



Public Cloud Infrastructure-as-a- Service (IaaS)

Risk Assessment Report October 2021

*Issued by
Digital Public Service Branch*



Document Control

Document Information

Project ID/Name	Public Cloud Infrastructure-as-a-Service Risk Assessment
Author	9(2)(a) PrivSec Consulting Ltd
Title	Public Cloud Infrastructure-as-a-Service (IaaS) Risk Assessment Report
Document Number	PC.IaaS.RA.2021.061

Revision History

Version	Date	Author	Description of changes
0.1	14/09/2021	9(2)(a)	Initial Draft
0.2	28/09/2021	9(2)(a)	Updates Based on Workshops
0.3	29/09/2021	9(2)(a)	Technical Quality Assurance
0.4	30/09/2021	9(2)(a)	Updates Based on QA
0.5	07/10/2021	9(2)(a)	Implemented Feedback from Agencies & DIA
0.6	12/10/2021	Yannick Devos	Quality Assurance
1.0	21/10/2021	Katrina Banks	Finalised for Sign-Off

Released under the Official Information Act 1982

Document Approval

I approve this Risk Assessment report; it presents the Information Security risks introduced to Consuming Agencies through the use of Public Cloud IaaS 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
Jane Kennedy General Manager AoG services Delivery, Digital Public Service Branch Department of Internal Affairs Te Tari Taiwhenua	Original Signed	28/10/21

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
Katrina Banks Manager Security AoG Services Delivery, Digital Public Service Branch Department of Internal Affairs Te Tari Taiwhenua	Original Signed	21/10/21

Glossary of Terms

Availability	Ensuring that authorised users have timely and reliable access to information.
API	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.
B2B	Business-to-business (B2B), also called B-to-B, is a form of transaction between businesses
Confidentiality	Ensuring that only authorised users can access information.
Consequence	The outcome of an event. The outcome can be positive or negative. However, in the context of Information Security it is usually negative.
Control	A risk treatment implemented to reduce the likelihood and/or impact of a risk.
Gross Risk	The risk without any risk treatment applied.
Impact	See Consequence.
Information Security	Ensures that information is protected against unauthorised access or disclosure users (confidentiality), unauthorised or improper modification (integrity) and can be accessed when required (availability).
Integrity	Ensuring the accuracy and completeness of information and information processing methods.
Likelihood	See Probability.
NIST	The National Institute of Standards and Technology (NIST) is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness.
Probability	The chance of an event occurring.
POC	A proof of concept (POC) is a demonstration to verify that certain concepts or theories have the potential for real-world application.
Recovery Point Objective (RPO)	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.
Recovery Time Objective (RTO)	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.
Residual Risk	The risk remaining after the risk treatment has been applied.
Risk	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.
Risk Appetite	The amount of risk that the organisation is willing to accept in pursuit of its objectives.

IN-CONFIDENCE

Risk Owner	A person or entity with the accountability and authority to manage a risk. Usually, the business owner of the information system or service.
SRS Panel	The ICT Security and Related Services Panel (SRS Panel) are a group of industry experts contracted to provide government agencies with ICT services and advice on a range of security and privacy practices.
Stakeholder	A person or organisation that can affect, be affected by, or perceive themselves to be affected by a risk eventuating.
Threat	A potential cause of a risk.
Vulnerability	A weakness in an information system or service that can be exploited by a threat.

Released under the Official Information Act 1982

Contents

Document Control	2
Document Information	2
Revision History	2
Document Approval	3
Executive Summary	7
Introduction	7
Key Risks	7
Gross Risks	9
Consuming Agency Key Recommendations	10
Service Provider Key Recommendations	12
Residual Risks	13
Business Context	14
Certification Approach	14
Cloud Service Models	15
Shared Responsibilities for Security in Cloud Service Models	16
Scope	17
Stakeholders	17
Information Classification	18
Business Processes Supported	18
Business Impact	19
Security Requirements	19
Users	20
Legislation, Policy and Guidelines	20
Information Protection Priorities	20
Detailed Risks	22
Controls Catalogue	51
Appendix A – Consulted Agencies	62
Appendix B – Project Overview	63
Appendix C – Risk Assessment Guidelines	64
Rating Risk	64
Likelihood (Probability) Assessment	64
Impact (Consequences) Assessment	64
Appendix D – Mapping of Services Between Service Providers	67
Appendix E – Controls and Considerations for Offshore Hosted Office Productivity Security Requirements	68

Executive Summary

Introduction

This report presents the findings of an Information Security Risk Assessment of Public Cloud Infrastructure as a Service (IaaS) 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 Public Cloud IaaS provider 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 Public Cloud IaaS, 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 **Public Cloud IaaS Service Provider** are used in this report, they refer to **Consuming Agency (CA)** and **Public Cloud IaaS Service Provider (SP)** respectively.

9(2)(k)



9(2)(k)



Released under the Official Information Act 1982

Gross Risks

Table 1 illustrates the rating of each risk without any controls in place.

Table 1 – Gross Risk Ratings

9(2)(k)

Consuming Agency Key Recommendations

The Risk Assessment included key controls that if implemented, helps to address the identified risks. A controls validation plan (CVP) was also developed to specify the recommended controls outlined in the Risk Assessment.

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

1. Risk Management and Due Diligence

Before the consumption of the Public Cloud IaaS service, 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. It may also involve conducting a data impact assessment, privacy assessment, or jurisdictional Risk Assessment depending on the types of data to be stored. Aspects related to supply chain risks and the ability to obtain appropriate security assurance from the supplier must be included.

This enables CA's to meet their obligations to protect the confidentiality, integrity, availability and privacy of official information.

2. Access Controls

Robust access controls within a cloud environment are needed to ensure that only those who require access can access resources. Utilising tools such as privileged access management, access groups and conducting access reviews can reduce the likelihood of security issues related to access. Ensuring strong password policies are used by staff and enabling MFA for all users accessing an IaaS providers portal are important in reducing the likelihood for compromise.

3. System Maintenance

Having well defined system maintenance in place for IaaS resources is as important for retaining the security posture of services. As the responsibility for patching, upgrading and maintenance of operating systems and applications resides with an Agency as part of the shared responsibility model for IaaS, Agencies must assign these responsibilities to themselves or another party, such as a managed service provider.

4. Hardening IaaS Resources

It is the responsibility of CA to ensure that any resources established within their IaaS environment are appropriately hardened. Unlike a Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) service, it is the responsibility of the Agency to ensure that the servers and applications have appropriate security controls applied. This may include installing endpoint detection tools, applying patches, ensuring that logging is appropriately configured, and applying standard operating system builds.

5. Logging, Alerting and Monitoring

Agencies should ensure they have appropriate logging enabled within their IaaS instances to monitor access and activities, as well as ensuring logging is being captured from virtual machines, as would happen in a traditional on-premises environment. Monitoring the environment will

ensure that activities that malicious activities are detected early and reduces the impact to Agencies.

6. Resilience, BCP and Disaster Recovery Plans

If a security incident occurs, and IaaS resources are no longer available, it is important that appropriate resiliency is in place to ensure critical services still function. Depending on the importance of the services hosted within the environment, services such as auto-scaling groups may help reduce the effect of an attack. Similarly, hosting services over multiple availability zones may reduce the effect of an issue affecting one site.

Strong business continuity plans are important to reduce the impact of an outage of services. Depending on the criticality of a service, manual processes may be able to be reverted to, or alternative systems utilised.

Released under the Official Information Act 1982

Service Provider Key Recommendations

To mitigate and manage the identified gross risks rated as 9(2)(k) 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. A robust supply chain monitoring may include conducting Risk Assessments on providers, conducting audits, ensuring robust change management is in place for introducing new vendors and technologies, and monitoring the cyber threat landscape.

3. Access Controls

Robust access controls within a SP environment are needed to ensure that only those who require access can access resources. SP must ensure that the principal 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 and enforcing MFA for all actions reduces the likelihood for compromise.

4. System Hardening

SP must ensure that appropriate hardening has occurred to hypervisors and supporting infrastructure to reduce the likelihood of compromise of IaaS 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. Ensure systems are part of regular patching, and maintenance is important in ensuring the ongoing security posture of the SP.

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)(k)



Business Context

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

Certification Approach

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

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

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 IaaS 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.

The certification of Public Cloud IaaS will be up to and including IN-CONFIDENCE. If agencies wish to use the services for storing and processing data up to and including Classification Removed then the CA should ensure that the controls highlighted in *Appendix E – Controls and Considerations for Offshore Hosted Office Productivity Security Requirements* are implemented. Where possible, these controls have been highlighted within the controls catalogue as being CA responsibility for Classification Removed

Cloud Service Models

The following table summarises the cloud service models¹ defined by National Institute of Standards and Technology (NIST²). Only IaaS solutions (first item in the table below) are in scope of this security Risk Assessment:

Table 4 – Cloud Services Models

Services	Service Description	Real World Examples
Infrastructure as a Service (IaaS)	The provision of computing resources (i.e. processing, memory, storage and network) to allow the customer to deploy their own operating systems and applications. 9(2)(k)	9(2)(b)(ii)
Platform as a Service (PaaS)	The provision of standardised operating systems and application services (e.g. web server or database platform) delivered on IaaS services to enable customers to deploy and run their own applications developed using programming languages supported by the service provider. 9(2)(k)	
Software as a Service (SaaS)	The provision and consumption of the service provider's standardised application services (e.g. email or customer relationship management) usually on a pay-per-use basis using a web browser or thin client application. 9(2)(k)	

The following table summarises the difference between public and private cloud providers. Only Public Cloud IaaS providers are in scope of this security Risk Assessment:

¹ All of Government Cloud Computing: Information Security and Privacy Considerations April 2014

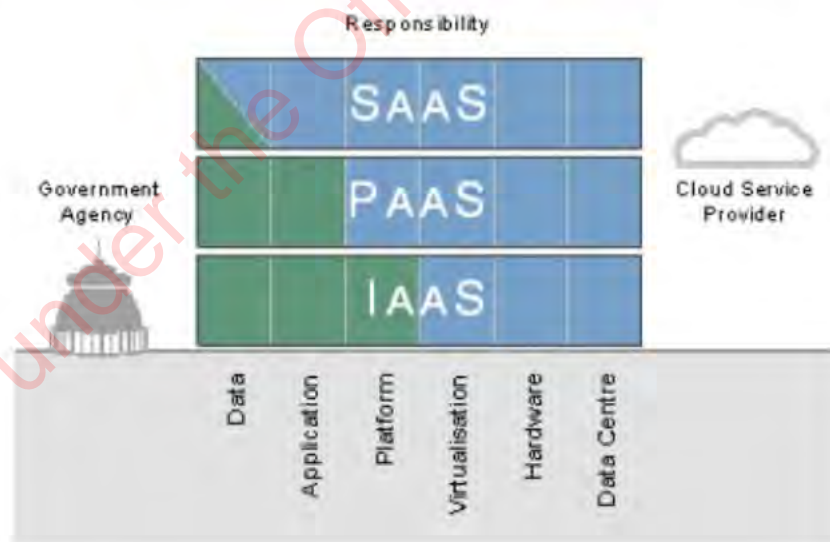
² The NIST Definition of Cloud Computing: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>

Table 5 – Public vs. Community vs. Private Cloud

Service Type	Description	Real World Examples
Public Cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.	<ul style="list-style-type: none"> • Amazon Web Services (AWS) Elastic Cloud Compute (EC2) • Microsoft Azure • Catalyst Cloud • Google Compute Platform (GCP)
Community Cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.	<ul style="list-style-type: none"> • Government IaaS platforms • Datacom Government Cloud
Private Cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.	<ul style="list-style-type: none"> • Self-hosted VMWare Cluster • Private Openstack Instance

Shared Responsibilities for Security in Cloud Service Models

The following diagram³ and table summarises the responsibility boundary for each of the cloud service models:



³ All of Government Cloud Computing: Information Security and Privacy Considerations April 2014

Table 6 – As-a-Service Responsibilities

Cloud Service	SP Responsibility	CA Responsibility
Infrastructure as a Service (IaaS)	9(2)(k)	
Platform as a Service (PaaS)		
Software as a Service (SaaS)		

Scope

The following services are considered within the scope of this assessment, which constitute base IaaS services:

- On-demand compute instances;
- Block Storage;
- Object Storage;
- Software Defined Networking;
- Dedicated Private Network;
- Identity and Access Management;
- Imaging Service;
- Ingress Protection;
- Load Balancing;
- Automate Tasks;
- Auto Scaling;
- Cost Metrics/ Telemetry; and
- Virtual Private Network.

Further details about how these services map to services provided by popular IaaS providers can be found in *Appendix D – Mapping of Services Between Service Providers*.

Stakeholders

The key stakeholders for a generic Software as a service are:

- Consuming Agency;
- Service Provider; and
- Integrator/ Third Party Provider.

Information Classification

Based on the New Zealand Government Security Classification System⁴, the information that will be stored, processed or transmitted by the IaaS service has been classified for **Classification Removed** and below. The compromise of information classified as **Classification Removed** and below can:

- Adversely affect diplomatic relations;
- Hinder the operational effectiveness or security of New Zealand or friendly forces;
- Adversely affect the internal stability or economic wellbeing of New Zealand or friendly countries;
- Prejudice the maintenance of law, including the prevention, investigation and detection of offences, and the right to a fair trial;
- Affect adversely the privacy of natural persons, including that of deceased natural persons.
- Impede government negotiations (including commercial and industrial negotiations);
- Disclose a trade secret or unreasonably to prejudice the commercial position of the person who supplied or is the subject of the information;
- Endanger the safety of any person;
- Prejudice measures protecting the health or safety of members of the public;
- Prejudice measures that prevent or mitigate material loss to members of the public;
- Breach legal professional privilege;
- Impede a Minister of the Crown or any Department or organisation holding the information to carry out, without prejudice or disadvantage, commercial activities; and
- Lead to the disclosure or use of official information for improper gain or advantage.

If, as the result of a security certification audit, the current risk position of a Public Cloud IaaS service is not appropriate for the certification of holding **Classification Removed** information, it may still be appropriate for lower classifications such as **Classification Removed** or IN-CONFIDENCE. This will depend on the nature of the audit findings and any compensating controls that are in place or could be implemented by the consuming agencies with support from the SP. These compensating security controls are similar to the security requirements for offshore hosting on Public Cloud which are detailed at *Appendix E – Controls and Considerations for Offshore Hosted Office Productivity Security Requirements*.

Business Processes Supported

Each CA will be using the IaaS services 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 security requirements for the service. This will ensure that agencies understand the security requirements that the service needs to meet.

During workshops conducted with agencies, some of the use cases they are or are planning on using Public Cloud IaaS services for included:

- Using an on shore Public Cloud IaaS provider to establish a disaster recovery data back-up for an offshore IaaS hosted service;
- Hosting learning management systems for use within and external to agencies;
- Hosting solutions used by NZ citizens that were previously hosted on on-premises infrastructure;
- Hosting web applications, websites and databases; and
- Hosting services that require scalability due to increased traffic during certain times.

⁴ <https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/classification-system/national-security-information/>

Business Impact

Each CA will be using the IaaS 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 IaaS 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 a Public Cloud IaaS provider have been defined as follows:

Confidentiality

The confidentiality of the information transmitted, stored or processed by the IaaS service is assumed as critical for consuming agencies. This is largely driven by the classification of information that will be transmitted, stored or processed by the service. The information processed in the cloud must be protected from unauthorised access and disclosure.

If the confidentiality of information was compromised, the following impacts are expected:

- Disclosure of agency information to unauthorised personnel;
- Loss of key stakeholder confidence in the IaaS;
- 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 IaaS service is assumed as critical for consuming agencies. It is assumed that consuming agencies will be using the 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 was compromised, the following impacts are expected:

- Modification of agency information by unauthorised personnel leading to inaccurate or corrupted data;
- Loss of key stakeholder confidence in the IaaS;
- Reputation damage for the affected CA; and
- Further investigation where required by law.

Availability

The availability of the information transmitted, stored or processed by the IaaS service is assumed as critical for consuming agencies. It is assumed that consuming agencies will be using the IaaS service to store and process information that business relies on. Prolonged service outages can have an adverse impact on business processes reliant on the IaaS, affecting business outcomes.

If the availability of information was compromised, the following impacts are expected:

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

Privacy

Personal identifiable information may be transmitted, stored or processed by the IaaS service. Therefore, it is important that consuming agencies identify and document the types of personal identifiable information that will be transmitted, stored or processed in the IaaS environment.

If personal information will be transmitted, stored or processed within the IaaS environment, 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 IaaS services are configured and operating to help agencies meet the requirements from the Privacy Act 2020. Additionally, Consuming agencies must perform a Privacy Impact Assessment (PIA) to ensure the appropriate level security controls are implemented to protect the CIA of private information.

Users

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

Table 7 – User Groups & Descriptions

User Group	Description
CA IaaS Administrators	Agency staff with privileged access to the IaaS environment. Responsible for managing and configuring the Agency's resources, user accounts, groups and permissions within the cloud environment.
CA Billing Staff	Agency staff with access to the billing information within an IaaS environment.
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 Providers staff with access to the part of the cloud service.
SP Administrators	SP staff with access to the information systems supporting the IaaS service. Responsible for managing the supporting infrastructure and systems that support the service.
SP Third Party	Parties used to supply services to third parties such as datacentre operators.
External Users	Members of the public using public facing applications hosted on Public Cloud IaaS.

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 an IaaS 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 3.4).

Information Protection Priorities

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

Table 8 – 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 88.

Table 9 – 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

Detailed Risks

Table 10 presents the risks associated with use of a Public Cloud IaaS Provider.

Table 10 – Public Cloud IaaS Services Risk Assessment

Risk ID	Risk Description	
IAAS.R01	Lack of Understanding of Agency Security Requirements for IaaS 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R02	Agency Affected by Security Issue Targeted at Another Cloud Platform Tenant 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description
IAAS.R03	Agency Loses Control of Cloud Resources 9(2)(k)



Released under the Official Information Act 1982

Risk ID	Risk Description
IAAS.R04	Unapproved Use of IaaS (Shadow IT) 9(2)(k)



Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R05	Unauthorized CA Administrator Access 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R06	Poor Access Configuration by Agencies 9(2)(k)	

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R07	Network or Technical Misconfiguration Leading to Compromised Hosted Resource 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R08	<p>Malicious Service Provider Administrator Accesses Resources</p> <p>9(2)(k)</p>	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R09	Man in the Middle Attack on Access to Administrative Interface 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R10	Encryption Keys are Mismatched 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description
IAAS.R11	Physical Access Gained to IaaS Hosting Services



Released under the Official Information Act 1982

Risk ID	Risk Description
IAAS.R12	Cross Tenancy Vulnerability by Service Provider 9(2)(k)



Released under the Official Information Act 1982

Risk ID	Risk Description
IAAS.R13	Vulnerability in Software Deployed by Consuming Agency 9(2)(k)



Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R14	Inadequate Security Hardening of IaaS Services 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R15	Data Hosted or Processed in a Foreign Jurisdiction 9(2)(k)	

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R16	Agency Stores Inappropriate Data in IaaS Service 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description
IAAS.R17	Bill Shock or Service Degradation to Agencies due to Over Subscription



Risk ID	Risk Description
IAAS.R18	<p data-bbox="359 344 768 401">Service Provider Unable to Meet IaaS Service Uptake</p> <p data-bbox="350 422 427 449">9(2)(k)</p>



Risk ID	Risk Description	9(2)(k)
IAAS.R19	<p data-bbox="359 338 774 394">Data Not Appropriately Sanitised After Contract Termination</p> <p data-bbox="359 432 774 1058">9(2)(k)</p>	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R20	Insufficient Change and Release Management 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R21	Virtual Machine, Storage, or Service Provider is Compromised by Malware or Ransomware 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R22	Cloud Services Unavailable due to Denial of Service (DoS) 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R23	Cloud Services Unavailable due to Service Provider Outage 9(2)(k)	

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R24	Natural Disaster Causes an Outage at a Datacentre 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R25	Insufficient Network Capacity Between an Agency and the Cloud Provider 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R26	Supply Chain Security 9(2)(k)	

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R27	Lack of Out-of-Band Administration 9(2)(k)	

Released under the Official Information Act 1982

Risk ID	Risk Description	9(2)(k)
IAAS.R28	Ineffective SP Security Incident Management due to Inadequate Logging and Monitoring 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description
IAAS.R29	Ineffective CA Logging and Monitoring 9(2)(k)



Released under the Official Information Act 1982

Controls Catalogue

Table 11 presents the recommended controls to effectively manage the risks recorded in Table 10:

Table 11 – Recommended Controls

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
C01	Contracts and SLAs	<p>Ensure that contracts and associated Service Level Agreements (SLAs):</p> <ul style="list-style-type: none"> Clearly define the legal jurisdiction for contractual disputes relating to the use and function of the service; Clearly define the ownership of the data stored, processed and/or transmitted by the service; Define in which jurisdiction official information can and will be stored, processed and/or transmitted by the service; 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; Ensure that the time to return to full service after a failure or outage, including data restoration, meets the organisation's business continuity requirements; Require that all access to the organisation's information and systems be monitored; Require and specify means to notify to the organisation of any actual or possible unauthorised access; Require engagement with the organisation in resolution of any information access incidents or issues; Require regular reports be delivered from SP on their performance against the SLA's; 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; 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 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. 	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"> Defining the Information Security requirements of the service; Assessing whether the defined Information Security requirements are met by the service; Identifying and assessing any third-party dependencies that the service provider may have; and Ensuring third parties can meet New Zealand security requirements as contractor. <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"> Security vetting all new staff before beginning employment and on a regular basis thereafter; Undertaking an induction process that covers their responsibilities for Information Security; Acknowledging the Code of Conduct and Information Security policy; Acknowledging the employee's Terms and Conditions of Employment; Receiving regular security awareness training; Monitoring and management of changes in employee circumstances and behaviour; and Removing access rights when their employment or contract ceases. 	Likelihood	3.2 3.3 3.5 5.1.7 9.2 19.1.18 22.1.27
C06	Security Vetting	<p>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.</p>	Likelihood	3.5 9.2 9.4

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
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 9.4 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"> • 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 • 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. 	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"> • Assigning access rights aligned with the defined access control policy; • Reviewing access rights on a regular basis; • Disable accounts when a user leaves an organisation; • Disable accounts when a user no longer requires access; and • Remove or update access rights (e.g., when a user change roles within an organisation). 	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"> • Enforcing the use of individual user IDs and passwords to maintain accountability; • Allowing users to select and change their own passwords; • Enforcing a choice of quality passwords (what quality passwords are should be explained in the password policy), including minimum password length and complexity requirements; • Forcing users to change their passwords at the first log-on or if reset; and • Enforcing regular password changes (at least every 90 days) and as needed. 	Likelihood	16.1.40 16.1.41
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"> • Encrypted email; • A secure password reset mechanism that positively authenticates the user (such as a challenge question or multifactor authentication); • A text message to a verified mobile number; and • A telephone call. 	Likelihood	16.1.40 16.1.41

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
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"> • Something you know (e.g., username and password (one-time password (OTP) or reusable), personal identification number (PIN)); • Something you have (e.g., hardware or software token, digital certificate, smartcard); and • Something you are (e.g., biometric fingerprint). 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 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
C20	Logging and Auditing	Ensure that information systems are configured with adequate logging, archived and retained for at least 18 months. Events to be logged includes: <ul style="list-style-type: none"> • User login; • All privileged operations; • Failed attempts to elevate privileges; • Security related system alerts and failures; • System user and group additions, deletions and modification to permissions; • Unauthorised or failed access attempts to systems and files identified as critical to the Agency; • Date and time of the event; • Relevant system user(s) or processes; • Event description; • Success or failure of the event; • Event source (e.g., application name); and • IT equipment location/identification. For higher handling requirements Agencies must ensure that logging and appropriate supporting processes are implemented.	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)	Ensure that security related event logs are analysed regularly using automated security information and event management (SIEM) tools or equivalent to help identify anomalies	Impact	7.1

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
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"> • 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; • Information Security incident response and management training for all system users and administrators; • Address authority responsible for initiating investigations of an Information Security incident; • Detecting security incidents to minimise impacts; • Reporting security incidents, assisting in documenting and understanding the risks and impacts; and • Managing security incidents by identifying and implementing processes for incident analysis and selection of appropriate remediation. 	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 consider carefully 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 Classification Remov 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
C25	Encryption of Data at Rest	<p>Ensuring business Classification Remov private, or otherwise classified information stored on media is encrypted using approved encryption algorithms and protocols, reduces the likelihood of unauthorised disclosure.</p> <p>For higher handling requirements Agencies must ensure that data is encrypted at rest.</p>	Likelihood, Impact	17.1 17.2 17.3 22.1.24.C.04
C26	Physical Security	<p>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.</p> <p>This also involves ensuring environmental controls such as Air Conditioning, Uninterrupted Power Supplies (UPS), and fire suppression are in place to protect the facility.</p> <p>For higher handling requirements Agencies must ensure appropriate physical security controls are in place.</p>	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	<p>Ensure that equipment or assets supporting the service are protected against loss, damage, theft and unauthorised access. The considerations for equipment security includes:</p> <ul style="list-style-type: none"> • Ensuring IT equipment always reside in an appropriate class of secure room; • Storing IT equipment during non-operational hours in an appropriate class of security container or lockable commercial cabinet; • 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; • Using IT equipment without non-volatile media as well as securing its volatile media; • Using an encryption product to reduce the physical storage requirements of the non-volatile media as well as securing its volatile media; and • 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. 	Likelihood, Impact	8.4 9.2 10

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
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"> • Information Security Policies (SecPol) – setting the strategic direction for Information Security; • Systems Architecture – illustrates the structural design of the system including any outsourced services; • Security Risk Management Plans (SRMPs) – identifying security risks and appropriate treatment measures for systems; • System Security Plans (SecPlan) – specifying the Information Security measures for systems; • Standard Operating Procedures (SOPs) – ensuring security procedures are followed in an appropriate and repeatable manner; • Incident Response Plans (IRPs) – outlining actions to take in response to an Information Security incident; • Emergency Procedures – ensuring classified information and systems are secured before personnel evacuate a facility in the event of an emergency; and • 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. 	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"> • An upgrade to, or introduction of, IT equipment; • An upgrade to, or introduction of, software; • Environment or infrastructure change; and • Major changes to access controls. 	Likelihood	3.3 6.3 16.3.5
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.	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 standardized, 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

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
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"> • Using structured Internet and network addressing and naming schemas (e.g., IPv4/6, DNS); • Identifying and creating network trust domains based on business security requirements (e.g., Guest networks, user networks, etc.); • Limiting access to network services and security domains (e.g., Management zones); and • Protecting network records using secure protocols and cryptographic technologies (e.g., DNSSEC, secure routing). 	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"> • Network-Based Intrusion Prevention System (NIPS): monitors the entire network for suspicious traffic by analysing protocol activity; • Wireless Intrusion Prevention Systems (WIPS): monitor a wireless network for suspicious traffic by analysing wireless networking protocols; • 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 • 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. 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"> • All changes must be tested in a non-operational environment before being transferred into the operational environment; • Testing must not be done in operational environments; • Rules for the transfer or installation of software into operational environments from non-operational environments; • Users must have different accounts for operational and non-operational environments; and • 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. 	Likelihood, Impact	14.4
C43	Firewalls	Firewalls are deployed to monitor and control connections and information flows between security domains. For Classification Rem 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"> • Clustering; • Load balancing; • Network redundancy; and • System redundancy. 	Likelihood, Impact	3.3 6.4.5

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
C47	Information Security Review	<p>Ensure Information Security reviews are conducted at least annually to maintain the security of systems and detect gaps and deficiencies, including:</p> <ul style="list-style-type: none"> Identifying any changes to the business requirements or concept of operation for the subject of the review; Identifying and changes to the security risks faced by the subject of the review; Assessing the effectiveness of the existing countermeasures; Validating the implementation of controls and countermeasures; and Reporting on any changes necessary to maintain an effective security posture 	Likelihood	3.2 4.1 4.2 4.3 4.4 4.5 6.1
C48	Architecture and Design Review	<p>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.</p> <p>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.</p> <p>Architecture and Design Reviews should be regularly conducted to verify that changes in the threat landscape and NZISM requirements are considered.</p>	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	<p>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:</p> <ul style="list-style-type: none"> Security posture of the organisation has been incorporated into its system security design; Controls are correctly implemented and are performing as intended; Changes and modifications are reviewed for any impact or implications; and Effectiveness of Information Security measures for systems is periodically reviewed and validated. <p>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.</p>	Likelihood	3.3 4.1 4.2 4.3 6.1 6.2
C50	Data Loss Prevention	<p>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 classification 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.</p> <ul style="list-style-type: none"> 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; Tools like DLP and CASB are installed on the endpoints and enabled with logging/monitoring to protect from security incidents of information disclosure; Data loss protection rules shall be configured in protection mode; Rules Shall be reviewed and modified on regular basis, and upon related security incident/breach; and Administrative access to these tools is classification to authorised personal only. 	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	<p>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).</p> <p>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).</p> <p>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.</p>	Likelihood, Impact	12.2 12.7.19 12.7.20 14.3 14.4 14.5 19.0 20.3
C52	Data Management	<p>Ensure data transfers are performed in accordance with the policy and processes and are approved by a trusted source.</p> <p>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.</p>	Likelihood, Impact	20.0 22.1

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
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
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"> To identify the source of DoS, either internal or external; How to diagnose the incident or attack type and attack method; and How to minimise the effect of a DoS attack. Ensure a Virtual Machine (VM) migration and decommissioning policy and related SOPs are in place.	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

Table 12 – Controls to Risk Mapping

9(2)(k)



The table content is redacted with a large grey block. A diagonal watermark is visible across the redacted area.

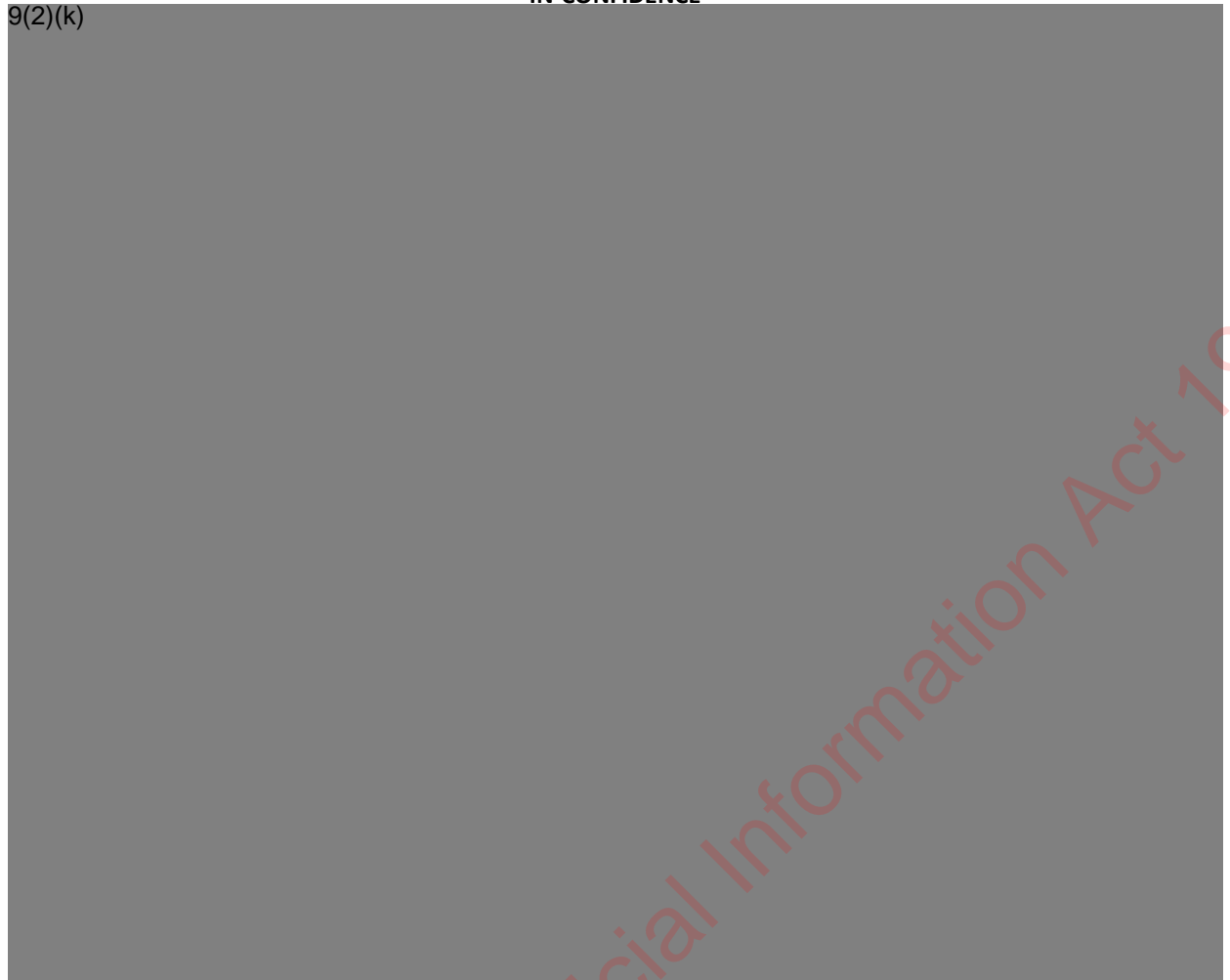
Released under the Official Information Act 1982

9(2)(k)



Released under the Official Information Act 1982

9(2)(k)



Released under the Official Information Act 1982

Appendix A – Consulted Agencies

The following Agency stakeholders were involved in a risk workshop to inform the Risk Assessment:

Table 13 – Consulted Agencies

Attendee	Role	Agency Name
James Robertson	Manager, DigitalNZ Systems	Department of Internal Affairs
Naomi Young	Team Leader, Capability and Learning Design	New Zealand Customs Service
Larry Mitipelo	Thrive System Administrator	Ministry of Justice
Jared Licht	Chief Information Security Officer	New Zealand Defence Force
Aidan Kirrane	Software Applications Manager	New Zealand Electoral Commission
Nicole Higgle	Cyber Security Analyst	New Zealand Electoral Commission
Gordon McBride	Senior Architect	Department of Internal Affairs

Appendix B – Project Overview

Scope

The Department of Internal Affairs (DIA), as Government Chief Digital Officer (GCDO) have written this Risk Assessment report and Controls Validation Plan (CVP) for service providers, for the use of Public Cloud Infrastructure as a Service (IaaS) by consuming Agencies. The objective was to create a generic Risk Assessment and Controls Validation Plan (CVP) for the use of any Public Cloud IaaS provider by consuming Agencies.

The following IaaS services are within the scope of the assessment, and are considered the core IaaS services:

- On-demand compute instances
- Block Storage
- Object Storage
- Software Defined Networking
- Dedicated Private Network
- IAM
- Imaging Service
- Ingress Protection
- Load Balancing
- Automate Tasks
- Auto Scaling
- Cost Metrics/ Telemetry
- Virtual Private Network (VPN)

Further details regarding how these services map to specific offerings by common service providers can be found in *Appendix D – Mapping of Services Between Service Providers*.

Approach

The Risk Assessment followed the 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 DIA
- Identification of risks and controls associated with the use of Public Cloud IaaS Services
- Development of a Risk Assessment report in draft
- Running workshops with consuming Agencies
- 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
- GCIO Cloud Questionnaire
- Infrastructure as a Service (IaaS) Public Cloud Risk Assessment Report, v1.0, 31/05/2016
- GCIO Microsoft Azure Risk Assessment Report, v1.1, 13/03/2017
- Principles of Māori Data Sovereignty, Brief #1, October 2018

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 14 – 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 15. 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 15 – AoG DIA All-of Government Risk Consequence Guide (choose the scale that best applies to you)

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

Table 16 – 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 17 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 17 – 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

Appendix D – Mapping of Services Between Service Providers

The following service names map the generic services covered by the scope of this assessment to specific services provided by various Public Cloud IaaS providers used by Agencies. As functionality of services vary between SP this is only considered indicative.

Table 18 – IaaS Service Mapping

9(2)(b)(ii)



Appendix E – Controls and Considerations for Offshore Hosted Office Productivity Security Requirements

GCDO/GCSB guidance on Security Controls for Hosted Offshore Office Productivity Services⁵ identifies baseline controls that Agencies need to address to ensure compliance of relevant controls from the NZISM. Although not specifically targeted at addressing IaaS services, the controls identified in this document are directly applicable where Agencies need to address higher levels of handling requirements (i.e., **Classification Removed**). Where appropriate, the controls below have been incorporated into this Risk Assessment to maintain alignment.

The following list outlines recommendations Agencies should be aware of in the consumption of the Public Cloud service:

- No material classified at CONFIDENTIAL and above can be stored in offshore office productivity services;
- Agencies must ensure that data is encrypted in transit and at rest;
- Agencies must have sole control over associated cryptographic keys;
- Agencies must ensure that multi-factor authentication is used to control access to the service;
- Agencies must have decommissioning processes as outlined in the NZISM;
- Agencies must ensure that there are appropriate security controls over physical access to Datacentres;
- Agencies must have assurance checks on cloud service providers in accordance with the NZISM;
- Agencies must have controls over the interaction between Public Cloud services and end user devices;
- Agencies must have assurance that appropriate patching and maintenance of software is undertaken;
- Agencies must have process controls relating to intrusion detection, investigations and enterprise logging;
- Agencies must ensure compatibility with existing government security technology services such as **Classification Removed** and, where appropriate, cyber defence capabilities;
- Agencies must ensure there are technical protections to prevent data-mingling on shared storage platforms;
- Where necessary, re-architect Agency ICT networks to ensure that cloud services can be used safely and effectively; and
- Agency must revise their Agency disaster-recovery plans to cater for cloud-based services.

⁵ https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/assets/Uploads/Security-Requirements-for-OH-Office-Productivity-Jan-2017.pdf