



Webinar

*Mike Mitchelmore*

# Getting the Most From Your Cloud Investment



# Agenda

Today's webinar will be a broad discussion around the following points of interest:

- The Cloud environment - who, what, and how do you use Cloud
- Why are the Cloud contract terms and conditions important to IT
- Planning for the tools that allow you to manage Cloud
- How do you ensure value from SaaS and PaaS and when is IaaS a value proposition.
- Security, privacy, and data sovereignty.
- Storage and retrieval of data.
- Service continuity.

# Defining Cloud Management<sup>1</sup>

Cloud management is the process of maintaining control and oversight of Cloud computing infrastructure, resources, and services in public, private, or hybrid Cloud environments. With Cloud management tools and technologies, IT administrators achieve control, visibility, and scalability while also being able to adapt rapidly to change.

<sup>1</sup> <https://cloud.google.com/learn/what-is-cloud-management>

# Challenges in Managing Cloud

**Interoperability** – avoid silos

**Cloud Sprawl** – maintain control

**Cost Assessment** – understand the real costs

**Security and Privacy** – understand and manage the risk

# Defining Cloud Use

*How do organisations use Cloud – Why is this important?*

Business and/or IT	Development	Testing	Production
SaaS			✓
PaaS		✓	✓
IaaS	✓	✓	✓

*What is the difference between business as usual and 'production'?*

# Manage the Vendor and the Contract for Cloud

Understand the difference between:

- Strategic partnership
- Transactional relationships

Understand the need for your Cloud Service Provider to report on:

- Upgrades and patch management
- Security patching
- Disaster recovery
- Cyber incident

Data stewardship versus ownership:

- Sovereignty
- Privacy

# How Does a Cloud Provider Contract Impact You?

Review your Cloud provider contracts to determine the impact the contract has on:

- **Location of Data:** is the data held under data sovereignty requirements. Is data replicated to on-premise or multiple Cloud providers.
- **Location of Cloud Data Centres:** is the Cloud architecture Global or Local, if local where are the data centres and what are the risks.
- **Contracted Recovery Time Objective (RTO) and Recovery Point Objective (RPO):** know the contract clauses around RTO and RPO, and how are they verified.
- **Security Compliance:** do you have specific security requirements; do you have restrictions on who can access your environment.
- **Patching and Upgrades:** service levels and RACI to manage the patching and periodic upgrades of the service.

# Monitoring the Cloud

Tool selection to manage:

- Performance
- Observability
- Automation
- Analytics
- Security
- DevSecOps
- FinOps



# Managing Cloud Starts with Architecture

Tool planning in the Cloud starts with design – use your provider to design for monitoring.

## Example sites:

- [Cloud Architecture Center | Google](#)
- [Azure Arc | Microsoft Learn](#)
- [APM Tool – Amazon CloudWatch – AWS](#)
- [Management and Operations | Oracle](#)
- [What is Cloud Management? | IBM](#)

# Open Source Monitoring Tools

<https://www.cloudzero.com/blog/cloud-computing-tools/>

[7 Best Cloud Analytics Tools for 2024 \(Paid & Free\) \(comparitech.com\)](#)

[Best Cloud Management Software - 2024 Reviews & Pricing \(softwareadvice.com\)](#)

[Best Cloud Management Platforms in 2024: Compare Reviews on 130+ Products | G2](#)

# FinOPS<sup>2</sup>

An operational framework and cultural shift that brings technology, finance, and business together to drive financial accountability and accelerate business value realisation through cloud transformation.

- FinOps enables enterprises to drive financial accountability and maximize business value.
- FinOps helps understand the complexity and challenges to traditional IT financial management.
- FinOps helps to identify the building blocks and key success metrics for business value realisation.

<sup>2</sup> <https://cloud.google.com/learn/what-is-finops>

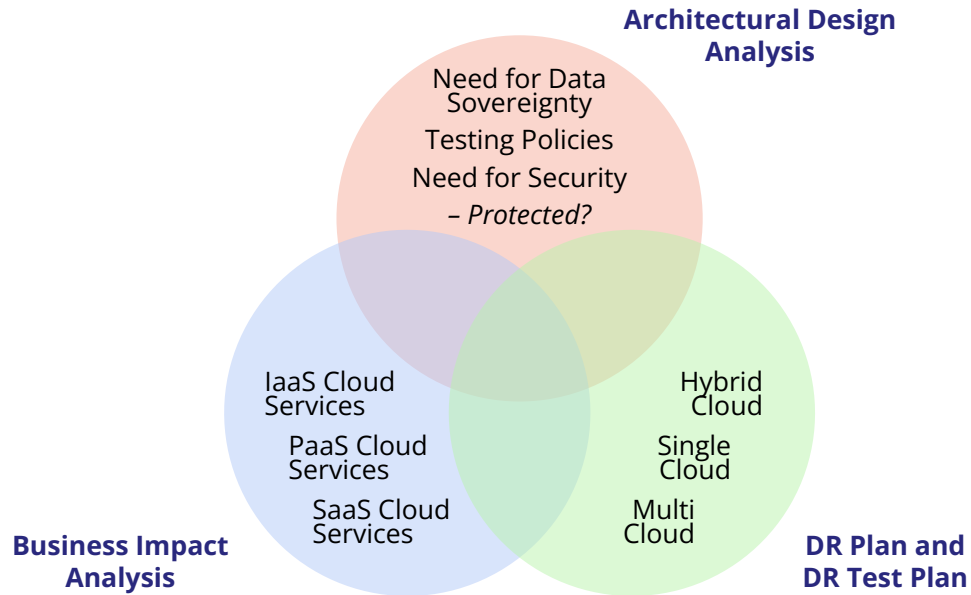
# Privacy, Security, and Data Sovereignty

- Know the contract conditions around privacy, security and data sovereignty.
- Shape and drive the agenda with communication service providers (CSP).
- Understand the risks and how to mitigate them.

# Data Data Data

- Data Storage
- Data Retrieval
- Data Stewardship
- Data Analytics
- Data Vault

# How You Engage in Disaster Recovery (DR) for Cloud



# Next Steps

- A. Convene a workshop to discuss your current Cloud approach and how it is managed (or not).
- B. Convene a workshop with architecture and contract/vendor management to determine the current aspects of Cloud covered under the agreements you have in place.
- C. If your organisation currently subscribes to IBRS, request a whiteboard session to work through the challenges and opportunities to improve your maturity in a Cloud environment.
- D. Conduct a roundtable discussion with business leaders to clarify the risk exposure and the need for improvements in the approach to management of Cloud and your maturity level.
- E. Develop an action plan to improve your Cloud maturity.

# Q & A



*Submit an inquiry or schedule  
a whiteboard session*



IBRS is a boutique Australian ICT Advisory Company.

We help our clients mitigate risk and validate their strategic decisions by providing independent and pragmatic advice while taking the time to understand their specific business issues.

<https://ibrs.com.au>   [info@ibrs.com.au](mailto:info@ibrs.com.au)   02 4758 9111   PO Box 519, Hazelbrook NSW 2779, Australia

© IBRS 2024

All Rights Reserved. This document and its entire contents may be used for information and educational purposes only.

All images remain the property of original copyright holders.