Choosing a Cloud Provider - Your Top Four Considerations

When choosing your Cloud IaaS provider there are a range of factors to consider. These essential areas are especially relevant when you provide services to organisations that have high data security requirements (such as Government and/or Critical National Industry organisations).

1. Cloud Commercials

Pricing

A founding principle of cloud services is that you should only ever pay for what you use. For example, you should be able to save money by scaling VM sizes up or down or even turning off VMs you are not using. Just powering down VMs when they are not in use outside business hours (typically >70% of the time) can deliver immediate efficiencies.

- Does your Cloud Provider charge you on a pay as you use basis?
- Can you check what you are using at any point in time with visibility of up to the last hour?

Not all Cloud Providers offer the same charging regime.

- What do the prices you are charged include?
- Are there any hidden or additional costs, e.g., ingress or egress fees, data migration or exit fees?

Lock-in

While you are looking for a Cloud Provider to meet your needs now, this may not be the case down the track as your needs and the needs of your customers change. NIST[1] defined Cloud Providers must provide commercial as well as technical flexibility and adaption. Cloud is also a competitive market and you want to ensure you have the flexibility to move if you are not satisfied with the service.

- Can you purchase a single unit of compute for one hour, a Gigabyte of data for one month or sign-up a single user for a month or do you have to commit for a month, a year or even longer?
- How flexible is the Cloud Provider – can you move your data to another Provider if necessary or are there contractual issues preventing or hindering this?

[1] National Institute of Standards and Technology, NIST. https://www.nist.gov

Some Cloud Providers not only hide lock-in into their hidden pricing costs but also, as an alternative to adaptable, open-source solutions, provide proprietary services that, while useful now, effectively act as technical lock-in to prevent you moving to other services and Cloud Providers if your requirements change.

- What is the process to exit your Cloud Provider?
- How easy (or difficult) is it to unpick the variety of services and/or migrate your data?
- How confident are you that all you customer data, meta-data, monitoring data and other derived data have been destroyed beyond the Cloud Provider's future access?

2. Information Security and Governance

Sovereignty

If you are providing services to Government you will almost certainly need to ensure your Cloud Provider can guarantee that both your data and all the associated metadata, analytics and monitoring data will remain in Australia, on infrastructure owned and managed by Australian citizens.

- Do you know where your data goes – including the metadata, the monitoring data and the derived data?
- Is your Cloud Provider subject to extra-territorial jurisdictional (i.e., non-Australian) laws?
- Can a foreign government or authority request access to your data, from your Cloud Provider without your consent or even knowledge?
- Will all the service and support from your Cloud Provider (and their staff who have access to any of your data) be provided from within Australia by Australian citizens operating only under Australian law?

Governance

The relationship between you and your Cloud Provider is more than the sum of the commercial contracts and the technical agreements. It is based on trust around delivering confidentiality, integrity and availability of the service and related data combined with understanding of the relative roles and responsibilities.

- Do you know and are you confident with the maturity of your Provider's security operations and governance processes?
- Are the roles and responsibilities of you and your Cloud Provider documented and clear?
- Have you checked that user access and activity is fully auditable?

Relevant certifications (e.g., ISO27001) are a good indicator that the Cloud Provider is committed to best practice in information security, especially where the certification applies across all aspects of the organisation, end to end development, management, operation and security of information systems and infrastructure as well as service delivery.

- What certifications does your Cloud Provider hold that provides you with the confidence that can meet your information security, privacy and operational service delivery needs?
- If your provider is selling their capability based on non-Australian reference cases and attestation, are they capable of exact replication of the infrastructure, processes and people in Australia?
- How else is your Cloud Provider demonstrating compliance with any mandatory or regulatory infrastructure, security and privacy requirements (e.g. the ISM, PSPF, IRAP)?

Information Security

The nature of your service or the data you have access to, may be subject to a specific data classification security requirement.

- Can your Cloud Provider meet your needs and accommodate you if there are any changes?
- Has your Cloud Provider demonstrated that they comply with the Australian Attorney General Departments' Protective Security Policy Framework (PSPF) underpinned with controls outlined within Australian Signals Directorate's Information Security Manual (ISM)? Compliance with these is mandatory when working with government.
- Has your Cloud Provider demonstrated compliance with the new ASD/ACSC security assessment framework to OFFICIAL and PROTECTED controls?

3. Architecture and Operations

Scalability

A key benefit of Cloud IaaS is that you can 'right-sized' your infrastructure from the outset to ensure you only purchase the VMs you need but that you can scale up when you need more capacity or need to support more users.

- Does your Cloud Provider have the technical adaptability and commercial elasticity for you to scale up and/or down on demand?
- Are you confident they can scale to meet your needs as you grow or adjust instantly to unanticipated demand?

Automation and Orchestration

Automation and orchestration allow you to optimise the efficiency of your cloud-based operations through auto-sizing or tiering of your environments to suit your applications' needs.

- What automation and orchestration features does your Cloud Provider offer? For example, can you automatically tether capacity to a schedule or directly to demand?
- Do you have access to API based, Infrastructure-as-Code capabilities to run, scale, network and modify your infrastructure to reduce the pressure on and errors from your technical resources?

4. Infrastructure Design

Data Centres

Data centres are a key physical asset that not only underpins physical security but also provides one element of the jurisdictional status of your data's security. If you re providing services to Government, check your Cloud Provider operates from a Data Centre that is Australian owned, operated and located in Australia.

- For geo-resilience and business continuity purposes, is your Cloud Provider operating from multiple (at least 2) Data Centres, located in geographically and power-grid separated sites, inter-connected by low latency, redundant fibre?
- For Government and Critical National Industries, is your Cloud Provider operating within a Certified Sovereign Data Centre?

Multi-Layer Security

You cannot afford for the security of your data to be compromised. Check your Cloud Provider has incorporated security-by-design features that are built into all levels of the infrastructure from physical set-up, to network and hosting layers and related standard operating procedures.

- What advanced security features does your Cloud Provider have available?
- Do you need: sophisticated security monitoring that supports intrusion detection, prevention, alerts, analysis and response capabilities; multi-factor authentication; data encryption; and policies and procedures that stipulate the scope and behaviour of the broader cloud community?

Ultimately, your chosen Cloud IaaS Provider needs to meet your specific business, security and technical needs. While the above is not exhaustive, it provides a useful guide to assist you choosing a Cloud Provider that meets your needs, the needs of your customers and protection of their data.

About AUCloud

AUCloud is a sovereign cloud Infrastructure-as-a-Service (IaaS) provider, exclusively focussed on the needs of the Australian Government and Critical National Industry (CNI) communities. Operating from ASIO T4 standard geo-resilient sovereign certified data centre campuses In Canberra and Sydney, AUCloud provides two independent environments: an OFFICIAL Data Community Environment (ODCE) and a PROTECTED Data Community Environment (PDCE), both are IRAP assessed to the PROTECTED level controls of the Australian Signals Directorate (ASD) Information Security Manual (ISM).

AUCloud solutions enable customers to benefit from sovereign data protection with the scale, automation, elasticity and lower costs typically associated with global cloud offerings.

AUCloud is ISO27001 certified across all technical and business areas of the organisation; VMware Cloud verified; and recognised as a Cisco Master Partner for Cloud and Managed Services.

For more information to assist you select the right Cloud Provider for you, contact us for more information

- sales@australiacloud.com.au
- 1800 282 5683