



# Government Chief Digital Office

## Microsoft Azure and Azure Active Directory Security Risk Assessment Report

*Issued by*

*All of Government Service Delivery  
Digital Public Service Branch*



**Te Tari Taiwhenua**  
Internal Affairs

**Te Kāwanatanga o Aotearoa**  
New Zealand Government

Released under the Official Information Act 1982

## Document Control

### Document Information

<b>Project ID/Name</b>	Microsoft Azure and Azure Active Directory
<b>Author</b>	9(2)(a) – Quantum Security Services Ltd.
<b>Title</b>	GCDO – Microsoft Azure and Azure Active Directory Security Risk Assessment Report
<b>Version</b>	v1.1 dated 30 August 2022
<b>Document Number</b>	Cloud.Microsoft.SRA.2022_097

### Revision History

Version	Date	Author	Description of changes
0.1	28/03/2022	9(2)(a)	Initial Draft
0.2	28/03/2022	9(2)(a)	Peer Review
0.3	29/03/2022	9(2)(a)	Quality Assurance
0.4	31/03/2022	9(2)(a)	Draft Release
0.5	26/04/2022	9(2)(a)	Updates based on Lead Agency and Consuming Agency feedback
0.6	12/05/2022	9(2)(a)	Prepared for Approval
1.0	13/05/2022	Mae Koh	Prepared for Approval
1.1	30/08/2022	9(2)(a)	Adjustments to risk ratings and controls mapping from SSC QA

## Document Approval

I approve this Risk Assessment report; it presents the Information Security risks introduced to Consuming Agencies through the use of Microsoft Azure Services.

I acknowledge that I have been advised of the risks identified in this report. However, it is not a commitment to manage the risks that have been identified.

Acknowledged by	Signature	Date
<b>Jane Kennedy</b> General Manager AoG Service Delivery, Digital Public Service Branch Department of Internal Affairs Te Tari Taiwhenua	pp Richard Ashworth Original Signed	7 September 2022

I acknowledge that this Risk Assessment has been completed in accordance with the Government Chief Digital Officer's Information Security Risk Assessment process.

Acknowledged by	Signature	Date
<b>Katrina Banks</b> Manager Security AoG Service Delivery, Digital Public Service Branch Department of Internal Affairs Te Tari Taiwhenua	Original Signed	30 August 2022

## Glossary of Terms

<b>Availability</b>	Ensuring that authorised users have timely and reliable access to information.
<b>API</b>	A set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service.
<b>B2B</b>	Business-to-business (B2B), also called B-to-B, is a form of transaction between businesses.
<b>Confidentiality</b>	Ensuring that only authorised users can access information.
<b>Consequence</b>	The outcome of an event. The outcome can be positive or negative. However, in the context of Information Security it is usually negative.
<b>Control</b>	A risk treatment implemented to reduce the likelihood and/or impact of a risk.
<b>Gross Risk</b>	The risk without any risk treatment applied.
<b>Impact</b>	See Consequence.
<b>Information Security</b>	Ensures that information is protected against unauthorised access or disclosure users (confidentiality), unauthorised or improper modification (integrity) and can be accessed when required (availability).
<b>Integrity</b>	Ensuring the accuracy and completeness of information and information processing methods.
<b>Likelihood</b>	See Probability.
<b>Probability</b>	The chance of an event occurring.
<b>Recovery Point Objective (RPO)</b>	The earliest point time that is acceptable to recover data from. The RPO effectively specifies the amount of data loss that is acceptable to the business.
<b>Recovery Time Objective (RTO)</b>	The amount of time allowed for the recovery of an information system or service after a disaster event has occurred. The RTO effectively specifies the amount of time that is acceptable to the business to be without the system.
<b>Residual Risk</b>	The risk remaining after the risk treatment has been applied.
<b>Risk</b>	The effect of uncertainty on the business objectives. The effect can be positive or negative. However, in the context of Information Security it is usually negative.
<b>Risk Appetite</b>	The amount of risk that the organisation is willing to accept in pursuit of its objectives.
<b>Stakeholder</b>	A person or organisation that can affect, be affected by, or perceive themselves to be affected by a risk eventuating.
<b>Threat</b>	A potential cause of a risk.
<b>Vulnerability</b>	A weakness in an information system or service that can be exploited by a threat.

## Contents

<b>Document Control</b>	<b>2</b>
Document Information	2
Revision History	2
<b>Document Approval</b>	<b>3</b>
<b>Glossary of Terms</b>	<b>4</b>
<b>Executive Summary</b>	<b>6</b>
Introduction	6
Key Azure Cloud Risks	6
Summary of Cloud Service Risks	7
Gross Risk Position	8
Consuming Agency Key Recommendations	9
Service Provider Key Recommendations	11
Residual Risks	12
<b>Business Context</b>	<b>13</b>
Certification Approach	13
Connectivity and Service Provisioning Scenarios	13
Shared Responsibility Model for Security in the Azure Cloud	14
Stakeholders	14
Information Classification	14
Business Processes Supported	14
Business Impact	15
Security Requirements	15
Users	16
Legislation, Policy and Guidelines	16
Information Protection Priorities	17
Technical Context and Scope	18
Threat Actors	19
<b>Detailed Risks</b>	<b>21</b>
Generic Cloud Service Risks	33
<b>Threat Assessment</b>	<b>50</b>
<b>Controls Catalogue</b>	<b>52</b>
<b>Appendix A – Consulted Stakeholders</b>	<b>64</b>
<b>Appendix B – Project Overview</b>	<b>65</b>
<b>Appendix C – Risk Assessment Guidelines</b>	<b>66</b>
Rating Risk	66
Likelihood (Probability) Assessment	66
Impact (Consequences) Assessment	66

## Executive Summary


### Introduction

This report presents the findings of an Information Security Risk Assessment of Microsoft Azure Cloud that may be utilised by consuming agencies. The Risk Assessment followed the Government Chief Digital Officer's (GCDO) Risk Assessment process, which is based on the AS/NZS ISO 31000:2009 and ISO/IEC 27005:2011 risk management standards.

As this is a generic Risk Assessment report, the risks identified, and ratings assessed may be different and unique in the context of consuming agencies and the Microsoft Azure Cloud services being consumed. Therefore, agencies reading this report should review the risks using their own risk management framework. This ensures that the risks identified are specific to the agency's adoption of Microsoft Azure Cloud are within their business context, and risk appetite.

The details of the Risk Assessment scope can be found in [Appendix B](#). Where **Consuming Agency** and **Azure Cloud Service Provider** are used in this report, they refer to **Consuming Agency (CA)** and Microsoft Azure Cloud **Service Provider (SP)** respectively.

9(2)(b)(ii), 9(2)(k)



9(2)(b)(ii), 9(2)(k)



Released under the Official Information Act 1982

9(2)(b)(ii), 9(2)(k)

### Gross Risk Position

Table 1 – Gross Risk Ratings illustrates the rating of each risk without any controls in place. The table below includes the gross risk positions of both Azure specific and generic cloud risks.

#### Table 1 – Gross Risk Ratings

9(2)(b)(ii), 9(2)(k)

Released under the Official Information Act 1982



## Consuming Agency Key Recommendations

The Risk Assessment determined that the following key controls, if implemented, will help to address the identified risks. A controls catalogue was also developed to specify the recommended controls outlined in the Risk Assessment and is detailed in the Controls Catalogue section.

To mitigate and manage the identified gross risks rated as 9(2)(b)(ii), 9(2)(k)

the following key recommendations should be undertaken:

### 1. Vulnerability and Configuration Management

A robust vulnerability management process to ensure the security of the Microsoft Azure Portal should be developed and followed. This may include regular vulnerability assessments and reviews of the management console.

Change and configuration management procedures should be defined and followed to ensure that risks associated with misconfigurations are addressed and mitigated. This should also include the ongoing upskill or training of CA administrators to manage resources on the Azure Cloud.

### 2. Risk Management and Due Diligence

Before the consumption of the Azure Cloud services, agencies should be informed and aware of the implicating risks associated with using the service. This can be done by performing a comprehensive Risk Assessment to identify the risks and controls associated with the service.

Agencies must be aware of their responsibilities for security when consuming Azure Cloud services. This enables them to meet their obligations to protect the confidentiality, integrity, availability, and privacy of official information.

### 3. Access Management

CA users that require access to the Microsoft Azure Portal should only be provided with the minimum permissions required to perform their duties. A robust process that defines user access management can ensure that permissions are appropriately and timely updated. This prevents the risk of unauthorised access to the management console. The use of multifactor authentication also reduces the likelihood of unauthorised access to the management console.

CA users should be made aware of their responsibilities towards protecting the confidentiality of their credentials to access the Microsoft Azure Portal, including those of programmatic API keys. Regular user awareness and training programmes should be developed and made available to users. Topics include responsibilities and good practices on how to securely keep user credentials.

This is crucial as unauthorised access may allow individuals to access the personal information of other users of Azure services, as well as personal information contained in cloud services.

### 4. Strong Encryption and Secure Key Management

The use of strong encryption to protect data at rest and in transit is a key control to address confidentiality and integrity risks within the cloud.

Agencies should ensure that all requirements for protecting data at rest and in transit are well defined, configured and implemented. This includes the secure management of cryptographic keys used to encrypt agency data.

### 5. Logging and Auditing

## IN-CONFIDENCE

The presence of adequate logging and regular monitoring of the Azure services across tenancies can enable the CA to detect or investigate security incidents associated with the portal, should they occur. This includes ensuring sufficient logging and monitoring on the management console.

### 6. Security Blueprints, White Papers and Technical Training

In order to maintain secure infrastructure and services for their agencies, CA administrators should utilise security blueprints, white papers and technical training from Azure to advance their capability.

Azure offers a security blueprint referred to as the "[NZISM Restricted Blueprint](#)". This provides governance [guardrails](#) using [Azure Policy](#) that help agencies assess specific [New Zealand Information Security Manual](#) (NZISM) controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement controls for New Zealand ISM Restricted.

In addition to the above, the [Azure Policy control mapping](#) provides details on policy definitions included within this blueprint and how these policy definitions map to the controls in the New Zealand Information Security Manual. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions.

Utilising these tools is overall beneficial to improving an agency's security posture when consuming Azure Cloud services

Released under the Official Information Act 1982

## Service Provider Key Recommendations

To mitigate and manage the identified gross risks rated 9(2)(b)(ii), 9(2)(k) the following key recommendations should be undertaken. The following key recommendations can be undertaken by SPs.

### 1. Physical Security Controls

SPs must ensure that appropriate physical security controls are applied to their environment to ensure resources are well protected, and CA data is kept secure. Conducting physical security reviews on datacentres will assist in ensuring that they are protected from accidents, natural disasters, attacks and unauthorised physical access. They will also ensure that there are appropriate protections in place such as fire suppression if an issue were to occur.

### 2. Supply Chain Management

SPs should ensure robust supply chain management processes are in place to reduce the likelihood and impact of an issue with one of their providers. Robust supply chain monitoring may include conducting Risk Assessments on providers, conducting audits, ensuring robust due diligence and change management is in place for introducing new vendors and technologies, and monitoring the cyber threat landscape.

### 3. Access Controls

Robust access controls within an SP environment are needed to ensure that only those who require access can access resources. SPs must ensure that the principle of least privilege is used within their environment, as well as regular access reviews and robust logging of administrator actions. Ensuring strong password policies are enforced along with Multi-Factor Authentication (MFA) for all actions reduces the likelihood for compromise.

### 4. System Hardening

SPs must ensure that appropriate hardening has occurred to hypervisors and supporting infrastructure to reduce the likelihood of compromise of cloud resources. Ensuring services are hardened to industry best practice, as well as conducting design and architecture reviews on implementations, reduces the likelihood of misconfiguration and vulnerabilities being introduced. Ensuring systems undergo regular patching and maintenance is important in ensuring the ongoing security posture of the SP.


### 5. Encryption of Data at Rest and in Transit

SPs must ensure all data in transit or stored in the cloud is encrypted using approved encryption algorithms to ensure private, or otherwise classified information stored is protected against unauthorised disclosure. Encryption must also be applied to any data in transit to prevent the capturing and disclosure of data moving across networks.

## Residual Risks

The tables below illustrate the expected residual rating of each of the risks if all the recommended controls are implemented and appropriately configured and managed.

9(2)(b)(ii), 9(2)(k)



## Business Context

This section provides an overview of the business context for the Microsoft Azure Cloud services that are in scope of this Information Security Risk Assessment.

## Certification Approach

The following business context considerations have been made for the Risk Assessment, with input from a sample of agencies:

- Share security responsibility model when consuming the Azure service;
- Key stakeholders involved when consuming the Azure service;
- Classification of the information stored, processed and transmitted by the Azure service;
- Different types of users with access to the Azure service;
- Information Security requirements for the Azure service in terms of confidentiality, integrity, availability, privacy and any other relevant legislation; and
- Information protection priorities when consuming the Azure service.

Consuming agencies consuming the Risk Assessment must ensure that they:

- Review the business context assumptions made during the Risk Assessment and ensure that they accurately reflect the agency's own context;
- Define the business process that will be supported by the Azure service;
- Identify and document the business impact should an Information Security or privacy incident occur; and
- Consider the agency's use context and risk appetite and evaluate assigned risk ratings.

## Connectivity and Service Provisioning Scenarios

We identified three provisioning scenarios that CAs can use to subscribe to Azure and manage their assets in Azure's cloud:

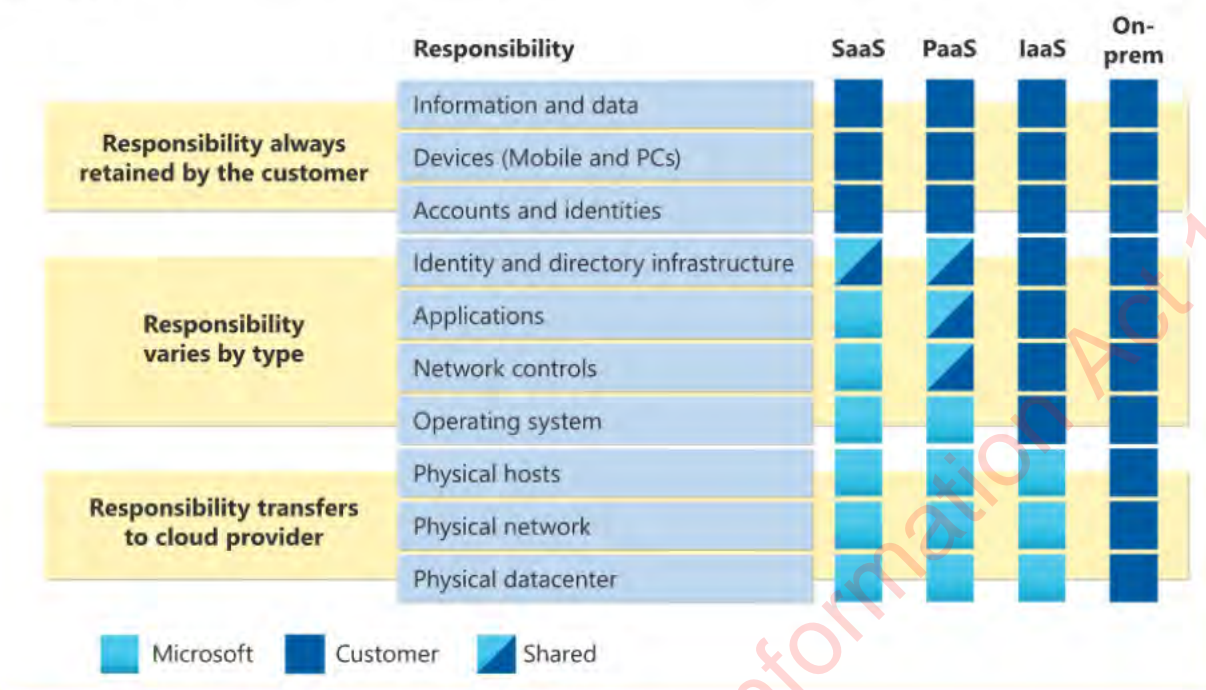
- Having direct contractual relationships with Microsoft Azure and directly managing their assets using their own set of credentials;
- Having contractual relationships with a New Zealand reseller and directly managing their assets using their own set of credentials; and
- Having contractual relationships with a New Zealand reseller and partly or fully delegating their assets' management to this reseller.

Similarly, we identified four connection scenarios that CA can use to interconnect their networks to Microsoft Azure:

- Direct connection to the public IP addresses of the Virtual Machines over the public internet;
- VPN connection to a Virtual Network Gateway in Azure configured with private IP addresses over the public internet;
- Dedicated connection to a VNet (virtual network) in Azure configured with public IP addresses over a dedicated link to a third-party provider using ExpressRoute; and
- Dedicated connection to a VNet (virtual network) in Azure configured with private IP addresses over a dedicated link to a third-party provider using ExpressRoute.

## Shared Responsibility Model for Security in the Azure Cloud

The following diagram<sup>1</sup> and table summarises the responsibility boundary for each of the cloud service models:



### Stakeholders

The key stakeholders for a generic Cloud Service are:

- Department of Internal Affairs;
- Consuming Agency;
- Microsoft Azure, Microsoft Cloud Infrastructure and Operations (MCI), their subcontractors and third-parties hosting Azure’s Datacentre in Australia; and
- The Service Provider through whom the said Microsoft Azure Cloud services might have been contracted.

### Information Classification

Based on the New Zealand Government Security Classification System<sup>2</sup>, the information that will be stored, processed, or transmitted by the Azure service has been classified for RESTRICTED and below.

The compromise of information classified as RESTRICTED and below can:

- Adversely affect diplomatic relations;
- Hinder the operational effectiveness or security of New Zealand or friendly forces; and
- Adversely affect the internal stability or economic wellbeing of New Zealand or friendly countries.

### Business Processes Supported

Each CA will be using the Azure service to support different types of business processes. Therefore, it is important for each agency to understand what business processes will be supported and define the

<sup>1</sup> Microsoft Shared Responsibilities for Cloud Computing dated January 2022

<sup>2</sup> <https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/classification-system/national-security-information/>

security requirements for the service. This will ensure that agencies understand the security requirements that the service needs to meet.

## Business Impact

Each CA will be using the Azure service to transmit, store or process different types of information, in addition to providing access to different information systems and services. Therefore, it is important for each agency to identify and document the types of information that will be transmitted, stored, or processed in the cloud environment. This will ensure that agencies understand the business impact if the confidentiality, integrity and availability of the information was compromised.

## Security Requirements

The Confidentiality, Integrity and Availability requirements for the consumption of the Azure service have been defined as follows:

### Confidentiality

The confidentiality of the information transmitted, stored, or processed by the Azure service is considered as **5 – Critical**. This is largely driven by the **RESTRICTED** classification of information that will be transmitted, stored, or processed by Azure.

If the confidentiality of information stored or processed by Azure was compromised, the following consequences are expected:

- Disclosure of sensitive information to unauthorised personnel;
- Loss of key stakeholder confidence in the Azure service;
- Reputation damage for the affected CA; and
- Further investigation where required by law.

### Integrity

The integrity of the information transmitted, stored or processed by the Azure service is considered as **5 – Critical** for consuming agencies. It is assumed that consuming agencies will be using the cloud service to store and process information that business processes rely on for decision-making. Inaccurate or corrupted information can cause consuming agencies to lose their data source of truth and affect business outcomes.

If the integrity of information stored or processed by Azure were to be compromised, the following consequences are expected:

- Modification of agency information by unauthorised personnel leading to inaccurate or corrupted data;
- Incorrect business decision making or actions taken by the CA;
- Loss of key stakeholder confidence in the Azure service;
- Reputation damage for the affected CA; and
- Further investigation where required by law.

### Availability

The availability of the information transmitted, stored, or processed by Azure service is considered as **5 – Critical**. It is assumed that consuming agencies will be using the service to store and process information that business processes rely on. Prolonged service outages can have an adverse impact on business processes reliant on the service, affecting business outcomes.

If the availability of information stored or processed by Azure was compromised, the following consequences are expected:

- Loss of productivity at CA;
- Failure to deliver key services;
- Loss of key stakeholder confidence in the Azure service;
- Reputation damage for the affected CA; and
- Further investigation where required by law.

## Privacy

Personal information may be transmitted, stored, or processed by Azure. Therefore, the Privacy of the information transmitted, stored, or processed by Azure service is considered as 5 – Critical.

If personal information will be transmitted, stored, or processed by Azure, consuming agencies must ensure that the privacy of the information is adequately protected from unauthorised access, disclosure or modification during storage and in transit. Consuming agencies should also ensure that the service is configured and operating to help agencies meet the requirements from the Privacy Act 2020.

## Users

The users and security roles for cloud services have been defined as following:

**Table 4 – User Groups & Descriptions**

User Group	Description
CA Administrators	Agency staff with privileged access to the cloud service. Responsible for managing and configuring the agency's cloud resources, user accounts, groups and permissions.
CA Users	Agency users with role-based access to the cloud service. Responsible for using the service to deliver and meet its associated agency business outcomes.
CA Third-Party Providers Administrators	Third-Party Provider staff with access to the part of the cloud service. Contracted by the CA in Azure services or ExpressRoute connectivity provisioning.
Azure Administrators	Microsoft Azure Service Organization (Azure) and Microsoft Cloud Infrastructure and Operations (MCIO) staff with access to the information systems supporting the cloud service.
External Users	Members of the public using public facing applications hosted on Microsoft Azure Cloud.

## Legislation, Policy and Guidelines

Government agencies must ensure that they can demonstrate compliance with applicable legislation, policies, guidelines and any other external requirements when using a cloud service.

For purposes of completing this Risk Assessment, the following legislation, policy and guidelines were identified to be applicable to the generic context:

- Official Information Act 1982;
- Privacy Act 2020;
- Public Records Act 2005;
- Protective Security Requirements (PSR); and
- New Zealand Information Security Manual (NZISM v 3.5).



### Information Protection Priorities

For purposes of completing this Risk Assessment, the following represents the information protection priorities for a cloud service:

**Table 5 – Information Protection Priorities**

Attribute	Priority Rating
Confidentiality	5
Integrity	5
Availability	5
Privacy	5

Table 9 represents the scale used to define the information protection priorities shown in Table 58.

**Table 6 – Information Protection Priority Scale**

Priority Rating	Scoring
Critical	5
Highly Important	4
Important	3
Some Importance	2
Unimportant	1
Not Applicable	0

Released under the Official Information Act 1982

9(2)(b)(ii), 9(2)(k)

Released under the Official Information Act 1982

## Threat Actors

The following threat actors were identified when performing a high-level threat assessment relating to Public Cloud Services from the Cloud Services Providers. The threat actors relate to threat sources within the detailed Risk Assessment in Table 9 and Table 10, with further analysis and scenarios in the Threat Assessment in Table 11.

**Table 8 – Threat Descriptions**

Role	Description
Determined Thief or Vandal	An individual or group that has formulated a plan to breach the logical perimeter(s) of the cloud service provider and gain or elevate privileged access to information resources.
Escorted Party	A party that is being escorted through the cloud service provider datacentre, either under Change Control or part of a tour. Such parties may take malicious or accidental actions, the latter being more likely. These parties have been granted access and have been through many security controls.
Hostile Intelligence Agencies	Hostile foreign intelligence agencies may target cloud service providers to gain access to government information. A likely avenue of attack is network (internet) based, particularly for RESTRICTED classified information and below. Such parties may conduct technical attacks from outside the cloud service provider perimeter(s), which will be more challenging to detect if using passive techniques. Hostile intelligence agencies may seek to subvert other authorised parties within the cloud service provider with a view to conducting an insider attack i.e., a threat within a threat.
Interested or Informed Outsiders	An individual or group outside the cloud service provider that attempts to gain unauthorised access to user accounts and/or infrastructure to retrieve sensitive information. Motivation for this may be the type of data the cloud service provider stores on behalf of a government agency or information learned from a member of staff within, or service provider to, the cloud service provider.
Internal Threat	<ol style="list-style-type: none"> <li>1. A party that has authorised access within the cloud service provider and abuses this privilege to steal information and/or media and/or disrupt services for personal gain.</li> <li>2. A party that has authorised access within the cloud service provider and unintentionally performs actions that result in unauthorised access to cloud service provider resources and/or disrupts services.</li> <li>3. An internal threat actor party within the cloud service provider with anti-government or anti-establishment political or personal views, and who manipulates their role within the cloud service provider.</li> </ol>
Issue Motivated Group	A party that has a grievance or issue with the cloud service provider or one of their customers (which may be government) and seeks to disrupt operations of the cloud service provider to draw attention to their cause. This may be directly or indirectly affecting government agencies.
Natural Disaster or Person-Made Hazard	A natural disaster or person-made hazard impacts the infrastructure behind the cloud service provider, such as a datacentre, or the people working remotely for the cloud service provider, resulting in loss of data and/or disruption to service and/or Business as Usual (BAU) processes.
Opportunistic Thief or Vandal	An individual or group that causes harm but not in a pre-meditated manner. These parties are most likely to only damage physical security e.g., plant and/or telecommunications equipment at a cloud service provider physical location.
Organised Crime	These groups may target the cloud service provider if they consider they can gain something of value from doing so.

IN-CONFIDENCE

Role	Description
Unescorted Party	A party that has gained authorisation to enter the cloud service provider datacentre without escort and is trusted to some degree. Such parties may take malicious or accidental actions, the latter being more likely.

Released under the Official Information Act 1982

## Detailed Risks

Table 9 presents the risks associated with use of Azure Cloud and Azure AD services.

9(2)(b)(ii), 9(2)(k)

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982



Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982



### Generic Cloud Service Risks

Table 10 presents the risks associated with use of a Generic Cloud Service that may be applicable when consuming the Azure Cloud Service.

Table 10 – Generic Cloud Services Risk Assessment

Risk ID	Risk Description	9(2)(k)
GC-R01	Information Disclosure, Modification or Loss due to Poorly Defined Service Agreements 9(2)(k)	9(2)(k)
GC-R02	Information Disclosure or Loss due to Legal Jurisdictional Rules 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description
	9(2)(k)
GC-R03	<b>Māori Data is Relocated Outside of New Zealand</b> 9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
GC-R04	<p>Information Disclosure, Modification or Loss due to Data Distribution</p> <p>9(2)(k)</p>	<p>9(2)(k)</p>
GC-R05	<p>Information Disclosure, Modification or Loss due to Data Lock In</p> <p>9(2)(k)</p>	

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
GC-R06	<p><b>Information Disclosure, Modification or Loss due to Insider Threats</b></p> <p>9(2)(k)</p>	9(2)(k)
GC-R07	<p><b>Information Disclosure, Modification or Loss due to Ineffective Security Incident Response and Management</b></p> <p>9(2)(k)</p>	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description
	9(2)(k)
GC-R08	<b>Information Disclosure, Modification or Loss due to Inappropriate Use of Cloud Service</b> 9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description
GC-R09	<b>Information Disclosure, Modification or Loss due to Incomplete Segregation of SP Tenant Data</b> 9(2)(k)



Released under the Official Information Act 1982

Risk ID	Risk Description
GC-R10	Information Disclosure, Modification or Loss due to Virtualisation Technology Vulnerabilities 9(2)(k)

9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
GC-R11	<b>Information Disclosure, Modification or Loss due to Insecure Facilities</b> 9(2)(k)	9(2)(k)
GC-R12	<b>Information Disclosure due to Incomplete Data Deletion</b> 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982



Risk ID	Risk Description
	9(2)(k)
GC-R13	<b>Information Disclosure, Modification or Loss due to Malware</b> 9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
GC-R14	<p>Cloud Services Outages due to Inadequate Service Backup and Recovery Procedures</p> <p>9(2)(k)</p>	9(2)(k)
GC-R15	<p>Cloud Service Degradation or Outage due to Inadequate Network and Server Capacity Management</p> <p>9(2)(k)</p>	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
9(2)(k)	9(2)(k)	9(2)(k)
GC-R16	Information Disclosure, Modification or Loss due to Social Engineering Attacks 9(2)(k)	

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
GC-R17	<p data-bbox="278 338 759 401">Information Disclosure due to Incomplete Segregation of SP Management Networks</p> <p data-bbox="278 401 759 1010">9(2)(k)</p>	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description
GC-R18	Information Disclosure, Modification or Loss due to Inappropriate SP User Access Management 9(2)(k)



Released under the Official Information Act 1982

Risk ID	Risk Description
GC-R19	Information Disclosure, Modification or Loss due to Compromised SP User Credentials

9(2)(k)

9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
GC-R20	<b>Information Disclosure, Modification or Loss due to SP System Misconfiguration</b> 9(2)(k)	9(2)(k)
GC-R21	<b>Ineffective Security Incident Management due to Inadequate Logging and Monitoring</b> 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description
GC-R22	<p>Information Disclosure, Modification or Loss due to Poorly Defined Roles and Responsibilities</p> <p>9(2)(k)</p>
GC-R23	<p>Information Disclosure, Modification or Loss due to Insecure Data Migration</p> <p>9(2)(k)</p>

Released under the Official Information Act 1982



Risk ID	Risk Description
9(2)(k)	9(2)(k)
GC-R24	<p>New Services are not Implemented Securely by the CA</p> <p>9(2)(k)</p>

Released under the Official Information Act 1982

### Threat Assessment

This section provides details of the threats identified during the high-level threat assessment. The threat assessment has been performed to assist the DIA in understanding key threats relating to the Public Cloud Services from the Cloud Services Providers. The STRIDE framework has been used to determine threats relating to key area: Spoofing, Tampering, Information Disclosure, Denial of Service and Elevation of Privilege.

**Table 11 – Detailed Threat Scenarios**

Threat Actor		STRIDE Category
Determined Thief or Vandal		Information Disclosure
Escorted Party		Denial of Service Information Disclosure Elevation of Privilege
Hostile Intelligence Agency		Denial of Service Information Disclosure Elevation of Privilege
Interested or Informed Outsiders		Denial of Service Information Disclosure Elevation of Privilege
		Denial of Service Information Disclosure
		Denial of Service Information Disclosure
		Denial of Service Information Disclosure Elevation of Privilege

Released under the Official Information Act 1982

Threat Actor	STRIDE Category
	spoofing Information Disclosure
Internal Threat	Impersonation Elevation of Privilege
Issue Motivated Group	Repudiation
Natural Disaster or Person-Made Hazard	Impersonation Information Disclosure Denial of Service
Opportunistic Thief or Vandal	Impersonation Denial of Service
Organised Crime	Denial of Service
Unescorted Party	Denial of Service
	Information Disclosure
	Information Disclosure Denial of Service
	Repudiation Information Disclosure Denial of Service

Released under the Official Information Act 1982

## Controls Catalogue

Table 12 presents the recommended controls to effectively manage the risks recorded in Table 9:

Table 12 – Recommended Controls

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C01	Contracts and SLAs	<p>Ensure that contracts and associated Service Level Agreements (SLAs):</p> <ul style="list-style-type: none"> <li>Clearly define the legal jurisdiction for contractual disputes relating to the use and function of the service;</li> <li>Clearly define the ownership of the data stored, processed and/or transmitted by the service;</li> <li>Define in which jurisdiction official information can and will be stored, processed and/or transmitted by the service;</li> <li>Ensure that official and/or private information is appropriately protected to accepted Information Security standards in SP's environment, including backups and other environmental copies;</li> <li>Ensure that the time to return to full service after a failure or outage, including data restoration, meets the organisation's business continuity requirements;</li> <li>Require that all access to the organisation's information and systems be monitored;</li> <li>Require and specify means to notify to the organisation of any actual or possible unauthorised access;</li> <li>Require engagement with the organisation in resolution of any information access incidents or issues;</li> <li>Require regular reports be delivered from SP on their performance against the SLA's;</li> <li>Require the organisation to be allowed to carry out regular audits to ensure compliance with its requirements or provide a full copy of all relevant independent third-party audit reports;</li> <li>Require sufficient resiliency from SP in its own and its network provider's infrastructures to minimise the impact of infrastructure failures, denial of service and other internet based attacks; and</li> <li>Ensure the contract with SP outlines clearly the services in scope and that the organisation is alerted when requiring services that are not within the scope.</li> </ul>	Likelihood	2.2.5.C.01 2.3.20.C.01 2.3.23 3.2.9 3.2.11 3.3.7 3.3.11 4.4.8 6.4 22.1 22.1.18
C02	Due Diligence	<p>Ensure that adequate due diligence is undertaken across the service, specifically:</p> <ul style="list-style-type: none"> <li>Defining the Information Security requirements of the service;</li> <li>Assessing whether the defined Information Security requirements are met by the service;</li> <li>Identifying and assessing any third-party dependencies that the service provider may have; and</li> <li>Ensuring third parties can meet New Zealand security requirements as contractor.</li> </ul> <p>For higher handling requirements agencies must ensure that assurance checks are conducted on cloud providers.</p>	Likelihood	2.2.4 4.4.8 12.7
C03	Non-Disclosure and Confidentiality Agreements	<p>Identifying, articulating and regularly reviewing the organisation's requirements for confidentiality or non-disclosure agreements reflects the organisation's needs for the protection of its information. Ensuring contracts with SPs, Vendors and authorised third parties incorporate appropriate non-disclosure and confidentiality agreement provides the organisation with the assurance that its information will be safe from disclosure.</p>	Likelihood	4.4.8.C.02 4.4.8.C.03
C04	Risk Management	<p>Ensure that system undertakes risk identification and assessment, selection and implementation of baseline and other appropriate controls and the recognition and acceptance of residual risks relating to the operation of the system. Systems should be accredited before they are used operationally.</p> <p>Ensure that a Security Risk Management Plan (SRMPs) is developed to identify associated security risks for the system and address appropriate treatment measures including physical environments.</p>	Likelihood, Impact	2.3.20.C.02 3.3 12.7.14 4.4 4.5 5.1.8 5.1.9 5.3 22.1.21 22.2.13
C05	Human Resources Security	<p>Ensure that all employees and contractors understand their responsibilities and are suitable for the roles, which they are employed, including</p> <ul style="list-style-type: none"> <li>Security vetting all new staff before beginning employment and on a regular basis thereafter;</li> <li>Undertaking an induction process that covers their responsibilities for Information Security;</li> <li>Acknowledging the Code of Conduct and Information Security policy;</li> <li>Acknowledging the employee's Terms and Conditions of Employment;</li> <li>Receiving regular security awareness training;</li> <li>Monitoring and management of changes in employee circumstances and behaviour; and</li> <li>Removing access rights when their employment or contract ceases.</li> </ul>	Likelihood	3.2 3.3 3.5 5.1.7 9.2 19.1.18 22.1.27

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C06	Security Vetting	Ensure that authorised users of a system or service are vetted by an approved vetting service such as that provided by the Ministry of Justice. Only appropriately, authorised, cleared and briefed personnel are allowed access to the systems.	Likelihood	3.5 9.2 9.4
C07	Security Awareness Training	Ensure that all employees and contractors are provided with ongoing awareness training. Topics such as Information Security responsibilities (e.g., email security and using the internet), legislation and regulation, consequences of non-compliance with Information Security policies and procedures and potential security risks and counter measures should be covered.	Likelihood	3.2 3.3 5.6.3.C.01 9.1 9.3 15.0 19.1.18 22.1.27
C08	User Training	Ensure that all users of an information system are well trained in the correct use of the system to reduce the likelihood of inappropriate use or mistakes.	Likelihood	3.2 9.1 22.1.27
C09	Access Control	Ensure that users are only provided with access to the service that have been specifically authorised to use, including: <ul style="list-style-type: none"> <li>• Documenting of an access control policy that defines business requirements for access, principles for access (e.g., need to know, role based) and access control rules that will ensure these requirements are met; and</li> <li>• Implementing specific policies for access control based on business functions, processes or user roles and responsibilities, such as administrator access, user access, system access, remote access, network access, and discretionary and mandatory access.</li> </ul>	Likelihood, Impact	5.5.5 9.2 11.7 16.1 16.2 16.3 16.4 16.5 22.1.24 22.2.16
C10	Separation of Duties	Ensure that all critical tasks that may be disrupted by human error or through malicious intent are designed in such a way that a single individual is unable to perform an action that results in such a disruption.	Likelihood, Impact	16.2.6
C11	Role Based Access Control	Ensure that access to the service is controlled based on the roles of the individuals requiring access. Role based access controls allows access to be quickly, easily and uniformly granted, changed or removed for groups of users, without having to update the privileges for each user.	Likelihood, Impact	9.2 9.4 11.7 16.2.6 16.3
C12	User Account Lifecycle Management	Ensure that user accounts are managed through their lifecycle process, including: <ul style="list-style-type: none"> <li>• Assigning access rights aligned with the defined access control policy;</li> <li>• Reviewing access rights on a regular basis;</li> <li>• Disable accounts when a user leaves an organisation;</li> <li>• Disable accounts when a user no longer requires access; and</li> <li>• Remove or update access rights (e.g., when a user changes roles within an organisation).</li> </ul>	Likelihood, Impact	5.5.5 9.2.7 16.1 16.3
C13	Least Privileges	Ensure that only the minimum required access rights are granted to a user or system when accessing a system, preventing the assignment of excessive user permissions. Privileged access rights are controlled through formal authorisation process and implemented in accordance with the defined access control policy.	Likelihood, Impact	16.3 16.4.31.C.01 22.1.24
C14	Password Policy	Ensure the use of a robust password policy including: <ul style="list-style-type: none"> <li>• Enforcing the use of individual user IDs and passwords to maintain accountability;</li> <li>• Allowing users to select and change their own passwords;</li> <li>• Enforcing a choice of quality passwords (what quality passwords are, should be explained in the password policy), including minimum password length and complexity requirements;</li> <li>• Forcing users to change their passwords at the first log-on or if reset; and</li> <li>• Enforcing regular password changes (at least every 90 days) and as needed.</li> </ul>	Likelihood	16.1.40 16.1.41

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C15	Secure Password Distribution	Ensure that user passwords should be protected against unauthorised access when distributed initially. Distribution methods may include: <ul style="list-style-type: none"> <li>• Encrypted email;</li> <li>• A secure password reset mechanism that positively authenticates the user (such as a challenge question or multifactor authentication);</li> <li>• A text message to a verified mobile number; and</li> <li>• A telephone call.</li> </ul>	Likelihood	16.1.40 16.1.41
C16	Identity Management and Authentication	Identify management and authentication is the identification and authentication processes that verify the identity of a user or device. Secure authentication controls are implemented as physical or logical controls, and reduce the likelihood of unauthorised access to information, services, or systems in accordance with an access control policy.	Likelihood	9.2.6 16.1 22.2.16
C17	Multi-Factor Authentication	Where strong authentication and identity verification is required (e.g., privileged users, administrators) additional forms of authentication can be used (e.g., tokens, digital certificates, biometrics). Multi-factor authentication provides the strongest level of authentication, as it requires a combination of at least two of the following forms of identification: <ul style="list-style-type: none"> <li>• Something you know (e.g., username and password (one-time password (OTP) or reusable), personal identification number (PIN));</li> <li>• Something you have (e.g., hardware or software token, digital certificate, smartcard); and</li> <li>• Something you are (e.g., biometric fingerprint).</li> </ul> For higher handling requirements agencies must ensure multifactor authentication is enabled.	Likelihood	16.1.13 16.1.14 16.1.16 16.1.17 16.4.10 16.5 16.7 19.1.20 21.4.11
C18	Secure Management	Ensure that servers and information systems are administered and managed securely from a suitably hardened and configured central point such as a jump server. Access to the central point should be restricted with access and activities logged. Administrators should be issued with unique accounts that are different to the account used for daily activities such as email or web browsing.  A dedicated management network isolated from production networks should also be deployed to reduce the likelihood of management data being intercepted and disclosed, and to reduce the attack surface area of information systems.	Likelihood	18.1.14
C19	Data Backup	Ensure that backups of business-critical information, configurations, logs etc. are recoverable to assist in meeting the defined Recovery Point Objective (RPO), Recovery Time Objective (RTO) and the Maximum Tolerable Downtime (MTD). The data backup process may include appropriate controls required to protect the highest classification of information included in the backup as well as regular restoration tests to confirm its effectiveness. An offline encrypted copy of all backup's may be required and maintained in a location that meets the physical and environmental security requirements for back-up media. Consideration should be given to ensuring a local copy of backup data is held to support business continuity in case of failure of the service.  Ensure a backup, recovery and archiving plan is developed, implemented, and incorporated into the Disaster Recovery and Business Continuity plans.	Impact	5.5.5 6.4 6.4.6 13.3.5 16.3.7 16.5 17.1.45 22.2.15.C.03 22.1.26

Released under the Official Information Act 1982

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C20	Logging and Auditing	<p>Ensure that information systems are configured with adequate logging, archived and retained for at least 18 months. Events to be logged includes:</p> <ul style="list-style-type: none"> <li>• User login;</li> <li>• All privileged operations;</li> <li>• Failed attempts to elevate privileges;</li> <li>• Security related system alerts and failures;</li> <li>• System user and group additions, deletions and modification to permissions;</li> <li>• Unauthorised or failed access attempts to systems and files identified as critical to the Agency;</li> <li>• Date and time of the event;</li> <li>• Relevant system user(s) or processes;</li> <li>• Event description;</li> <li>• Success or failure of the event;</li> <li>• Event source (e.g., application name); and</li> <li>• IT equipment location/identification.</li> </ul> <p>For higher handling requirements agencies must ensure that logging and appropriate supporting processes are implemented.</p>	Likelihood, Impact	3.3 3.4 4.2.10 4.4 7.1 7.3 12.4 13.3.9.C.01 14.1 14.2 14.3 15.2 16.1.46 16.5 16.6 19.1.13.C.01 19.2 19.2.20 20.1.10.C.02 20.1.11.C.01 22.2
C21	Security Incident and Event Management (SIEM)	<p>Ensure that security related event logs are analysed regularly using automated security information and event management (SIEM) tools or equivalent to help identify anomalies.</p>	Impact	7.1
C22	Information Security Incident Management	<p>Ensure that an Incident Response Plan is developed and defines what constitutes an incident, and to outline the systematic process that is to be followed should an incident occur. An Information Security Communication Plan should also be developed to provide guidance on how and when to share information relating to a security incident with outside parties such as customers, vendors and the media. The Incident Response and Management Plan should include:</p> <ul style="list-style-type: none"> <li>• Address clear definitions of the types of Information Security incidents are likely to be encountered and provide broad guidelines on what constitutes an Information Security incident;</li> <li>• Information Security incident response and management training for all system users and administrators;</li> <li>• Address authority responsible for initiating investigations of an Information Security incident;</li> <li>• Detecting security incidents to minimise impacts;</li> <li>• Reporting security incidents, assisting in documenting and understanding the risks and impacts; and</li> <li>• Managing security incidents by identifying and implementing processes for incident analysis and selection of appropriate remediation.</li> </ul>	Impact	3.2 3.3 5.1.11 5.1.12 5.6 7.0 22.1.25
C23	Cryptographic Policy and Key Management	<p>Ensure that cryptographic keys are managed according to defined standards and procedures and protected against unauthorised access or destruction during their lifecycle, including creation, storage and protection, distribution, use, renewal, recovery, revocation, destruction.</p> <p>Agencies must ensure they have complete visibility over all uses and access of their private keys when operating with cloud service providers (ie. assured key management practices).</p> <p>Agencies must be able to demonstrate that any Third-Party holding, using or managing agencies private keys in order to ensure functionality of a service is not compromised, or to provide a greater level of assurance over the management and security of keys than an Agency itself may be able to provide, demonstrate (evidence-based) equitable credentials to that required of Agency staff or other government outsourced service providers.</p> <p>Agencies must ensure that their cloud key management decisions do not compromise the security of other tenants, agencies or external parties. In all cases, agencies should ensure the use of a hardware security module (HSM) or equivalent to generate, manage, and store cryptographic keys.</p> <p>In cases where sole control of private keys (such as Hold Your Own Key [HYOK] approach) is impractical, agencies must carefully consider the nature of information that they are entrusting to a cloud service provider, and the different threats, adversary motivations and mitigations that are applicable, in order to reduce the risk and information exposure.</p> <p>For higher handling requirements agencies must ensure they have sole control over associated cryptographic keys.</p>	Likelihood	17
C24	Encryption of Data in Transit	<p>Ensuring business sensitive, private, or otherwise classified information that flows over the public or untrusted network such as the internet or internal networks is protected using approved cryptographic protocols, reduces the likelihood of information being disclosed to, or captured by, an unauthorised person.</p> <p>For higher handling requirements agencies must ensure that data is encrypted in transit.</p>	Likelihood, Impact	8.3.5 16.1.37 17.2 17.3 17.4 21.4.13.C.01 22.1.24.C.04

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C25	Encryption of Data at Rest	Ensuring business sensitive, private, or otherwise classified information stored on media is encrypted using approved encryption algorithms and protocols, reduces the likelihood of unauthorised disclosure. For higher handling requirements agencies must ensure that data is encrypted at rest.	Likelihood, Impact	17.1 17.2 17.3 22.1.24.C.04
C26	Physical Security	Ensuring that all critical facilities such as datacentres, communication rooms, security containers, servers, networks, telecommunication equipment and other important assets are physically protected against accident, natural disaster, attacks and unauthorised physical access. This also involves ensuring environmental controls such as Air Conditioning, Uninterrupted Power Supplies (UPS), and fire suppression are in place to protect the facility. For higher handling requirements agencies must ensure appropriate physical security controls are in place.	Likelihood	8.1 8.2 8.3 9.2 9.4 16.1.45.C.01 11.4.12 11.5.15 11.7.32
C27	Equipment Security	Ensure that equipment or assets supporting the service are protected against loss, damage, theft and unauthorised access. The considerations for equipment security includes: <ul style="list-style-type: none"> <li>• Ensuring IT equipment always reside in an appropriate class of secure room;</li> <li>• Storing IT equipment during non-operational hours in an appropriate class of security container or lockable commercial cabinet;</li> <li>• Using IT equipment with removable non-volatile media which is stored during non-operational hours in an appropriate class of security container or lockable commercial cabinet as well as securing its volatile media;</li> <li>• Using IT equipment without non-volatile media as well as securing its volatile media;</li> <li>• Using an encryption product to reduce the physical storage requirements of the non-volatile media as well as securing its volatile media; and</li> <li>• Configuring IT equipment to prevent the storage of classified information on the non-volatile media when in use and enforcing scrubbing of temporary data at logoff or shutdown as well as securing its volatile media.</li> </ul>	Likelihood, Impact	8.4 9.2 10
C28	Secure Decommissioning and Disposal	Ensure that IT systems are safely decommissioned and that software, system logic and data are properly transitioned into new systems or archived in accordance with the organisation, legal and statutory requirements. IT systems no longer required should be sanitised and disposed of in an approved manner that reduces the likelihood of data recovered by an unauthorised party. Ensure that a policy and procedures is developed and implemented for the decommissioning and disposal of IT equipment, media, and other important assets. For higher handling requirements agencies must ensure they have a decommissioning process defined.	Likelihood	11.7.35 12.6 13.1 13.4 13.5 13.6 22.1.26
C29	Media Handling	Ensure that media containing information are protected against unauthorised access, misuse or corruption. This includes classifying, labelling and registering the media and clearly indicate the required handling instructions and level of protection to be applied.	Likelihood	13.2 13.3
C30	Documentation	Ensure that Information Security documentation is produced for systems, to support and demonstrate good governance. The following documents should be documented: <ul style="list-style-type: none"> <li>• Information Security Policies (SecPol) – setting the strategic direction for Information Security;</li> <li>• Systems Architecture – illustrates the structural design of the system including any outsourced services;</li> <li>• Security Risk Management Plans (SRMPs) – identifying security risks and appropriate treatment measures for systems;</li> <li>• System Security Plans (SecPlan) – specifying the Information Security measures for systems;</li> <li>• Standard Operating Procedures (SOPs) – ensuring security procedures are followed in an appropriate and repeatable manner;</li> <li>• Incident Response Plans (IRPs) – outlining actions to take in response to an Information Security incident;</li> <li>• Emergency Procedures – ensuring classified information and systems are secured before personnel evacuate a facility in the event of an emergency; and</li> <li>• Independent Assurance Reports – provides assurance to System Owners, Certifiers, Practitioners and Accreditors and to assist system designers, enterprise and security architects where assurance reviews cannot be directly undertaken on service providers.</li> </ul>	Likelihood, Impact	3.2 3.3 4.3.18 5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8 9.2.5
C31	Change Management	Ensure that Information Security is an integral part of the change management process and incorporated into the organisation's IT governance and management activities. All changes to the configuration of a system should be documented and approved through a formal change control process. All changes should be reviewed whether successful or not. Examples of a system change includes: <ul style="list-style-type: none"> <li>• An upgrade to, or introduction of, IT equipment;</li> <li>• An upgrade to, or introduction of, software;</li> <li>• Environment or infrastructure change; and</li> <li>• Major changes to access controls.</li> </ul>	Likelihood	3.3 6.3 16.3.5



IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C32	Performance and Capacity Management	A Performance and Capacity Plan ensure that the service has adequate resources available to meet the agreed SLAs. It includes monitoring of the service and defining and implementing expected thresholds with automated alerts being generated when they are exceeded. Performance and capacity monitoring may also include periodic reports to ensure that SLAs and contractual agreements are being met. In addition, monitoring the performance and capacity of services and systems can provide early warning for potential security threats, as well as triggers when additional resources should be allocated to meet increased demands.	Likelihood, Impact	3.2 3.3 12.7.19 22.1
C33	Malware Protection	The installation of malware protection software on all endpoints and devices will reduce the likelihood of malicious code infecting the service. Configuring the protection to perform real-time checks for malware, automatically update its definition database, quarantine any infected files and automatically alert System Administrator(s) will ensure any infection is managed. Additional controls that detect and/or prevent the use of known malicious websites may also be considered. This includes protection against the introduction and propagation of ransomware.	Likelihood, Impact	14.1
C34	Configuration Management	Configuration management is the process of controlling the configuration of the service's components to provide assurance that they have been deployed in accordance with the approved configuration and remain so throughout their lifecycle. It is used for establishing and maintaining consistency of a product's performance, functional and physical attributes with its requirements, design, and operational information throughout its life. Any changes to the system are proposed, evaluated, implemented, and documented using a standardised, systematic approach that ensures consistency, and proposed changes are evaluated in terms of their anticipated impact on the entire system.	Likelihood, Impact	5.5 12.2 14.1 18.1 22.2.14
C35	Release Management	A defined and implemented Release Management process will ensure software and firmware updates (including new releases) and configuration changes are deployed in a non-operational (e.g., development or test) environment prior to being deployed into production. It will also ensure that use cases, regression testing, and user acceptance testing is performed in line with the scope of the changes to the system.	Likelihood	14.4.4
C36	Patch and Vulnerability Management	Ensure that security patches are applied in a timely fashion to manage software and firmware corrections, vulnerabilities, and performance risks. Critical patches must be applied within two days of the release of a patch, and other patches should be applied as soon as possible or as per vendor recommendations. For higher handling requirements agencies must ensure that appropriate patching and maintenance of software is undertaken.	Likelihood	6.2 12.4
C37	System Hardening	Ensure standard operating environments (SOE) are hardened in order to minimise known vulnerabilities and attack vectors. Aligning with hardening standards (e.g., vendor guidelines or Centre for Internet Security [CIS] benchmark) limits the opportunity for a vulnerability in the service to be exploited.	Likelihood	14.1 14.2
C38	Security of Network Services	Ensure that network services (including those outsourced) are protected against malicious and accidental compromise by identifying and implementing appropriate security mechanisms and management processes. Means of securing network services include: <ul style="list-style-type: none"> <li>Using structured internet and network addressing and naming schemas (e.g., IPv4/6, DNS);</li> <li>Identifying and creating network trust domains based on business security requirements (e.g., Guest networks, user networks, etc.);</li> <li>Limiting access to network services and security domains (e.g., Management zones); and</li> <li>Protecting network records using secure protocols and cryptographic technologies (e.g., DNSSEC, secure routing).</li> </ul>	Likelihood	18.0
C39	Intrusion Detection and Prevention	Intrusion Detection and Prevention monitors network and/or system activities for malicious activity. The main functions are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. They can be deployed in four ways: <ul style="list-style-type: none"> <li>Network-Based Intrusion Prevention System (NIPS): monitors the entire network for suspicious traffic by analysing protocol activity;</li> <li>Wireless Intrusion Prevention Systems (WIPS): monitor a wireless network for suspicious traffic by analysing wireless networking protocols;</li> <li>Network Behaviour Analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations; and</li> <li>Host-Based Intrusion Prevention System (HIPS): an installed software package which monitors a single host for suspicious activity by analysing events occurring within that host.</li> </ul> For higher handling requirements agencies must ensure that IDP/IDS is implemented, along with appropriate supporting processes.	Likelihood, Impact	3.2 3.3 7.1.7 8.3 18.4
C40	Tenant Segregation	Tenant Segregation is achieved through the implementation of the appropriate multi-layered controls that considers the deployment (e.g., private, hybrid, public, etc.) and service model (SaaS, PaaS, and IaaS). Segregation (separation) between tenants' domains ensures that tenant information and services are isolated within enforced boundaries. Proper segregation also provides assurance that incidents are contained and only affect the affected tenant and do not extend to co-tenants. Effective tenant segregation ensures that one tenant cannot deliberately or inadvertently interfere with the security of the other tenants.	Likelihood, Impact	22.2
C41	Segregation of Networks	Ensure that the network is separated adequately, including the incorporation of security domains (Demilitarised zones and virtual local area networks) to segregate information systems with specific security requirements or different levels of trust. Where appropriate, isolation controls such as switch port isolation and private VLANs are used to isolate hosts within the same security domain.	Likelihood, Impact	18.1.13 19.1.14 22.3
C42	Separation of Non-Production Environments	To prevent unauthorised access or changes to the operational environment, non-operational environments such as development, test and training environments must be separated from operational ones. Consider the following to ensure effective separation of environments: <ul style="list-style-type: none"> <li>All changes must be tested in a non-operational environment before being transferred into the operational environment;</li> <li>Testing must not be done in operational environments;</li> <li>Rules for the transfer or installation of software into operational environments from non-operational environments;</li> <li>Users must have different accounts for operational and non-operational environments; and</li> <li>Operational or production data must not be used in non-operational environments, unless the same security controls are in place in the non-operational environment.</li> </ul>	Likelihood, Impact	14.4

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C43	Firewalls	Firewalls are deployed to monitor and control connections and information flows between security domains. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a firewall before granting access to internal systems. Configure the firewall rule-base to limit the inbound and outbound (ingress and egress) connections, protocols and ports required to support the service, and ensure firewalls are VoIP-aware.	Likelihood and Impact	14.1 14.4 14.5 18.1 19.1 19.3 19.5.26 21.1.5 21.4.10.C.14
C44	Business Continuity Plan	Ensure that Business Continuity Plans are established to assist in meeting business requirements, minimise disruption to the availability of information and systems and assist recoverability. By defining the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for the Service, business owners can ensure that continuity objectives are able to be achieved. Developing and testing a plan confirms that appropriate measures to ensure the continuity of critical business services are identified and implemented.	Impact	6.4
C45	Disaster Recovery Plan	Ensure that Disaster Recovery Plans are established to assist in meeting business requirements, minimise disruption to the availability of information and systems and assist recoverability. Defining, implementing, and testing a Disaster Recovery Plan supports the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirements defined in the Business Continuity Plan. For higher handling requirements agencies must ensure that Disaster Recovery plans cater for cloud-based services.	Impact	3.2.17 3.3.12 6.4
C46	System Redundancy	Ensure that sufficient redundancy exists within the system to protect against system outages. This can be done by including the following controls in system designs: <ul style="list-style-type: none"> <li>• Clustering;</li> <li>• Load balancing;</li> <li>• Network redundancy; and</li> <li>• System redundancy.</li> </ul>	Likelihood, Impact	3.3 6.4.5
C47	Information Security Review	Ensure Information Security reviews are conducted at least annually to maintain the security of systems and detect gaps and deficiencies, including: <ul style="list-style-type: none"> <li>• Identifying any changes to the business requirements or concept of operation for the subject of the review;</li> <li>• Identifying and changes to the security risks faced by the subject of the review;</li> <li>• Assessing the effectiveness of the existing countermeasures;</li> <li>• Validating the implementation of controls and countermeasures; and</li> <li>• Reporting on any changes necessary to maintain an effective security posture</li> </ul>	Likelihood	3.2 4.1 4.2 4.3 4.4 4.5 6.1
C48	Architecture and Design Review	Reviewing the architecture and design of the service ensures that it meets the functional and non-functional business requirements including adequate controls to protect the confidentiality, integrity and availability of information stored, processed, or transmitted by the service. An Architecture and Design review will also assess the organisation's adoption of, and integration with, the service to ensure that the organisation's own security controls will meet the businesses requirements. Architecture and Design Reviews should be regularly conducted to verify that changes in the threat landscape and NZISM requirements are considered.	Likelihood, Impact	4.3 5.1.8 6.1 14.2 14.3 14.4 14.5 18.1 19.1 19.3 21.4 22.2.14
C49	Security Tests and Controls Audit	Ensure that information assurance activities such as controls audit and technical security assessments are conducted against systems to demonstrate that due consideration has been paid to risk, security, functionality, business requirements and as a fundamental part of information systems governance and assurance. The assurance activities should focus on validating whether: <ul style="list-style-type: none"> <li>• Security posture of the organisation has been incorporated into its system security design;</li> <li>• Controls are correctly implemented and are performing as intended;</li> <li>• Changes and modifications are reviewed for any impact or implications; and</li> <li>• Effectiveness of Information Security measures for systems is periodically reviewed and validated.</li> </ul> Penetration tests (when allowed), also provide assurance that exploitable information system weaknesses are identified, controls are configured and enforced to protect against real world attack scenarios.	Likelihood	3.3 4.1 4.2 4.3 6.1 6.2

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C50	Data Loss Prevention	Depending on the solution and the risk posture of information leakage, Data Loss Prevention (DLP) or Cloud Access Security Broker (CASB) technologies or and techniques are implemented to safeguard sensitive or critical information from leaving the organisation. They operate by identifying unauthorised use and data exfiltration and take remedial action by monitoring, detecting, and blocking unauthorised attempts to exfiltrate data. For DLP to be effective, all data states (processing, transmission, and storage) are monitored. <ul style="list-style-type: none"> <li>Agency managed and/or unmanaged devices with an ability of information upload in the cloud storage are proactively monitored to avoid accidental information disclosure in the cloud instance or on their personal cloud drives;</li> <li>Tools like DLP and CASB are installed on the endpoints and enabled with logging/monitoring to protect from security incidents of information disclosure;</li> <li>Data loss protection rules shall be configured in protection mode;</li> <li>Rules Shall be reviewed and modified on regular basis, and upon related security incident/breach; and</li> <li>Administrative access to these tools is restricted to authorised personal only.</li> </ul>	Likelihood, Impact	7.3.7 7.3.8 14.1.13.C.03 21.4.5 21.4.14.C.02 21.1.24
C51	Application Security	Establishing rules for the development of software and systems will ensure that the developers use secure development practices such as those defined and documented by Microsoft and the Open Web Application Security Project (OWASP).  Functional testing is primarily used to verify that a service or a piece of software is providing the functionality required by the business. Typically, functional testing involves evaluating and comparing each service or software function with the business requirements (including security).  By implementing an application proxy at web-based interfaces, the service will be protected against a wide range of Layer 3 – 7 attacks including DoS (e.g., SYN Flooding, Smurf, ICMP Ping Flood, Fraggle attacks), SQL Injection and Cross Site Scripting (XSS). Inspecting external traffic (inbound and outbound), messages and attachments for malicious content at the gateway will reduce the likelihood of malicious code entering the service. The content filter can be configured to quarantine any suspicious files and automatically alert the System Administrator(s) when malicious content is detected. It may also be configured to restrict the file types that can be transferred into and out of the Organisation’s environment to only those that are required by the business.	Likelihood, Impact	12.2 12.7.19 12.7.20 14.3 14.4 14.5 19.0 20.3
C52	Data Management	Ensure data transfers are performed in accordance with the policy and processes and are approved by a trusted source.  All classified information that are stored within a database are labelled appropriately with protective markings and database files are protected from access that bypasses the database’s normal access controls.	Likelihood, Impact	20.0 22.1
C53	Governance	Ensure an appropriate governance structure is in place for providing oversight to make sure that risks are adequately mitigated, and controls are implemented to mitigate risks.	Likelihood, Impact	3.0 4.1 4.4 4.5 5.1 6.1 16.4 16.7 19.5 22.1
C54	Asset Management	Ensure physical measures are applied to facilities, IT equipment and communication devices so to protect systems and their infrastructure.	Likelihood	7.3.2 8.0 11.2.16.C.01 11.4 11.4.12 22.2.16.C.01
C55	Billing and Resource Management	To develop and manage Information Security budget projections and resource allocations based on short-term and long-term goals and objectives.	Likelihood	3.3 3.3.9.R.01
C56	Location of IaaS Service	Services may be hosted inside or outside of New Zealand, and it may be possible to choose what locations agencies can choose to house their services. If a SP has a global presence, data may transit, or be backed up in foreign datacentres which may not be transparent to CA.  Support services for services hosted in a country may be provided from another jurisdiction, which should be considered when purchasing IaaS services.	Impact	22.1.22
C57	Privacy Impact Assessment	To assess the privacy impacts of a project and where necessary (e.g., application, platform, database, a service, procedure), a privacy impact assessment (PIA) must be conducted in order to comply with Privacy Act’s, the privacy of individuals, and assist in making decisions about how to mitigate and manage privacy risks.	Impact	3.2 3.3 3.1.9.C.01 5 22.1.22
C58	Dedicated Network Connectivity	Dedicated network connectivity, or dedicated private networks, allow customers to attach their networks to service providers directly. This allows them to bypass network providers through a direct connection physically and reduces capacity and internet routing issues.	Impact	18.2 19.1

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C59	Denial of Service Protection	To protect a virtual environment from being exploited by a Denial of Service (DoS) attack, develop and implement a Denial of Service (DoS) response strategy that includes: <ul style="list-style-type: none"> <li>To identify the source of DoS, either internal or external;</li> <li>How to diagnose the incident or attack type and attack method;</li> <li>How to minimise the effect of a DoS attack; and</li> <li>How to protect against Distributed Denial of Service (DDoS) attacks.</li> </ul>	Impact	16.1.14 18.3 19.2 19.5 21.4 22.2.15
C60	Content Delivery Network	A content delivery network, or content distribution network (CDN), is a geographically distributed network of proxy servers and their datacentres. The goal is to provide high availability and performance by distributing the service spatially relative to end users.	Impact	N/A
C61	Exit Strategy	A planned approach to terminating a service in a way that will maximise benefit and minimise damage to the organisation. This may include considering termination and early-withdrawal fees, cancellation notification, data extraction mechanisms, and use of common information types that can be easily transferred.	Impact	N/A
C62	Out-of-band Administration	Administration of the servers has to be conducted through a dedicated network to prevent management data being intercepted and the network capacity being saturated by the users' activity or DoS attacks. This could be implemented by either a dedicated hardware network interface, dedicated VPN or by implementing traffic throttling at all the required stages to ensure enough network capacity is available for the administration access.  Access to console information like system logs, system command line and the ability to restart systems that are unresponsive should also be available independently of the ability to access the applications on the system.	Likelihood, Impact	18.6 22.3
AZ.C01	NZISM Restricted Blueprint	Azure offers a security blueprint referred to as the " <a href="#">NZISM Restricted Blueprint</a> ". This provides governance guardrails using Azure Policy that help agencies assess specific New Zealand Information Security Manual (NZISM) controls. This blueprint helps customers deploy a core set of policies for any Azure-deployed architecture that must implement controls for New Zealand ISM Restricted. The suggested controls and features suggested in the <a href="#">NZISM Restricted Blueprint</a> should be configured and applied to services.	Likelihood, Impact	N/A

Released under the Official Information Act 1982

**Table 13 – Controls to Risk Mapping**

9(2)(b)(ii), 9(2)(k)



Released under the Official Information Act 1982



Released under the Official Information Act 1982

9(2)(b)(ii), 9(2)(k)



Released under the Official Information Act 1982

## Appendix A – Consulted Stakeholders

The stakeholders below were consulted to inform the Risk Assessment. This took the form of three workshops. One was held with the vendor of Azure on 21/03/2022. Another was held for business context on 23/03/2022 with agency nominated business representatives. The final workshop was a technical context workshop on 25/03/2022 and was held with agency nominated technical representatives including solution architects.

**Table 14 – Consulted Stakeholders**

Attendee	Role	Agency Name
Alan Woods	Infrastructure Service Manager and Security Officer	Pharmac
David Lister	Senior Information Security Specialist	Ministry of Social Development
Dayanand Deshpande	Enterprise Architect	Ministry of Social Development
Gareth Miles	Senior Business Analyst and ICT Consultant	Electoral Commission
Hiren Desai	Solution Architect	Ministry of Social Development
Ian Henry	Senior Manager IT Services	Electoral Commission
Paul Headland	Technical Specialist Common Capabilities	Department of Internal Affairs
Rachel Goddard	DPO Identity and Application owner of Azure AD	Ministry of Social Development
Rhys Gibson	Manager of Programmes and Architecture	Tertiary Education Commission
Russell Craig	National Technology and Security Officer	Microsoft New Zealand
Samuel Johnstone	Information Technology Security Manager	Institute of Environmental Science and Research
Tiaan De Klerk	Principal Architect	Tertiary Education Commission



## Appendix B – Project Overview

The Risk Assessment was undertaken in accordance with the statement of work dated 22 February 2022.

### Scope

The Department of Internal Affairs (DIA), as Government Chief Digital Officer (GCDO) performed an information security Risk Assessment of the use and operations of the Microsoft Azure.

This Risk Assessment focused on the use of Azure Cloud services including:

- Azure Active Directory;
- Azure AD B2C;
- Azure AD B2B;
- Azure Windows Virtual Machines;
- Azure Linux Virtual Machines;
- Azure Storage;
- Azure Key Vault;
- Virtual Network; and
- Express Route.

### Approach

The Risk Assessment followed the Government Chief Digital Officer (GCDO) risk framework based on the AS/NZS ISO 31000:2009 and ISO/IEC 27005:2011 risk management standards. The assessment was conducted as a series of workshops and document reviews, including:

- Consumption of documentation provided by the project team;
- Identification of risks and consequences of security breaches associated with the use of the solution through business context and technical context workshops;
- Development of a Risk Assessment report in draft;
- Risk validation review by key stakeholders; and
- Issuance of a final Risk Assessment report.

### Documents Referenced

The following documentation were referenced and used to inform the Risk Assessment:

- All of Government Cloud Computing: Information Security and Privacy Considerations April 2014
- GCDO 105 Cloud Questionnaire
- Azure Cloud Risk Assessment Report, v1.0, 31/05/2016

## Appendix C – Risk Assessment Guidelines

### Rating Risk

The likelihood and impacts of the risks have been rated using the simple qualitative scales documented below. The identified risks were assessed with no controls in place. This provided the gross risk rating and enabled the effectiveness of the proposed controls to be assessed.

### Likelihood (Probability) Assessment

The qualitative scale used to assign a likelihood rating is presented in Table 13 below. Where information is available about the frequency of an incident in the past it should be used to determine the likelihood of the risk eventuating. However, where such information does not exist it does not necessarily mean that the likelihood of the risk eventuating is low. It may merely indicate that there are no controls in place to detect it or that the Agency has not previously been exposed to the particular risk.

Table 15 – DIA Risk Likelihood Scale

Rating	Description	Meaning
5	Almost Certain	It is easy for the threat to exploit the vulnerability without any specialist skills or resources, or it is expected to occur within 1 – 6 months.
4	Highly Probable	It is feasible for the threat to exploit the vulnerability with minimal skills or resources, or it is expected to occur within 6 – 12 months.
3	Possible	It is feasible for the threat to exploit the vulnerability with moderate skills or resources, or it is expected to occur within 12 – 36 months.
2	Possible but Unlikely	It is feasible but would require significant skills or resources for the threat to exploit the vulnerability or it is expected to occur within 3 – 5 years.
1	Almost Never	It is difficult for the threat to exploit the vulnerability or it is not expected to occur within 5 years.

### Impact (Consequences) Assessment

The qualitative scale used to assign an impact rating is presented in Table 16. All impacts were analysed in a business context. The impact of risks includes a consideration of any possible knock-on effects of the consequences of the identified risks, including cascade and cumulative effects.

Table 16 – AoG DIA All-of Government Risk Consequence Guide (choose the scale that best applies to the agency)

Rating	Description	Reputation	Health and Safety	Service Delivery	Financial
5	Severe	<ul style="list-style-type: none"> <li>The Agency suffers severe political and/or reputational damage that is cannot easily recover from.</li> <li>The Government suffers severe negative reputational impact, and the Prime Minister loses confidence in the Minister and/or the Agency's senior management.</li> <li>Minister and Chief Executive need to be briefed and regularly updated.</li> <li>Media interest is sustained for a prolonged period (i.e., over a week) with major criticism levelled at the Minister and/or the Agency.</li> <li>The Agency breaches multiple laws, which leads to legal action by affected stakeholders.</li> <li>External/independent investigation is commissioned by the SSC, GCDO or OPC.</li> <li>The SSC and GCDO manage the communications and recovery.</li> </ul>	<ul style="list-style-type: none"> <li>Loss of life.</li> <li>Major health and safety incident involving members of staff and/or members of the public.</li> <li>The injured party or parties suffer major injuries with long-term effects that leave them permanently affected.</li> <li>An external authority investigates the Agency's safety practices and the Agency is found to be negligent.</li> </ul>	<ul style="list-style-type: none"> <li>Severe compromise of the strategic objectives and goals of the Agency.</li> <li>Severe compromise of the strategic objectives of the NZ Government or other agencies.</li> <li>Severe on-going impact on service delivery across NZ Government or multiple agencies.</li> <li>Skills shortages severely affect the ability of the Agency to meet its objectives and goals.</li> <li>Staff work hours are increased by more than 50% (20 hours per week) for more than 30 days.</li> <li>Between a 10% or more increase in staff turnover in a six-month period that can be directly attributed to the risk eventuating</li> </ul>	<ul style="list-style-type: none"> <li>Impact cannot be managed without additional funding from government.</li> <li>Impact cannot be managed without significant extra human resources.</li> <li>Yearly operating costs increase by more than 12%.</li> <li>One-time financial cost greater than \$100,000.</li> </ul>
4	Significant	<ul style="list-style-type: none"> <li>The Agency suffers significant political and/or reputational damage.</li> <li>Minister suffers reputational damage and loses confidence in the Agency's senior management.</li> <li>Minister and Chief Executive need to be briefed and regularly updated.</li> <li>Media interest is sustained for up to a week with minor criticism levelled at the Agency.</li> <li>Key stakeholders need to be informed and kept up to date with any developments that affect them.</li> <li>The Agency breaches the law, which leads to legal action by affected stakeholders.</li> <li>External/independent investigation is commissioned by the SSC, GCDO or OPC.</li> <li>Communications and recovery can be managed internally with strong guidance from the SSC and GCDO.</li> </ul>	<ul style="list-style-type: none"> <li>A significant health and safety incident involving multiple members of staff and/or members of the public.</li> <li>The injured party or parties suffer significant injuries with long-term effects that leave them permanently affected.</li> <li>An external authority investigates the Agency's safety practices and the Agency is found to be inadequate.</li> </ul>	<ul style="list-style-type: none"> <li>Significant compromise of the strategic objectives and goals of the Agency.</li> <li>Compromise of the strategic objectives of the NZ Government or other agencies</li> <li>Significant on-going impact on service delivery across one or more business unit or multiple agencies.</li> <li>Skills shortages affect the ability of the Agency to meet its objectives and goals.</li> <li>Staff work hours are increased by more than 38% (10 – 15 hours per week) for 30 days.</li> <li>Between a 3% and 10% increase in staff turnover in a six-month period that can be directly attributed to the risk eventuating.</li> </ul>	<ul style="list-style-type: none"> <li>Impact cannot be managed without re-prioritisation of work programmes.</li> <li>Impact cannot be managed without extra financial and human resources.</li> <li>Yearly operating costs increase by 10% to 12%.</li> <li>One-time financial cost between \$50,000 and \$100,000.</li> </ul>
3	Moderate	<ul style="list-style-type: none"> <li>Agency suffers limited political and/or reputation damage.</li> <li>Minister is informed and may request to be briefed.</li> <li>The Chief Executive and senior management need to be briefed and regularly updated.</li> <li>The Agency breaches its compliance obligations.</li> <li>Media interest is sustained for less than a week with minor criticism levelled at the Agency.</li> <li>Key stakeholders need to be informed and kept up to date with any developments that affect them.</li> <li>External/independent investigation is commissioned by the Agency.</li> <li>Most communications and recovery can be managed internally with some guidance from the GCDO.</li> </ul>	<ul style="list-style-type: none"> <li>Health and safety incident involving multiple members of staff or one or more members of the public.</li> <li>The injured party or parties suffer injuries with long-term effects and are not permanently affected.</li> <li>The Agency's safety practices are questioned and found to be inadequate.</li> </ul>	<ul style="list-style-type: none"> <li>Compromise of the strategic objectives and goals of the Agency.</li> <li>Moderate impact on service delivery across one or more business unit due to prolonged service failure.</li> <li>Staff work hours are increased by less than 25% (8 – 10 hours per week) for a two-to-four-week period.</li> <li>Between a 1% and 3% increase in staff turnover in a six-month period that can be directly attributed to the risk eventuating.</li> </ul>	<ul style="list-style-type: none"> <li>Impact can be managed with some re-planning and modest extra financial or human resources.</li> <li>Yearly operating costs increase by 7% to 10%.</li> <li>One-time financial cost of \$20,000 to \$50,000.</li> </ul>
2	Minor	<ul style="list-style-type: none"> <li>Senior management and/or key stakeholders believe that the agencies reputation has been damaged.</li> <li>The Chief Executive needs to be advised.</li> <li>Senior management needs to be briefed.</li> <li>Media interest is short-lived (i.e., a couple of days) and no blame is directed at the Agency.</li> <li>Key stakeholders need to be informed.</li> <li>Communications and recovery can be managed internally.</li> </ul>	<ul style="list-style-type: none"> <li>Minor health and safety incident involving multiple members of staff or a member of the public.</li> <li>The injured party or parties suffers minor injuries with only short-term effects and are not permanently affected.</li> </ul>	<ul style="list-style-type: none"> <li>Minor impact on service delivery across one or more branch due to brief service failure.</li> <li>Limited effect on the outcomes and/or objectives of more than one business unit.</li> <li>Staff work hours are increased by less than 15% (6 hours per week) for less than two weeks.</li> <li>Less than a 1% increase in staff turnover in a six-month period that can be directly attributed to the risk eventuating.</li> </ul>	<ul style="list-style-type: none"> <li>Impact can be managed within current resources, with some re-planning.</li> <li>Increase of between 5% and 7% in yearly operating costs.</li> <li>One-time financial cost between \$10,000 and \$20,000.</li> </ul>
1	Minimal	<ul style="list-style-type: none"> <li>Reputation is not affected.</li> <li>No questions from the Minister.</li> <li>No media attention.</li> <li>All communications and recovery can be managed internally.</li> </ul>	<ul style="list-style-type: none"> <li>No loss or significant threat to health or life.</li> <li>The Agency's safety practices are questioned but are found to be appropriate.</li> </ul>	<ul style="list-style-type: none"> <li>Limited effect on the outcomes and/or objectives of a business unit.</li> <li>Staff work hours are increased by less than 5% (1 – 2 hours per week) for less than seven days.</li> <li>No increase in staff turnover as a result of the risk eventuating.</li> </ul>	<ul style="list-style-type: none"> <li>Impact can be managed within current resources, with no re-planning.</li> <li>Increase of less than 5% in yearly operating costs.</li> <li>One-time financial cost of less than \$10,000.</li> </ul>

**Table 17 – Risk Matrix**

Table 16 presents a 5x5 matrix for assigning a risk rating to a risk. It is used by mapping the likelihood and impact ratings. The rating being the point where the likelihood and impact ratings intersect.

Impact	Severe	15	19	22	24	25
	Significant	10	14	18	21	23
	Moderate	6	9	13	17	20
	Minor	3	5	8	12	16
	Minimal	1	2	4	7	11
		Almost Never	Possible but Unlikely	Possible	Highly Probable	Almost Certain
		Likelihood				

**Escalation of Risk**

Table 18 below provides an example of risk escalation and reporting table. It defines who must be informed and has authority to accept risk based on its magnitude.

**Table 18 – Risk Escalation and Reporting**

Risk Escalation and Reporting levels for each level of risk	
Zone 4	Chief Executive
Zone 3	Senior Leadership Team
Zone 2	Business Owner
Zone 1	Service Manager or Project Manager