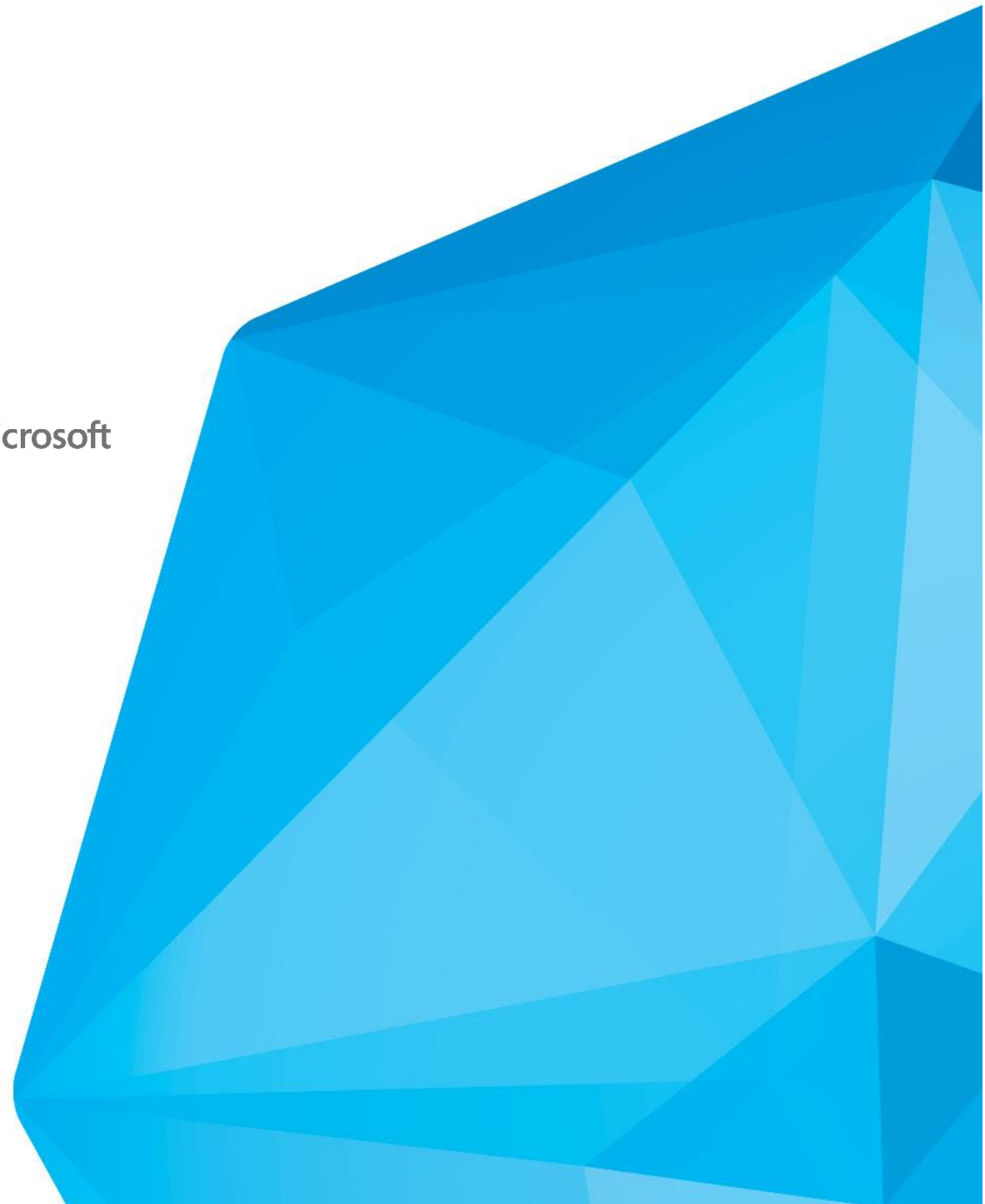
Microsoft Azure Compliance

In the context of Australian Security and Privacy Requirements



Disclaimer

October 2017

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. Customers reading this document bear the risk of using it.

This document does not provide customers with any legal rights to any intellectual property in any Microsoft product. Customers may copy and use this document for their internal, reference purposes.

The information contained in this document must not be construed as legal advice. Customers must seek their own legal counsel for advice on compliance with regulatory requirements impacting their organization

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

NOTE: Certain recommendations in this paper may result in increased data, network, or compute resource usage, and may increase a customer's license or subscription costs.

Audience

This white paper is intended for IT decision makers in Australia, and provides them with information about how Microsoft Azure addresses their country's compliance, security, and privacy requirements.

Acknowledgements

Authors

Frank Simorjay
Eric Tierling
Peter Foote (Cadence Preferred)

Contributors and Reviewers

Yen-Ming Chen
Dzahar Mansor
Glenn Pittaway
Dan Ryan
Tom Shinder
Andrew Cooke
Ben Gilbert
Katie Jackson
Stevan Vidich
Katie Look

Executive Summary

Microsoft Azure is a trusted cloud-based platform that provides Microsoft customers with the ability to realize the benefits of cloud computing. This white paper addresses questions posed by customers in Australia who are considering a move to the cloud. Questions about the security of cloud data, where data is stored, how it is used, and who can access it are common. These types of questions usually relate to one of three areas – compliance, security, and privacy.

For customers who are concerned about compliance in Australia, Azure complies with three pieces of Australian legislation, including the Certified Cloud Services List, the Protective Security Policy Framework, and the Privacy Act 1988. This compliance means both government and commercial customers can have confidence knowing they comply with Australian legislative and certification requirements when deploying data to the cloud.

Security is increasingly a primary focus for customers when contemplating the cloud. Microsoft Azure provides multiple levels of security, starting with physical protection of datacenter locations to protect against physical intrusion, power failure, and network outages. Azure uses encryption to protect data in transit and at rest, and extensive monitoring and logging provides operational staff and customers with visibility into the environment. Microsoft designs and operates Azure using security best practices, which are embodied in programs such as the Microsoft Security Development Lifecycle (SDL), Microsoft Operational Security Assurance (OSA), and an "assume breach" strategy. Together, these programs and strategies help ensure that Azure is resilient to attack. Microsoft has received ISO/IEC 27001 security certification, which validates the benefits of this approach.

With the global nature of the cloud, customers want to know their privacy is assured. Microsoft Azure sets and adheres to stringent privacy standards such as ISO/IEC 27018, which, among other things, assures customer data is never used for advertising. Should customers have concerns over data sovereignty, Azure provides complete control over where their data lives by allowing them to choose from 34 Azure regions (as of the time of this publication) in Asia, the Americas, and Europe. In addition, Microsoft does not provide any third party with direct or unfettered access to customer data[1], and always attempts to redirect government requests for data to the customer. Finally, tenant isolation and strict access controls help ensure that, by default, only customers can access their data.

Although Microsoft Azure addresses the compliance, security, and privacy requirements that Australia identifies, some requirements are the responsibility of the customer, such as controlling administrator passwords, and it is important for customers to understand the shared responsibilities associated with Microsoft Azure.

[1] https://www.microsoft.com/en-us/TrustCenter/Privacy/You-own-your-data#subcontractors

Table of Contents

Introduction

This paper is written for IT decision makers in Australia who are considering whether to move their data to Microsoft Azure, and answers several typical questions:

- Does Microsoft Azure meet Australian compliance requirements?
- Where is data stored and who can access it?
- What is Microsoft doing to protect data?
- How can a customer verify that Microsoft is doing what it says?

The content is divided into three main sections:

- *Australian compliance requirements*. This section focuses on how Azure meets legislative and certification requirements.
- *Key security principles*. This section provides technical information about how Azure addresses key security principles for customers located in Australia, such as encryption and security best practices.
- *Key privacy principles*. This section provides technical information about how Azure addresses key privacy principles for customers located in Australia, such as data location and government requests.

Understanding how Azure shares responsibility with customers to meet Australian security and privacy requirements is an important step toward moving data to the cloud.

Shared responsibilities between Microsoft and customers

When moving data to the cloud, it is important to remember that some security and privacy requirements are the responsibility of the customer, some are shared, and some are the responsibility of the cloud service provider (CSP). Read the Shared responsibility in cloud computing white paper to learn more about the responsibility for each cloud-based solution.

1. Australian compliance requirements

In October 2014, the Australian Department of Finance released version 3.0 of the Australian Government Cloud Computing Policy. Under the policy, agencies *must* now adopt cloud services for any new ICT services and when replacing existing ICT services, "where it (the cloud) is fit for purpose, provides adequate protection of data and delivers value for money."[2] The Australian Government procures approximately $6 billion of ICT services annually and is committed to leading by example, demonstrating the benefits of investing in and using cloud services.[3]

Although the Australian government has taken a cloud-first approach, it also recognizes the importance of customers performing due diligence prior to moving to the cloud. The following sections describe legislation and standards introduced by the Australian government that customers need to be aware of when moving to the cloud. The Australian Department of

[2] Australian Government Cloud Computing Policy, p4.

[3] Australian Department of Finance Cloud Computing (website).

Finance also has additional guides on their website that discuss such things as implementation, legal, financial, and community issues.

Certified Cloud Services List (CCSL)

The Certified Cloud Services List identifies cloud services that have successfully completed an Information Security Registered Assessors Program (IRAP) assessment by the Australian government, and have been awarded certification by the Australian Signals Directorate (ASD). Microsoft Azure was among the first cloud services to achieve this certification for the storage and processing of unclassified dissemination limiting marker (DLM) data. This certification can be used by all Australian and New Zealand government agencies.

The IRAP is based on the Australian Government Information Security Manual (ISM), which is the standard that governs the security of government ICT systems. With the 2016 release of the ISM by the ASD, it comprises three documents, including:

- Executive Companion (27 pages). This document provides useful information for executives, including an overview of the threat environment, FAQs, and an ISM overview.
- Principles (74 pages). This document details the guiding principles and rationale behind the controls that form the basis of the ISM. It also includes additional sections on areas such as Outsourced IT services, PSPF Infosec-4 explained, and Working Off-site.
- Controls (334 pages). This document details the technical security controls in 14 areas, such as Risk Management, Documentation, Monitoring, Physical and Personnel Security, Media, Email and Network Security, Communications Infrastructure, Cryptography, and Data Transfers.

NOTE: Although the ISM specifically targets government ICT systems, the security principles and controls are equally relevant for commercial customers.

Microsoft Azure compliance

In September 2014, Azure received its IRAP compliance, making it the first IRAP-assessed cloud service in Australia. In April 2015, the ASD announced the CCSL certification of Azure. This certification provides assurance to government customers and their partners that Microsoft has appropriate and effective security controls in place for the processing, storage, and transmission of unclassified (DLM) data, which covers the majority of government, healthcare, and education data in Australia.[4]

Protective Security Policy Framework (PSPF)

On 21st October 2014, the Australian Attorney General issued the "Directive on the Security of Government Business," which requires agency heads to apply the Protective Security Policy Framework (PSPF). The PSPF mandatory requirements "*assist Agency Heads and Senior Executives to identify their responsibilities to manage security risks, provide assurance to the government and the public that official resources and information are safeguarded, and incorporate protective*

[4] Microsoft Trust Center, CCSL compliance page.

security into the culture of their entity."[5]

There is a total of 36 mandatory requirements that relate to governance, personnel, information, and physical security. Although the requirements are the responsibilities of the agency, the PSPF does highlight the importance of the Australian Government ISM,[6] and that "*Agencies must ensure the contracted service provider complies with the requirements of this policy and any protective security protocols.*"[7]

Microsoft Azure compliance
Although the primary responsibility for compliance with the PSPF lies with the customer, Microsoft Azure complies with the PSPF where it relies on the Australian Government ISM standard. In addition, Azure complies with a number of industry standards such as ISO/IEC 27001 (for Information Security Management Systems, or ISMS), ISO/IEC 27018 (for personally identifiable data), Cloud Security Alliance (CSA) Cloud Controls Matrix 3.0.1 (for security and operational risk management controls), as well as other international security and privacy certifications.

Privacy Act 1988

Published in 1988 and updated periodically, the Privacy Act 1988 regulates how personal information is handled. It defines personal information as "*information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable*."[8] It also defines sensitive personal information.

The Privacy Act 1988 applies to Australian Government agencies, all private sector and not-for-profit organizations with an annual turnover of more than $3 million, all private health service providers, and some small businesses.[8]

The Privacy Act 1988 contains thirteen Australian Privacy Principles (APP) that relate to open and transparent management, anonymity and pseudonymity, collection, unsolicited information, notification, use or disclosure, direct marketing, cross border disclosure, adoption of identifiers, quality, security, access, and correction.

Microsoft Azure compliance
Although the primary responsibility for compliance with the Privacy Act 1988 lies with the customer, the Privacy Act 1988 implies specific privacy controls. Azure complies with many international security and privacy certifications, such as ISO/IEC 27018 (for personally identifiable data). For a more in-depth discussion on the Privacy Act 1988 and cloud services, as well as a host of other cloud services topics, refer to the Cloud Computing Regulatory Stock Take, a 90-page document published by the Australian Department of Communications in May 2014.

---

[5] Attorney-General Protective Security Policy Framework Mandatory Requirements (website).
[6] Attorney-General Protective Security Policy Framework, Gov-7 & Infosec-4 (website).
[7] Attorney-General Protective Security Policy Framework, Gov-12 (website).
[8] Office of the Australian Information Commissioner, Privacy Law (website).

Notifiable Data Breaches Scheme

On 22nd February 2017, the Australian Government passed an amendment to the Privacy Act, called the Privacy Amendment (Notifiable Data Breaches) Act 2017, which established a Notifiable Data Breaches (NDB) scheme. The scheme requires organizations covered by the Australian Privacy Act to notify any individuals likely to be at risk of serious harm by a data breach, as well as notifying the Office of the Australian Information Commissioner (OAIC). The scheme will come into force on 22nd February, 2018. The OAIC has a website where more information is available, and where additional guidance will be released as the enforcement date approaches.

Microsoft Azure compliance

The legal team from Microsoft Australia is aware of the NDB scheme and is working to make appropriate changes for Australian customers before its enforcement date.

2. Key security principles

This section provides technical information about how Azure addresses key security principles for customers located in Australia, such as encryption and security best practices.

Azure provides encryption for data in transit and data at rest

Microsoft Azure provides capabilities to help protect data both in transit and at rest. For data in transit, Azure uses the Transport Layer Security (TLS) protocol to encrypt connections between customer and Microsoft datacenters. TLS provides strong authentication, message privacy, integrity (by enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, ease of deployment, and ease of use. Perfect Forward Secrecy is also used so that each connection between client systems and Azure uses unique keys. In addition, Azure Virtual Networks provide the ability to use the industry-standard IPsec protocol to encrypt traffic between corporate VPN gateways and Azure, as well as between the virtual machines (VMs) located on virtual networks.

For data at rest, customers have a number of encryption options available to them, such as hard disk encryption for Windows VMs using BitLocker, and SQL database encryption using Transparent Data Encryption. Azure implements encryption using strong symmetric and asymmetric keys for encrypting and protecting confidentiality of data:

- Software-based AES-256 for symmetric encryption/decryption
- 2048-bit or better for asymmetric keys
- SHA-256 or better for secure hashing

Additional information is available in the Data Protection in Azure white paper (39 pages) and the Is your data safe at rest? video (5 mins).

Microsoft designs and operates Azure using security best practices

From the start, Microsoft designed Azure with security in mind. By taking advantage of the Microsoft Security Development Lifecycle (SDL) during the Azure development process, security concepts such as attack surface reduction and threat modeling are built into the service. From an operations perspective, Microsoft Operational Security Assurance, the "assume breach" strategy, and a global incident-response presence help ensure the Azure infrastructure is resilient to attack.

Vulnerabilities present a significant risk to any information system, particularly those that are exposed to the Internet. One of the initial steps to reducing risk is to understand threats, exploits, and vulnerabilities that target a region. The Microsoft Security Intelligence Report provides intelligence for 106 regions including Australia that can be used to better understand regional risk and exploits used by malicious entities. It is also important for customers to understand that when using Microsoft Azure they must ensure that the IaaS services they use are patched in a timely manner. Improved patch and vulnerability management is often cited as one of the main benefits of moving to the cloud.

Azure provides infrastructure protection

Azure infrastructure includes hardware, software, networks, administrative and operations staff, and the physical datacenters that house it all. Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft online services. Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards such as ISO/IEC 27001 for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel. Third parties undergo a review process and an approved vendor list is established and used. These vendors are required to comply with Microsoft security policies and are audited for compliance.

Customers can take advantage of datacenter redundancy

Customers may opt for in-country storage for compliance or latency considerations, or out-of-country storage for security or disaster recovery purposes. Data may be replicated within selected geographic regions for redundancy. Microsoft recommends replication of workloads across Azure regional pairs to benefit from Azure's isolation and availability policies.

Customers have visibility of their data through monitoring and logging

Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the Azure environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities provide visibility to customers.

Customers can protect their networks

Management workstations and external or less-trusted interfaces of a service should be identified and have appropriate protections to defend against attacks through them. If an

interface is exposed to consumers or outsiders and is not sufficiently robust, it could be subverted by attackers to gain access to the service or data within it. If the exposed interfaces include private interfaces (such as management interfaces), the impact may be more significant.

Azure uses an "assume breach" strategy

One key operational best practice that Microsoft uses to harden Microsoft Azure is known as the "assume breach" strategy. A dedicated team of software security experts simulate real-world attacks at the network, platform, and application layers, testing the ability of Azure to detect, protect against, and recover from breaches. Microsoft has also established a policy for customers to carry out authorized penetration testing on their applications hosted in Azure. Constantly challenging the security capabilities of the service can help Microsoft stay ahead of emerging threats.

3. Key privacy principles

This section provides technical information about how Azure addresses key privacy principles for customers located in Australia, such as data location and government requests.

Microsoft does not use customer data for advertising

Microsoft takes privacy very seriously and never uses enterprise customer data for marketing or advertising purposes. This policy is written into Microsoft Online Services Terms and affirmed by Azure certification to international privacy standard ISO/IEC 27018. Microsoft was the first major cloud service provider to incorporate the ISO/IEC 27018 privacy code of practice. Additional information is available in this 5-minute video: Privacy interview with Brendon Lynch, Microsoft Chief Privacy Officer.

Azure provides logical tenant isolation

Microsoft logically segregates storage and processing for different customers through specialized technology engineered to help ensure that customer data is not combined with anyone else's data, and to help prevent one malicious or compromised customer from affecting the service or data of another. Microsoft also takes strong measures to protect customer data from inappropriate use, access, or loss. Additional safeguards include proper controls for administrative access, such as secure user authentication.

For customers with an existing Azure subscription, additional information about tenant isolation is available in the "Office 365 Tenant Isolation" white paper, located on the Service Trust Portal (STP). The STP offers access to a deep set of security, privacy, and compliance resources, such as independent audit reports of Microsoft Azure, risk assessments, security best practices, and other similar materials.

Microsoft has transparent data-use policies and uses independent audits

The Microsoft Online Services Privacy Statement uses straightforward, transparent language to

provide clarity around Microsoft data-use policies. Azure also undergoes independent audits against international standards such as ISO/IEC 27001, ISO/IEC 27018, and CSA CCM 3.0.1, so customers can have confidence that Microsoft is honoring its commitments. Additional compliance reports are available on the Service Trust Portal.

Customers choose the region where their data lives

Customers have complete control over where their data is stored because they choose which region best meets their compliance needs. Currently, there are 34 Azure regions, including:

- *Asia*: Singapore, Hong Kong, China (Shanghai, Beijing), Japan (Osaka, Tokyo), India (Pune, Chennai, Mumbai), and Australia (New South Wales, Victoria).
- *Americas*: United States (Iowa, Virginia, Illinois, Texas, California), United States Government (Iowa, Virginia), Canada (Toronto, Quebec), and Brazil (Sao Paulo state).
- *Europe*: Ireland, Netherlands, Germany (Frankfurt, Magdeburg), United Kingdom (London, Cardiff).

In addition, Microsoft has announced another 6 Azure regions, specifically:

- US Government (Arizona, Texas), France (two regions – to be announced), South Africa (Cape Town, Johannesburg).

Additional information is available on the Azure Regions webpage.

Customers control access to their data

Microsoft has provided a self-service model for customers to access and manage their data. When Microsoft engineers or subcontractors need access to customer data, such as when troubleshooting an issue, they have to be explicitly granted access by the customer, and access is revoked when it is no longer necessary. The operational processes and controls that govern access to and use of customer data are protected by strong controls and authentication, such as multi-factor authentication, which helps limit data access to authorized personnel only.

Customers may extract their data upon termination of their subscription

If a customer chooses to end a subscription to a service, they are given 90 days to extract their data, after which Microsoft follows stringent standards in purging customer data from systems under its control.

How Microsoft responds to government requests

Microsoft does not provide any third party (including law enforcement, other government entity, or civil litigant) with direct or unfettered access to customer data except as directed by the customer. When a government or law enforcement request for customer data is received, Microsoft policy is as follows:

- Always attempt to redirect the third party to obtain the requested data from the customer. For valid requests that cannot be redirected to the customer, Microsoft discloses information only when legally compelled to do so, and only to the extent specified in the legal order.
- Promptly notify customers of any third-party request and provide a copy, unless legally

prohibited from doing so.

Microsoft never provides any government with its encryption keys or the ability to break its encryption. Additional information is available on the Microsoft Transparency Hub and Principles, Policies and Practices FAQ webpages.

Microsoft sets and adheres to stringent privacy standards

Microsoft cloud privacy is grounded in the Microsoft Privacy Standard (which details Microsoft core privacy requirements and practices) and the Microsoft Security Development Lifecycle (which addresses privacy requirements in the process of developing software). Microsoft backs those protections with strong contractual commitments to safeguard customer data. Additional information is available in this 5-minute video: Interview with Brad Smith, General Counsel, Microsoft: Security & Privacy in the Cloud.

Conclusion

Microsoft strives to be transparent in its compliance, security, and privacy practices. In addition, Microsoft-offers meaningful privacy choices and responsibly manages the data that it stores and processes. The Microsoft commitment to security and privacy of customer data is backed by the Microsoft Online Services Privacy Statement, which describes the specific privacy policy and practices involving customer data in Microsoft enterprise cloud services.

For customers who are concerned about compliance, Azure complies with three pieces of Australian legislation, including the Certified Cloud Services List, the Protective Security Policy Framework, and the Privacy Act 1988. This compliance means both government and commercial customers can have confidence knowing they comply with Australian legislative and certification requirements when deploying data to the cloud.

Microsoft believes that Azure can provide secure and compliant cloud services to meet the needs of government and commercial customers of all sizes.