Tasmanian Government Cloud Policy

Risk Assessment Guide

VERSION 1.0

MARCH 2020

Department of Premier and Cabinet

Tasmanian Government

Contents

GLOSSARY 3

PURPOSE 4

RISK MANAGEMENT 4

RISK MANAGEMENT PROCESS 5

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.
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.
NTIII	Networking Tasmania III (NTIII) refers to the Tasmanian Government's outsourced, managed data network arrangements, comprising a number of contractual agreements with suppliers for the delivery of data network and information and communications technology (ICT) services.
Risk-based	Risk based activities involve prioritised decision-making according to the level of risk and the risk tolerance of the organisation.
Risk management	Risk management refers to organisational arrangements for identifying, analysing, evaluating, monitoring, reporting and mitigating risks.
Risk management framework	A risk management framework comprises the foundational components and organisational arrangements for the design, implementation, monitoring, review and continuous improvement of risk management in an organisation
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.

Purpose

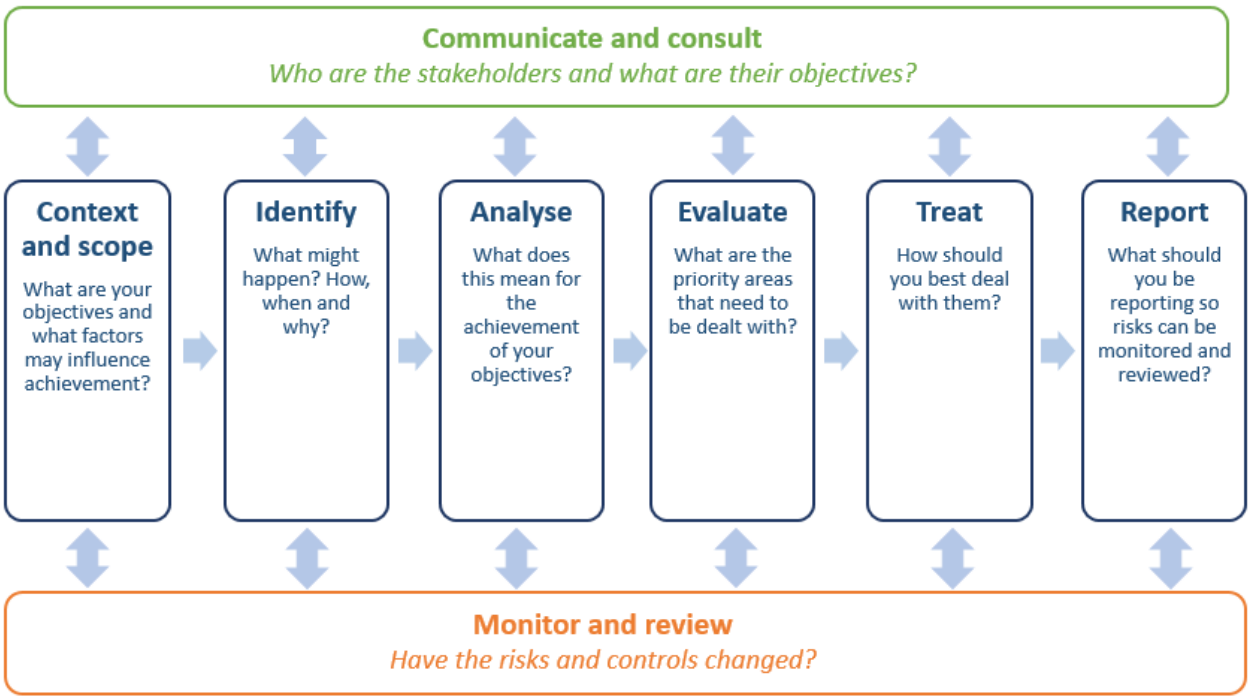
This *Risk Assessment Guide* was developed as a companion document to support implementation of the *Tasmanian Government Cloud Policy*. It provides guidance information and tools to support a common approach to cloud risk assessment procedures undertaken by Tasmanian Government agencies. The intended audience includes relevant executive managers and business system owners, and ICT, information and finance managers.

Risk management

AS/NZS ISO 31000 Risk management – Principles and guidelines defines risk as the effect of uncertainty on objectives. In a Cloud Policy context, adoption of a risk-based approach by agencies will encourage more effective and informed decisions about the selection of cloud-based services, systems or software to support the achievement of organisational objectives.

The relevant Treasurer's Instructions require that agencies use NTIII whole-of-government panel contracts, where they exist. At the time of publication of this Guide, whole-of-government panel contracts are in place for DCaaS and IaaS. While NTIII contract services are required to meet the Tasmanian Government's minimum legal, service level and cybersecurity requirements, services may not necessarily meet specific agency business needs and risk profiles without further consideration. As such, business owners must assess and manage their particular risks.

A summary of steps in the ***risk management process*** is provided in the diagram below, with more detailed information provided in the next sections of this document.



Risk management process

1. COMMUNICATE AND CONSULT

Understanding the perspectives of all stakeholders is critical to understanding the nature, severity, likelihood and potential impact of risks, and for identifying strategies for risk mitigation.

Cloud risk assessments should include the perspectives of organisational stakeholders responsible for:

- business systems (owners and users)
- finance
- security
- information technology
- information management
- business continuity.

2. ESTABLISH CONTEXT AND SCOPE

Before risks can be identified and analysed, it is important to define goals and objectives, as well as all the internal and external factors that may influence the successful achievement of both objectives and target outcomes.

2.1 External context

External factors that impact on, or present risks to, the initiative must be considered in risk assessment and management. Factors may include the impact of policies or related initiatives, for example, the Tasmanian Government Cybersecurity Policy or the Office of the State Archivist's policies and guidelines.

The scope of a cloud risk assessment might include the following broad risk areas:

- business
- information management
- information technology
- strategic
- operational
- legislative and regulatory.

2.2 Internal context

Internal and organisational risk factors may include:

- policies, standards and guidelines that may assist or hinder cloud service take-up
- ICT architecture and technical constraints
- availability of support resources, including funding and staffing
- internal culture, including risk and security culture
- agency readiness to support and manage cloud services once implemented: skills, funding, technology
- level of expertise in risk management.

2.3 Definition of risk evaluation criteria

This step includes defining the criteria – ***consequence, likelihood, control effectiveness*** *and* ***risk rating*** – against which risks will be analysed and assessed. The in-house risk management frameworks of most agencies include predefined criteria that should be used as a basis for cloud risk assessments.

Consequence assesses the risk's impact, usually shown as a matrix that relates the type and severity of impact:

Severity of impact	Type of impact				
	Financial	*Legal/compliance*	*Stakeholder*	*Business cost/performance*	*Project*
Extreme					
Major					
Moderate					
Minor					
Insignificant					

Likelihood is an assessment of certainty that the risk will materialise:

Likelihood	Description
Almost certain	Expected to occur
Likely	Could occur on balance of probability
Possible	Could occur, but may not
Unlikely	May occur but not anticipated
Rare	May only occur in exceptional circumstances

Control effectiveness assesses the collective usefulness of controls (policies, procedures, systems, checklists, processes, etc.) in reducing the likelihood and/or consequence of the risk:

Effectiveness rating	Description
Ineffective or non-existent	Controls are not at all effective: no effect on likelihood/consequence
Defective or negligible	Partial control in some circumstances: overall very little effect
Partially effective	Partial control most of the time: overall some effect
Reasonably or mostly effective	Effective in most circumstances: reasonably significant effect
Effective	Fully effective at all times: significantly reduced likelihood/consequence

Risk rating is calculated by multiplying consequence with likelihood to determine a rating, as below:

Likelihood	Consequence				
	Insignificant	*Minor*	*Moderate*	*Major*	*Extreme*
Almost certain	Moderate	Moderate	High	Extreme	Exterme
Likely	Low	Moderate	High	High	Extreme
Possible	Low	Moderate	Moderate	High	High
Unlikely	Minimal	Low	Moderate	Moderate	Moderate
Very unlikely	Minimal	Minimal	Low	Low	Moderate

Rating	Action required
Extreme	Immediate action required; risk reduction strategies to be identified & implemented before project is approved
High	Immediate action required; risk reduction strategies to be identified & implemented before project is initiated
Moderate	Senior management attention required; risk reduction strategies to be identified & implemented during project execution planning
Low	Management responsibility must be specified; risk reduction strategies to be identified & costed for possible action if funds permit
Minimal	Manage by routine procedures; no additional action required

3. RISK IDENTIFICATION

Risk identification is the process of recognising and describing events, circumstances and sources of risks that could influence the achievement of objectives, as well as possible causes and potential consequences. Risk identification can be based on historical data, theoretical analysis, informed opinions, expert advice and stakeholder input.

The type of questions used to identify risks may include:

- What could go wrong?
- What would cause this to occur?
- What would the effect on objectives be?
- How likely is this to occur?

4. RISK ANALYSIS

Risks must be analysed to better understand the likelihood, severity and potential consequences of risks and how these can be mitigated.

Risks raise questions that should be answered by the agency and/or potential vendor/s. Responses to these questions will help agencies to better understand risk likelihood, severity and potential consequences.

Risk analysis involves:

- The ***inherent risk rating*** of identified risks is determined by combined analysis of consequence and likelihood. This rating is determined before taking into account the effect of any mitigating or preventative controls.
- Key mitigating or preventative ***controls*** – policies, procedures, systems, checklists, processes, etc – for each risk are identified.
- The ***control effectiveness*** of identified controls is assessed.
- The ***residual risk rating*** of identified risks is determined after the effectiveness of identified controls is taken into account, being the expected level of risk remaining after control activities are applied.

5. RISK EVALUATION

Risk evaluation determines whether a risk requires further treatment. This is determined by comparing residual risk rating with the organisation's predetermined level of risk tolerance:

- Risks within tolerance are accepted.
- Risks above tolerance are treated.

If risk tolerance has not been predetermined, consultation with key internal stakeholders should be conducted to determine an acceptable and agreed level of tolerance.

6. RISK TREATMENT

The objective of risk treatment is to modify the risk by selecting and implementing treatment option/s. Broad treatment options may be considered, for example:

Avoid	Treat the risk by avoiding the event that would lead to the risk. This treatment may be appropriate if a particular activity has a significant number of high or extreme risks and the consequences of these outweigh the benefits.
Mitigate	Treat the risk by reducing the frequency (likelihood) or severity of impact (consequence).
Share	Treat the risk by transferring to a third party either: responsibility for undertaking a particular activity (outsourcing); or the consequence of a risk eventuating (insurance)
Tolerate	Reasons for tolerating risk include: • No other available treatment options • likelihood is so low that treatment is not warranted • consequence is insignificant enough that the use of treatment resources is not warranted • cost of treatment exceeds consequential cost should the risk occur

7. RISK MONITORING AND REVIEW

Risk monitoring and periodic reporting to governance groups are critical elements of risk management.

REFERENCES

Tasmanian Government (2019) *Tasmanian Government Cloud Policy.* Department of Premier and Cabinet.

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>.

DOCUMENT HISTORY

Version	Date	Comments
1.0	20200220	Finalisation for approval
D	20190912	Minor amendments
C	20190823	Refinement
B	20190802	Incorporation of feedback
A	20190718	Initial draft

AUTHOR

Digital Strategy and Services, Department of Premier and Cabinet

SUPPORTS

Tasmanian Government Cloud Policy V2.0

CLOUD POLICY AUTHORISATION

Tasmanian Government Cabinet

MONITORING PROGRESS OF IMPLEMENTATION

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

MAINTENANCE

Digital Strategy and Services, Department of Premier and Cabinet

ISSUED

March 2020

REVIEW DATE

No later than January 2022, or earlier if required

CREATIVE COMMONS STATEMENT