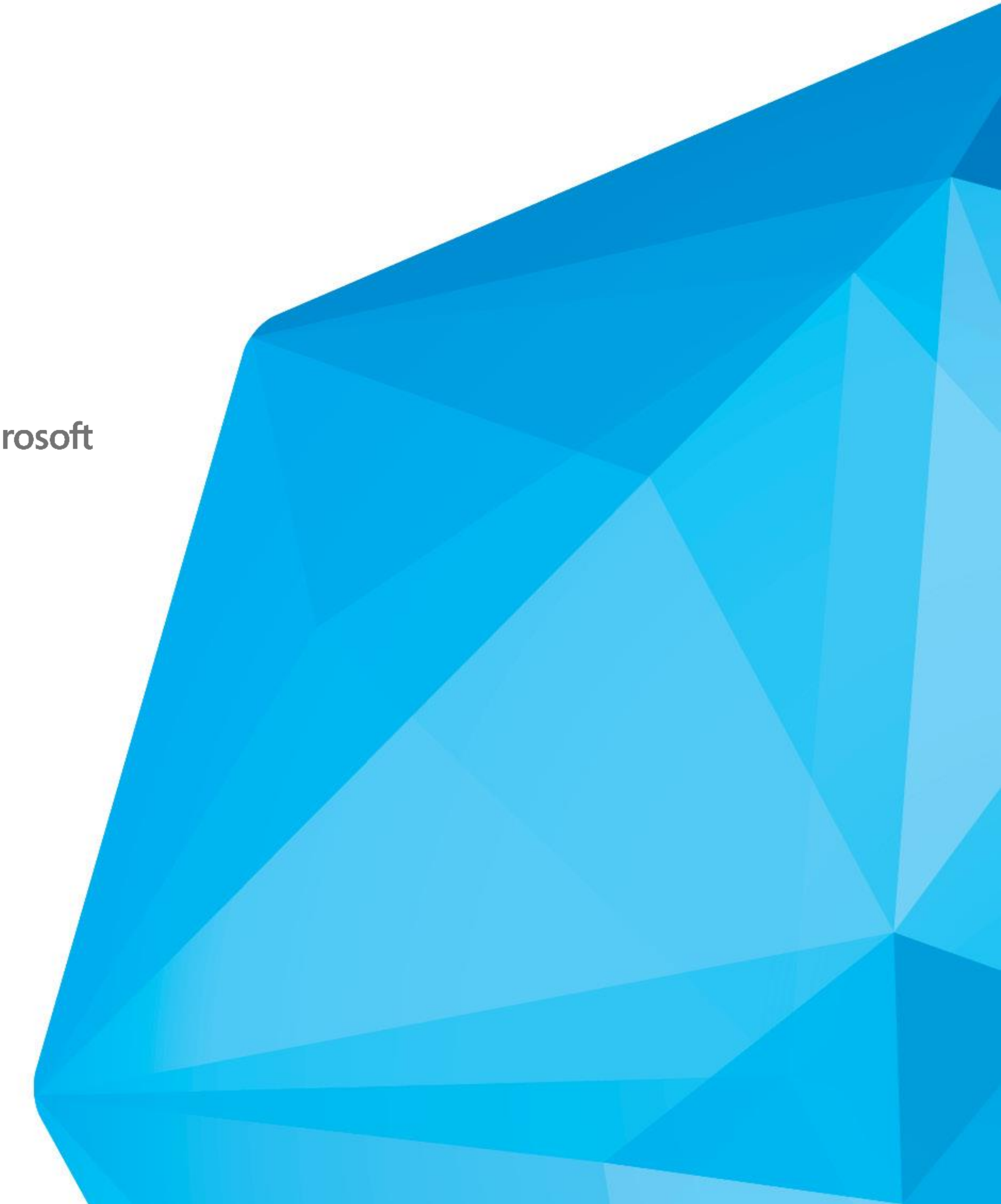
Microsoft Azure Compliance

In the context of New Zealand Security and Privacy Requirements



Microsoft

Disclaimer

Published August 2016

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 whitepaper is intended for IT decision makers in New Zealand, and provides them with information about how Microsoft Azure helps address their country's compliance, security and privacy requirements.

Acknowledgements

Authors

Russell Craig
Frank Simorjay
Peter Foote (Cadence Preferred)

Contributors and Reviewers

Yen-Ming Chen
Dan Ryan
Tom Shinder

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 New Zealand who are considering a move to the cloud. Questions such as how secure is cloud data, where is data stored, how is it used, and who can access it are common. These types of questions usually relate to one of three areas – compliance, security and privacy.

From a compliance perspective, the way Azure is designed, built, operated and independently certified enables government agencies to meet the security and privacy requirements established by three key New Zealand information security and privacy mechanisms: the Protective Security Requirements, the NZ government Cloud Computing Risk & Assurance Framework and the Privacy Act 1993.

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 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 adheres to stringent privacy standards such as ISO 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 26 Azure regions 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 only customers can access their data by default.

Although Microsoft Azure addresses the compliance, security, and privacy requirements that New Zealand 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 New Zealand who are considering whether to move their data to Microsoft Azure, and answers several typical questions:

- Does Microsoft Azure meet New Zealand's 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:

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

Understanding how Azure shares responsibility with customers to meet New Zealand 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. New Zealand compliance requirements

In August 2012, as outlined in the Cabinet minute entitled "Managing the Government's Adoption of Cloud Computing" Cabinet ministers agreed that "an all-of-government 'cloud first' approach be taken for the government's adoption of cloud computing;" (CAB Min (12) 29/8a recommendation 4.1 refers).

In late 2015 Cabinet ministers reviewed the Government ICT Strategy, and agreed to two measures designed to drive adoption of cloud services in government. First, they directed "the Government Communications Security Bureau (GCSB) and the Government CIO (GCIO) to work together to review the Cabinet policy for cloud computing and remove any barriers that may inhibit the accelerated adoption of cloud computing by agencies". Second, they directed "agency Chief Executives to accelerate their agencies' adoption of public cloud services as a way to drive innovation in line with the 'cloud first' policy [CAB Min (12) 29/8A], while balancing the needed to meet agency business requirements." [2]

Microsoft recognizes the need of any agency to undertake appropriate due diligence and risk assessment of cloud services, in accordance with New Zealand security and privacy requirements.

Protective Security Requirements (PSR)

On 8 December 2014, Cabinet approved the Protective Security Requirements. As stated, "The Protective Security Requirements (PSR) outlines the Government's expectations for managing personnel, physical and information security. The PSR will better help you manage business risks and assure continuity of service delivery. The PSR clearly sets out what agencies must and should consider to ensure they are managing security effectively."[3]

In particular, the PSR sets out "Strategic Security Objectives, Core Policies and the Mandatory Requirements for Agencies"[4]. Meeting PSR requirements is the responsibility of agencies. In regard to cloud services these requirements are contained in the New Zealand Government Information in Outsourced or Offshore ICT Arrangements section of the PSR, which states that agencies "must ensure cloud service providers apply the controls specified in the New Zealand Information Security Manual (NZISM) to any systems hosting, processing or storing agency data and systems". Customers should note that Microsoft understands the importance of this type of requirement, and works diligently to help customer meet their obligations (see the Shared responsibilities section of this paper for more details).

New Zealand Information Security Manual (NZISM)

Published by the Government Communications Security Bureau (GCSB). The GCSB states that "The New Zealand Information Security Manual (NZISM) is the New Zealand Government's manual on information assurance and information systems security." and also that "It [the NZISM] is consistent with a wide variety of risk management, governance, assurance and technical standards, including the ISO/IEC 2700x series, as well as IETF, OASIS, NIST and other recognised standards bodies."[5]

Microsoft has successfully met a wide range of standard including ISO 27001, 27017, 27018 certifications. Evidence of these attestations can be found at the Microsoft Trust center.

NZ Cloud Computing Risk and Assurance Framework (NZ CC)

In October 2013, Cabinet "agreed to a Cloud Computing Risk and Assurance Framework [CAB Min (13) 37/6B refers]"[6]. As part of this framework, in April 2014, the Government CIO published the

[2] See recommendations 8 and 10 of the Cabinet paper.

[3] https://protectivesecurity.govt.nz/home/what-you-need-to-know/

[4] https://protectivesecurity.govt.nz/home/what-you-need-to-do/strategic-security-objectives-core-policies-and-the-mandatory-requirements-for-agencies/

[5] http://www.gcsb.govt.nz/publications/the-nz-information-security-manual

[6] https://www.ict.govt.nz/assets/Cabinet-Papers/Cab-Minute-Cloud-Computing-Risk-and-Assurance-

"Cloud Computing Information Security and Privacy Considerations" (CCISPC)[7] – commonly referred to as the "GCIO 105 questions". To address the needs of customers, Microsoft has published a response document showing how Azure addresses the 105 questions set out in the CCISPC.

Privacy Act 1993

The Privacy Act 1993 governs how personal information is used and protected in New Zealand. The New Zealand Privacy Commissioner website defines personal information as "*any piece of information that relates to an identifiable human being, such as names, contact details, financial health, and purchase records.*"[8] It goes on to say that "*Your cloud provider might have some responsibility for handling the information safely - check the contract. But if you're putting client information in the cloud, you're still responsible for it. The buck stops with you. Period.*"[9]

Microsoft Azure compliance

The primary responsibility for compliance with the Privacy Act lies with the customer. For areas that the cloud provider is responsible for, Azure complies with many international security and privacy certifications. Microsoft Azure adher to ISO/IEC 27018 code of practice, which covers privacy protections for the processing of personal information by cloud service providers.

2. Key security principles

This section provides technical information on how Azure addresses key aspects of New Zealand's security and privacy requirements, 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

Framework-Oct-2013.pdf

[7] https://www.ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf

[8] NZ Privacy Commissioner website, What is Personal Information.

[9] NZ Privacy Commissioner website, Cloud Computing checklist for small businesses.

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 targeting a region. The Microsoft Security Intelligence Report provides intelligence for 106 regions including New Zealand 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 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.

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. By constantly challenging the security capabilities of the service, Microsoft can stay ahead of emerging threats.

3. Key privacy principles

This section provides technical information on how Azure addresses key privacy principles for customers located in New Zealand, 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 27018, for which Microsoft was the first major cloud service provider to incorporate the ISO 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 on tenant isolation is available in the "Azure Active Directory Multi-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 27001, ISO 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 26 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.

In addition, Microsoft has announced another 8 Azure regions, specifically:

➢ US Department of Defense (two sites – to be announced), Germany (Frankfurt, Magdeburg), United Kingdom (two sites – to be announced), South Korea (Seoul, another to be announced).

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 NZ legislation, including the Protective Security Requirements, the Cloud Computing Risk & Assurance Framework, and the Privacy Act. This compliance means both government and commercial customers can have confidence knowing they comply with New Zealand 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.