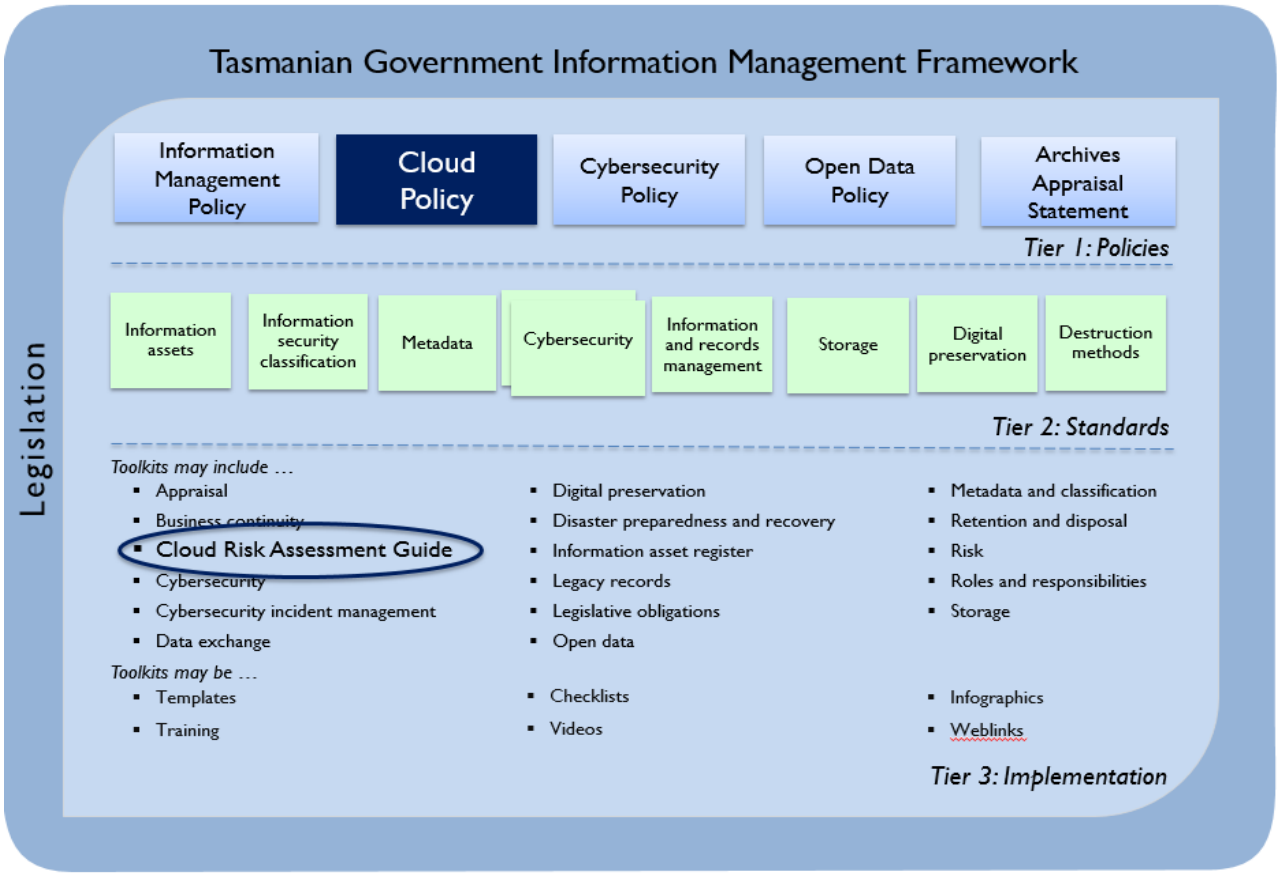
*The Tasmanian Government Cloud Policy* has been developed to provide a consistent, risk-based approach to the Tasmanian Government's adoption of cloud services. It includes a policy statement, principles and responsibilities relevant to the Policy.

This Policy applies to all Tasmanian Government agencies, as listed in Schedule 1 of the *State Service Act 2000*. Other organisations may choose to adopt this Policy as good practice.

The Policy is supported by Tasmanian Government standards, including common approaches to identity, access to systems and information security classification. The *Tasmanian Government Cloud Risk Assessment Guide* provides detailed guidance to support implementation of the Policy.

# Context

*This Policy* is a principal component of the Tasmanian Government's Information Management Framework. The framework comprises information management policies, standards, implementation guidance and tools for use by Tasmanian Government organisations. An overview of the Policy's contextual framework is provided below.


Tasmanian Government Information Management Framework
Information Management Policy
Cloud Policy
Cybersecurity Policy
Open Data Policy
Archives Appraisal Statement
Tier 1: Policies
Information assets
Information security classification
Metadata
Cybersecurity
Information and records management
Storage
Digital preservation
Destruction methods
Tier 2: Standards
Legislation
Toolkits may include …
Appraisal
Business continuity
Cloud Risk Assessment Guide
Cybersecurity
Cybersecurity incident management
Data exchange
Digital preservation
Disaster preparedness and recovery
Information asset register
Legacy records
Legislative obligations
Open data
Metadata and classification
Retention and disposal
Risk
Roles and responsibilities
Storage
Toolkits may be …
Templates
Training
Checklists
Videos
Infographics
Weblinks
Tier 3: Implementation

# Policy statement

*The Tasmanian Government* will adopt a cloud-first, value-for-money and risk-based approach to the implementation of ICT services and solutions.

Cloud service and solution options may be located off-island and the risk assessment must include consideration of cybersecurity and data sovereignty risks.

Preference will be given to on-island cloud services and solutions assessed as offering equivalent value-for-money and risk profiles as off-island alternatives.

# Responsibilities

*Each Tasmanian Government Head of Agency* is responsible for ensuring their organisation complies with the following:

1. Include cloud services as part of the options analysis for new and replacement ICT services and solutions to meet business needs, and undertake total cost of service assessment and total life-cycle risk assessment of the options identified
2. Choose cloud services in preference to other options in circumstances where the cloud services represent best total cost of service and mitigation of risk
3. Procure cloud services through standard procurement processes that consider cost, risk, benefit and local impact, as defined by the Treasurer's Instructions*
4. Incorporate transition to cloud services in internally developed and managed digital and ICT strategies and roadmaps, including mitigation strategies for managing use and for managing multiple environments in a hybrid cloud scenario
5. Report to the Digital Services Board, at least annually, on the uptake of cloud services.

**Note*: *The relevant Treasurer's Instructions require that agencies use the Networking Tasmania whole-of-government panel contracts, where they exist. At the time of publication of this Policy, whole-of-government panel contracts are in place for DCaaS and IaaS, but not PaaS and SaaS. DCaaS and IaaS services must therefore be procured through the panel. Suppliers may provide their own services or sub-contract or broker services from other suppliers.*

*The Digital Strategy and Services division of the Department of Premier and Cabinet* is responsible for:

1. Establishment and ongoing management of whole-of-government Networking Tasmania contracts for cloud services
2. Management of Networking Tasmania core infrastructure components to meet the dependency, criticality and information security needs of Tasmanian Government agencies
3. Cybersecurity risk management of whole-of-government service providers
4. Development and dissemination of advice and guidance to agencies in relation to relevant industry trends, implementation, risk assessment and appropriate mitigation strategies

# Principles

This Policy endorses the Australian Government's principles-based approach for the adoption of cloud services:

| | |
|---|---|
| *Make risk-based decisions when applying cloud services* | Risk-based decisions are required to understand the security needs of a cloud service and to apply the appropriate security controls. |
| *Design services for the cloud* | Cloud techniques increase the speed at which resources can be accessed and used, reduce manual tasks through automation, and allow applications to be run independent of the infrastructure, enabling more opportunities for the provision and expansion of services. |
| *Use as much cloud as possible* | Agility comes from models that leverage standardised cloud technologies, which allows agencies to keep pace with industry disruptions and innovation cycles, as well as maintaining business process and technology currency. |
| *Avoid customisation and use services 'as they come'* | Agility comes from using the service 'as it comes' without the introduction of bespoke processes that erode the business agility of the service by adding complexity and requiring intervention during change cycles. |
| *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 needed to provision, configure, backup, restore, patch, update and deploy services. |
| *Monitor the health and usage of services in real time* | Monitoring allows agencies to have visibility of their cloud usage and cloud health, and enable them to control costs. |

# Benefits

Implementation of this Policy is expected to enable achievement of the following benefits:

- improved agility – making it easier for agencies to scale resources up or down as required
- improved customer service – with greater potential to store and share data to gain insights into clients' needs and resolve issues
- increased workplace mobility – as cloud services support access from any location
- improved data sharing – by enabling common and consistent solutions across government agencies
- increased workplace collaboration – by making it easier to liaise and collaborate with staff across different agencies, in different locations and with external stakeholders
- improved relationships with vendors – by providing greater clarity on responsibilities and opportunities
- improved security – better processes and approaches to ICT and cybersecurity risks support security improvement
- increased confidence in speed of delivery – reduced downtimes and the ability to release new service iterations during business hours
- increased standardisation of ICT policy and process implementation and/or change across government.

## REFERENCES

Mell, P and Grance, T (2011) *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*. National Institute of Standards and Technology. Gathersburg, US. Available at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

SAI Global (2009) *AS/NZS ISO 31000 Risk management – Principles and guidelines*. Available at Standards Select, accessible through: <http://www.dpac.tas.gov.au/divisions/digital_strategy_and_services>.

Digital Transformation Agency (2017) *Secure Cloud Strategy*. Australian Government. Available at: <https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/cloud/secure-cloud-strategy.pdf>

## DOCUMENT HISTORY

| Version | Date | Comments |
|---|---|---|
| 2.0 | 20200220 | Finalisation for approval |

## AUTHOR

Digital Strategy and Services, Department of Premier and Cabinet

## POLICY REPLACES

*Tasmanian Cloud Policy V1.0* (October 2015)

## POLICY AUTHORISATION

Tasmanian Government Cabinet

## MONITORING PROGRESS OF POLICY IMPLEMENTATION

Monitoring will occur through the Tasmanian Government's digital services governance framework

## POLICY MAINTENANCE

Digital Strategy and Services, Department of Premier and Cabinet

## POLICY ISSUED

June 2020

## REVIEW DATE

No later than January 2022, or earlier if required

## CREATIVE COMMONS STATEMENT