Security Considerations when Choosing a Cloud Service Provider

When choosing a cloud service provider (CSP) there are a range of factors to consider. The security of your cloud provider is an essential area for assessment, especially when providing services to organisations that have high data security requirements (such as Government and/or Critical National Industry organisations).

1. Commitment to Security

Cloud adoption comes with its own set of unique changes in the way an organisation operates. One of the most significant is the addition of a CSP to your supply chain. Cloud computing requires a degree of trust in your CSP who is handling your data and potentially has a direct impact on ensuring the confidentiality, integrity and availability of your services.

When choosing a CSP you should ensure that the CSP has made a commitment to security that encompasses more than just the services they provide. It's vitally important that the CSP has demonstrated a commitment to secure-by-design practices and has a strong track record of transparency and implementing security across their own systems, services and supply chains.

- Can they demonstrate their approach to secure technical and application development?
- Do their security practices and methodologies apply to people, process and technology?
- How do they manage their supply chain risks?
- Do they provide a set of community rules to ensure that security responsibility and expectations are clearly defined?
- Do their policies and procedures stipulate the scope and behaviour of their broader cloud community?

2. Sovereignty

If you are providing services to Government and Critical National Industry organisations you will almost certainly need to ensure your CSP can guarantee that both your data and all associated types of data – customer data, metadata, account data and analytics and monitoring data will remain in Australia, on infrastructure owned and managed by Australians.

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

3. Governance

The relationship between you and your CSP 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 an understanding of respective roles and responsibilities.

- Do you know and are you confident of the maturity of your CSP's security operations and governance processes?
- Are the roles and responsibilities of you and your Cloud Provider documented and clear?
- Is there a clear understanding of the shared responsibility nature of cloud operations?
- Have you checked that user access and activity is fully auditable?

Relevant certifications are a good indicator that the CSP is committed to 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 CSP have that provide confidence that they can meet your security, privacy and operational service delivery needs?
- Check the detail - are you consuming a global service or something that meets the specific needs and requirements of an Australian organisation?
- How else is your CSP demonstrating compliance with any mandatory or regulatory infrastructure, security and privacy requirements (e.g. ISO 27001, ISM, PSPF, CPG 234)?

4. Cyber Security

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

- Can your CSP meet your needs and accommodate you if there are any changes?
- Has your CSP demonstrated that they comply with security requirements such as the Australian Attorney General Departments' Protective Security Policy Framework (PSPF) underpinned by controls outlined within the Australian Signals Directorate's Information Security Manual (ISM)? Compliance with these is often mandatory when working with government.

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

- What advanced security features are available?
- Do you need sophisticated security monitoring that supports intrusion detection, prevention, alerts, analysis and response capabilities; multi-factor authentication; and data encryption?

Ultimately, your CSP needs to meet your specific business and technical needs. While the above is not exhaustive, it provides a useful guide to assist you in choosing a CSP that meets your security needs, the security 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 about security considerations when choosing a cloud service provider, contact us directly

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

Data Security
is our DNA

australiacloud.com.au