ICT Shared Capabilities

Telecommunication as a Service

Risk Assessment Report August 2021

Issued by

Digital Public Service Branch

Te Tari Taiwhenua
Internal Affairs

New Zealand Government

Document Control

Document Information

Project ID/Name	ICT Shared Capabilities, Telecommunication as a Service (TaaS)
Author	Pravin Kasbekar, Security Consultant, AoG Services Delivery
Title	ICT Shared Capabilities Telecommunication as a Service Risk Assessment Report
File name	Telecommunication as a Service Risk Assessment Report

Revision History

Version	Date	Author	Description of change
2.4	19/03/2021	Pravin Kasbekar	Initial refresh document released in draft to consulted agencies.
3.0	12/04/2021	Pravin Kasbekar	Risk Assessment updated to aggregate similar risks and the same control sets. Included feedback from risk review workshop with consulted agencies.
3.1	17/06/2021	9(2)(a)	QA Review Lateral Security.
3.2	21/06/2021	Katrina Banks	Added Management Platform Risks.
3.3	21/07/2021	9(2)(a)	Included Management Platform Risks in document tables.
3.4	25/08/2021	Katrina Banks	Finalised

Document Approval

I approve this Risk Assessment report; it presents the information security risks introduced to Consuming agencies through the use of Telecommunications as a Service (TaaS).

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.

Name and Role	Signature	Date
Jane Kennedy General Manager AoG Services Delivery Department of Internal Affairs Te Tari Taiwhenua	Signed on Original	1 September 2021

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

Name and Role	Signature	Date
Katrina Banks Manager Security AoG Services Delivery Department of Internal Affairs Te Tari Taiwhenua	Signed on Original	31 August 2021

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.

Information Security Professional Services
Industry security experts who provide government agencies with ICT services and advice on a range of security and privacy practices.

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.

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.

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.

Threat Assessment A process of evaluating, verifying perceived threats to ICT services.

Vulnerability] A weakness in an information system or service that can be exploited by a threat.

Contents

List of Tables:

Executive Summary

Introduction

This report presents the findings of an information security Risk Assessment of the Telecommunications as a Service (TaaS). It identifies information security risks for New Zealand Government Agencies (Subscribing Agencies) adopting one or more TaaS services. The Risk Assessment followed the Government Chief Information Officer's (GCIO) Risk Assessment process[1], which is based on the AS/NZS ISO 31000 and ISO/IEC 27005 risk management standards.

This version of Risk Assessment is a comprehensive refresh of the previous TaaS Risk Assessment v2.3, with the vision of simplifying the Digital Public Service Security Certification process for Service Providers and Subscribing Agencies. Though this is a generic Risk Assessment Report based on the recent threats and cyber-attack patterns, the risks identified, and ratings assessed may be different and unique in the context of Subscribing Agencies and the type of TaaS Service involved. Therefore, agencies reading this report should review the risks in view of their adverse deployment of TaaS, while using their own risk management framework. This ensures that the risks identified are specific to the Agency's adoption of TaaS, are within their business context, and risk appetite.

The details of the Risk Assessment scope and TaaS, can be found in Appendix B.

Split Risk Model and Ownership

The Risk Assessment has the "Service Provider Target Rating" that represents a risk rating if the TaaS Service Provider owned security controls are implemented and effective. The "Subscribing Agency Residual Risk Rating" that represents a risk rating if Subscribing Agency owned security controls are implemented and effective.

A split risk model further separates the controls recommended for the Subscribing Agency and those recommended for the Service Provider. This is represented through detailing all identified risks across five risk sections:

- **Detailed Risk Findings – Common Risks Section** - applicable to all TaaS towers and TaaS Management Platform of a Service Provider and their risk IDs are differentiated by; CR<risk number> e.g. **CR01**
- **Detailed Risk Findings – Connectivity Services Section** - specific to Connectivity tower services and their risk IDs are differentiated by; CS-R<risk number> e.g. **CS-R01**
- **Detailed Risk Findings – Communication Services Section** - specific to Unified Communications tower services and their risk IDs are differentiated by; UC-R<risk number> e.g. **UC-R01**
- **Detailed Risk Findings – Contact Centre Services Section** - specific - to Contact Centre tower services and their risk IDs are differentiated by; CC-R<risk number> e.g. **CC-R01**
- **Detailed Risk Findings – Managed Security Services Section** - specific to Contact Centre tower services and their risk IDs are differentiated by; MS-R<risk number> e.g. **MS-R01**
- **Detailed Risk Findings – Service Aggregation Services Section** - specific to Service Aggregation tower services and their risk IDs are differentiated by; SA-R<risk number> e.g. **AS-R01**

[1] [1] https://www.ict.govt.nz/guidance-and-resources/information-management/privacy-and-security/

Agency Responsibilities

The Overall Risk Position in an All of Government (AoG) service delivered by DIA as Lead Agency (LA) is different between Subscribing Agencies (SAs) based on the following factors such as: Business Context, Risk Environment and Risk Appetite. SAs consuming the TaaS services are responsible for performing their own Security Risk Assessment (SRA) and Privacy Impact Assessment. This may be achieved by leveraging this TaaS Risk Assessment and incorporating it into the Agency's risk management framework.

Complementary Products, Changes and/or Uplift/s of the TaaS Service/s are out of scope of this Risk Assessment (refer to Technical Context Section 3 Technical Context" for in-scope services) and may require additional assessments. Specific SAs implementations, interdependencies and the use of legacy services also need to be considered.

Certification and Accreditation

The Service Security Certificate (SSC) or Service Security Audit Risk Report (SSARR) provides a summary of the security posture and residual risks after assessing the Service Provider controls. Based on the SSC or SSARR findings and Subscribing Agencies assessment of risks, Subscribing Agencies need to determine, implement and certify any additional security controls outside of the Lead Agency certification activities. Subscribing Agencies need to follow their own Certification and Accreditation process to accredit the adopted TaaS service prior to making the service available for production use.

If the risk position of the service is not appropriate based on the findings from the Service Provider audit, the Lead Agency will issue a Service Security Audit Risk Report instead of a SSC.

How to use this Risk Assessment

It is recommended that Agencies adopt this report and review the risks, ratings, and controls using their own risk management framework. This is to ensure that the information security and privacy risks are assessed correctly in their context.

Agencies (or other organisations) that do not have a risk management framework can use the GCDO's risk framework. But they must review the risks, ratings and controls, and make any changes to ensure it is applicable in their context.

9(2)(k)

[redacted]

9(2)(k)

[redacted]

9(2)(k)

[redacted]

9(2)(k)

[redacted]

9(2)(k)

[redacted]

9(2)(k)

[redacted]

9(2)(k)

[redacted]

9(2)(k)

[redacted]

9(2)(k)

[redacted]

9(2)(k)

[redacted]

9(2)(k)

[redacted]

9(2)(k)

[redacted]

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) 9(2)(k) the following key recommendations should be undertaken:

1. **Risk Management and Due Diligence**
   Before the consumption of any TaaS, agencies should be informed and aware of the implicating risks associated with using the service. This can be done by performing a suitable Risk Assessment to identify the risks and controls associated with the service. All identified risks should be understood and formally accepted with an appropriate risk management plan. The controls identified should be validated or assurance obtained from the SP, to ensure that they are operating as designed.

   The amount of due diligence should also extend out to any third parties supporting the SaaS. While it may not be possible to audit the SP directly, agencies may be able to rely on independent third-party audit reports where appropriate.

2. **Contracts and Service Level Agreements**
   Contracts and service level agreements with the SP defines the agency's requirements for the service. They should include elements such as terms of service, associated service levels, key performance indicators and metrics demonstrating service performance.

   Agencies must ensure that the SP is aware of their information security requirements by formalising contract provisions or service level agreements. In addition, monitoring of the SaaS performance should be performed on a regular basis to ensure that expectations are met. This includes any third parties that may be contracted by the SP to provide part of the SaaS.

3. **Configuration and Vulnerability Management of Underlying Infrastructure**
   Change and vulnerability management procedures should be defined and followed by the SP, to ensure that the risks associated with misconfigurations and vulnerabilities that affect the underlying infrastructure of the SaaS are mitigated. This ensures that data belonging to different SP tenants are well segregated and prevented from unauthorised access.

   A robust vulnerability management process to maintain the currency of all components of the underlying infrastructure such as servers, hypervisors and network devices, should be developed and followed. This includes regular vulnerability assessments, as well as software and firmware patching and updating. The requirements for change and vulnerability management should be included in the contracts or service level agreements with the SP.

4. **User Awareness and Training**
   Users with access to the agency's data on the cloud, including SP and CA staff, should be made aware of their requirements towards protecting the confidentiality, integrity, availability and privacy of the information processed by the service.

   Regular user awareness and training programs should be developed and made available to all users. The suggested topics to be covered include responsibilities, consequences or non-compliance with information security requirements, potential security risks and countermeasures associated with user behaviour.

5. **Incident Response and Management**
   The presence of adequate logging and regular monitoring of the SaaS helps the SP and CA detect or investigate security incidents should they occur. This includes enabling sufficient logging and monitoring on the underlying infrastructure supporting the SaaS.

   Along with sufficient logging and monitoring, a robust incident management and response plan can help the agency manage the impact should a risk occur. The incident response plan should define what constitutes an incident and outline the systematic approach that will be followed when an incident occurs.

6. **Secure Facilities**
   Effective physical controls should be implemented at the SP's facilities and physical assets to ensure that information is physically protected from unauthorised access by both malicious SP personnel and third parties.

7. **SaaS/Cloud Integration design review incorporating Information Security risk management for TaaS**
   A SaaS/Cloud integration designs and network schematics should be developed, reviewed and followed to ensure that information security for a TaaS product is not exposed or breached. This includes identifying the information security risks and controls associated with the SaaS/Cloud integration and assigning appropriate responsible party for each risk and control (e.g. the consumption cloud services like Pure Cloud, Teams, Zoom, Azure, AWS, SaaS etc. using TaaS services like CAB, SEEMail, Application Publishing, Application Consumption etc.).

8. **Cloud Security Access Brokerage and Data Leak protection**
   Human errors are frequent threat to the organisation. The likelihood of Subscribing Agency staff uploading highly classified information or uploading infectious file on the TaaS Service (which may be also integrated with cloud) can cause significant impact to CIA of an information. It is highly recommended that Subscribing Agency implement the controls like CASB and DLP to reduce this risk to an acceptable level.

9. **Separate SEEMail Risk Assessment**
   The SEEMail Risk Assessment will be updated by the Lead Agency and will be provided to TaaS Service Providers and Subscribing Agencies. Additionally, the TaaS Service Providers will also need to perform their own technical Risk Assessment for the SEEMail service.

Gross/Residual Risks TaaS Services

Tables below illustrates the gross rating for all parties, target risk rating for a Service Provider and a residual risk rating for a Subscribing Agency if recommended controls are implemented correctly and operating effectively. Tables below represent the risks for all TaaS towers.

9(2)(k)

[redacted]

Gross/Residual Risks TaaS Management Platform

The tables below illustrate the gross and residual risk ratings for a Service Provider Management Platform for a Service Provider if recommended controls are implemented correctly and operating effectively. Tables below represent the risks for all platforms used to provide TaaS towers.

9(2)(k)

[redacted]

Business Context

This section provides an overview of the business context of Telecommunications as a Service (TaaS) that is in scope of this information security Risk Assessment.

Important for Agencies

This is an All-of-Government (AoG) Risk Assessment and attempts to capture a common business context for the majority of New Zealand Government Agencies.

If this common context does not match your organisation's business context, it is recommended that you tailor it to match your business needs.

This common context aims to represent most government agencies, and support agencies who do not have an information security capability to complete the Risk Assessment process. This common context provides as a starting point for each Subscribing Agency to review and make any changes as appropriate in their own context.

A set of context surveys were submitted to several agencies and organisations, and their responses were analysed to create the following business context. For a complete list of consulted agencies see Appendix A – Consulted Agencies.

Business Owner

*Each Subscribing Agency procuring a TaaS service is ultimately accountable for the security of the information that they transmit, process, store and access in TaaS. Each Subscribing Agency needs to identify and assign a **Business Owner** accountable for ensuring that their security requirements are identified, defined, and met by the TaaS Services they adopt.*

The General Manager of All of Government Services Delivery is accountable for ensuring that AoG's security requirements for TaaS services are identified and defined:

Jane Kennedy
General Manager - All of Government Services Delivery
Digital Public Service Branch
Department of Internal Affairs.

Service Owner(s)

Each Subscribing Agency is responsible for the security of their information transmitted to, processed and stored in the TaaS services they consume. Each Subscribing Agency needs to identify and assign a Service Owner responsible for the day-to-day operation and management of the TaaS services they adopt.

All of Government Services Delivery is responsible for managing the commercial relationship and the performance of the TaaS Service Providers:

Manager Commercial and Supplier Relationships - All of Government Services Delivery
Digital Public Service Branch
Department of Internal Affairs.

Service Providers[2]

Each Subscribing Agency needs to review, identify and capture any additional Service Providers applicable to their use of TaaS.

TaaS has several Service Providers that each provide one or more services from within each tower. Each Service Provider will likely have their own third parties and supply chain of providers who are not listed.
All TaaS Service Providers will be delegated the responsibility for the day-to-day operation and delivery of the TaaS services, including the ongoing management of the security of the TaaS services. This includes managing technical security risks for the service and providing security assurance reporting to Subscribing Agencies and the GCDO.

Other Stakeholders

Each Subscribing Agency needs to review, identify and capture any additional Service Providers applicable to their use of TaaS.

Subscribing Agencies

Each Subscribing Agency consuming a TaaS service is a stakeholder as they transmit, process, store and/or access information and information services using TaaS.

Information Classification

Each Subscribing Agency needs to review, identify and confirm the maximum classification of information that they will use in the TaaS services they adopt.

TaaS Services are provided for the information classified at Classification Removed IN-CONFIDENCE and Unclassified. Based on the New Zealand Government Security Classification System[1] TaaS services need to protect information classified at Classification Removed

A compromise of the security and/or privacy of the information transmitted, processed and/or stored by the TaaS services could:

- prejudice the maintenance of law and order.
- impede the effective conduct of government in New Zealand.
- adversely affect the privacy of New Zealand citizens.
- damage the interest of New Zealand.
- endanger the safety of New Zealand citizens.
- affect national interests in an adverse manner.

Business Processes Supported

Each Subscribing Agency needs to identify and capture their business processes that will be supported with their use of TaaS.

Based on the survey results, TaaS services will be used in many ways, to support very different business processes.

[2] In this document the word "vendor" is used in the risk tables.
[1] Available from: https://protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/classification-system/

Agencies must also consider any service dependencies when consuming TaaS services. There are several services that require additional services to be consumed. For example; TaaS Contact Centre services may require Legacy Gateway services to operate on GNet.

Business Impact

Each Subscribing Agency needs to identify and capture their business impact(s) should an information security or privacy incident occur, which compromises the confidentiality, integrity, and or availability of their information or information services.

Table 8 below presents the most frequent business impact ratings from the survey respondents. The ratings represent the maximum possible business impact, should the confidentiality, privacy, integrity, or availability of their information be compromised. The business impact scale is based on the GCIO Risk Assessment Framework[3], and is measured against Agency Reputation, Health & Safety, Service Deliver and Financial.

Table 8 – Most frequent business impact ratings from previous survey respondents

	Agency Reputation	Health & Safety	Service Delivery	Financial
Confidentiality	5 - Severe	4 - Significant	3 - Moderate	3 - Moderate
Privacy	5 - Severe	4 - Significant	2 - Minor	2 – Minor
Integrity	5 - Severe	1 - Minimal	4 - Significant	3 - Moderate
Availability	5 - Severe	1 - Minimal	4 - Significant	4 - Significant

User and Devices

Each Subscribing Agency needs to identify and document the different types of Users and Devices that will have access to their information, information services, and the TaaS services they adopt.

A common set of users and devices have been identified for this Risk Assessment:

- **Service Provider Administrators** – Administrators who do not have access to information, but have the necessary access to manage the infrastructure, systems and services that support TaaS and the services within it.
- **Service Provider Service Accounts** – Non-user accounts used to authenticate services to TaaS systems.
- **Service Provider Engineer/Technician** – Technicians (most likely contractors) who do not have access to information, but have the necessary access to install, configure and service infrastructure or devices that may be located at the Agency site, third party site or other locations.
- **Agency Administrator** – Administrators who may or may not have access to information but have access to manage the Subscribing Agency's instance of TaaS and manage the settings and configuration of the services and user accounts, groups and permissions.
- **Agency User** – Standard users who have access to their agency's information services and use these services and systems to perform their role.
- **Agency Device** – Specific device accounts that are used to identify and authenticate non-user agency devices (e.g. Laptops, Servers, Mobile Devices, Teleconferencing equipment).

[3] https://snapshot.ict.govt.nz/dmsdocument/3-risk-assessment-process-information-security/html

- **Service Provider Hardware** – Hardware infrastructure or devices that may be located at the Agency site, third party site or other locations.

Security Requirements

Each Subscribing Agency needs to identify and document their own security requirements in terms of Confidentiality, Privacy, Integrity and Availability and/or any other relevant legislation.

> **Important: The All of Government Internet referred to as GNet must be treated as an untrusted network.**
>
> **It is designed to provide connectivity between any person or device, and any other peer device or information service connected to GNet. This can also include Legacy WAN networks bridged to GNet.**
>
> **This architectural decision needs to be understood when capturing their confidentiality, privacy, integrity and availability requirements and evaluating TaaS Services.**

Confidentiality and Privacy

Based on the survey respondents, the confidentiality and privacy of the information transmitted, stored and/or processed within the TaaS services is important for most Subscribing Agencies.

For most Subscribing Agencies, the TaaS services will be used to transmit, store and/or process a variety of types of information including:

- Nondescript unclassified information.
- Classified government information.
- Commercial & business-to-business information.
- Research data.
- Personal information including health data.

TaaS services must therefore ensure that information is not accessed by, or disclosed to, unauthorised parties. Unauthorised access to, or disclosure of, Subscribing Agency information will lead to a compromise of classified, Classification Removed and/or personal information. This could potentially result:

- Citizens being disadvantaged, threatened and/or endangered.
- Property being damaged or destroyed.
- Commercial and research (intellectual property) interests being damaged.
- A compromise in the safety of key assets and/or public officials.
- Diplomatic relations being adversely affected.
- Significant reputational damage to the Agency.
- Hindering the operational effectiveness or security of New Zealand.
- Adversely affecting the internal stability or economic wellbeing of New Zealand.

Additionally, unauthorised access to, or disclosure of, personal information may gain the attention of the media and Ministers, lead to legal action being taken against the Agency or investigation/monitoring by the Privacy Commissioner.

Integrity

Based on the survey respondents, the integrity of the information transmitted, stored and processed in the TaaS service is considered important for most Subscribing Agencies.

The information transmitted, processed and stored by the TaaS services must be protected against accidental or deliberate modification and/or corruption. Should information handled by TaaS services be modified or deleted, then the Agency's information services receiving this information will be impacted, with potential personal, financial or legal ramifications and incorrect decision making by Subscribing Agencies business processes with a negative effect on the operation of the Agency. Completeness and accuracy of data are often paramount.

The integrity of the information stored and processed in the TaaS services is critical, particularly for security-related event logs and audit information. Should this information be compromised then a Subscribing Agency may be unable to detect, respond to, investigate, and/or resolve an information security or privacy incident.

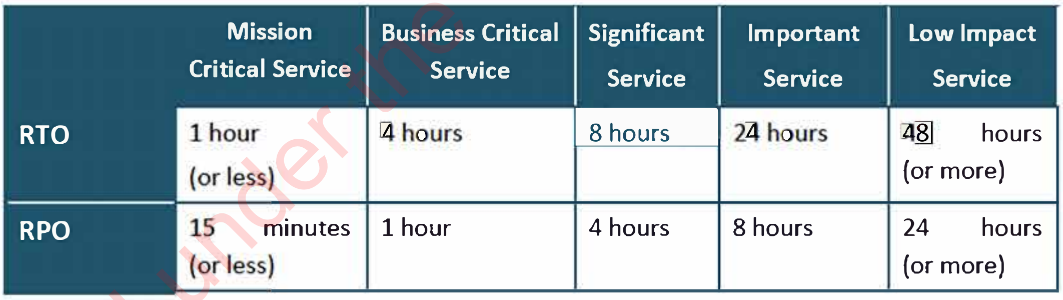
Availability

Based on the survey respondents, availability is considered an important security requirement for many components of TaaS. Subscribing Agencies generally have a clear understanding of their availability requirements, with most business services requiring 24/7 availability - especially those Business services relating to emergency and health support.

The TaaS services will used to provide users and devices access to an Agency's information services during and outside of business hours and provide access from on-premise and off-premise locations. A compromise of these services will significantly interrupt the operation of the processes and the functions of each Subscribing Agency.

Based on the survey respondents, the most frequent Recovery Time Objective (RTO) was one (1) hour or less, with a Recovery Point Objective (RPO) of four (4) hours.

Table 9 – Previous Survey RTO and RPO Scale



	Mission Critical Service	Business Critical Service	Significant Service	Important Service	Low Impact Service
RTO	1 hour (or less)	4 hours	8 hours	24 hours	48 hours (or more)
RPO	15 minutes (or less)	1 hour	4 hours	8 hours	24 hours (or more)

Legislation, Policy and Guidelines

Based on the survey results, there are a significant number of security-related legislation, policies and standards that Subscribing Agencies may need to demonstrate compliance with when consuming TaaS services. Government Agencies must ensure that they can demonstrate compliance with applicable legislation, policies, guidelines and any other external requirements when using TaaS Risk Assessment.

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 1993.
- Public Records Act 2005.
- Protective Security Requirements (PSR).

- New Zealand Information Security Manual (NZISM v 3.4).

9(2)(k)

[redacted]

9(2)(k)

[redacted]

9(2)(k)

[redacted]

Detailed Findings – Common Risks

Error! Reference source not found. below presents the Common Risks (CR) associated with the use of TaaS (Any product under any tower). The risk IDs mentioned in the bracket and in bold letters are from earlier TaaS Risk Assessment Report version 2 .3. The controls that are underlined and in bold letters are key controls.

Table 10 – Common Risks[4]

Risk ID	Risk Description	9(2)(k) [redacted]
CR01	**Malicious Parties (R01, R05, R06 & R33)** 9(2)(k) [redacted]	[redacted]

[4] All new risk should be added the end of any table in this document to preserve the autonumbering and version alignment.

Risk ID	Risk Description	9(2)(k) [redacted]
CR02	**Technical Attacks (R02, R03, R04 & R36)** 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
CR03	**Malware Infections (R07& R51)** 9(2)(k) [redacted]	

[5] Sufficient LAN/WiFi, network segmentation controls are in place to avoid the propagation of virus/malware

Risk ID	Risk Description	9(2)(k
CR04	**Service Management (R08, R09, R10, R13, R14, R15 & R16)** 9(2)(k) [redacted]	[redacted]
CR05	**Human Error (R17, R18, R49, R50 & R55)** 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	[redacted]
CR06	**Insider Threat (R19 & R20)** 9(2)(k) [redacted]	[redacted]

[6] On top of standard change management, Subscribing Agency to ensure this control is also applied to the changes related to business rules or processes, that are applied on the ICT systems. (e.g. contact centre business process change that needs configuration change on the application)

[7] Controlled system configuration changes that are driven by business processes changes.

Risk ID	Risk Description	9(2)(k [redacted]
	9(2)(k) [redacted]	
CR07	**Incident Management (R21, R22 & R23)**	
	9(2)(k) [redacted]	

9(2)(k)

[redacted]

Risk ID	Risk Description
	9(2)(k) [redacted]
CR08	**Information and Service Assurance (R24, R25, R26 & R27)** 9(2)(k) [redacted]

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	
CR09	**Service Resiliency (R11, R28 & R29)** 9(2)(k) [redacted]	

[8] Physical and Environmental Security for agency managed site, kit, cabinets (e.g. switch cabinet at agency site, SP's Access Point at agency site etc.)

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	
CR10	Governance and Assurance (R30 & R31)	
	9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	
CR11	Jurisdictional / Cloud Adoption Risk (New Risk) 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	[redacted]

Risk ID	Risk Description	9(2)(k)
CR12	**Information Disclosure, Modification or Loss due to Inappropriate Use of IMS** 9(2)(k) [redacted]	[redacted]

Detailed Findings – Connectivity Services

Table 11 below presents the Connectivity Services Risks (CS-R) associated with the use of TaaS (Any product under connectivity tower). The risk IDs mentioned in the bracket and in bold letters are from earlier TaaS Risk Assessment Report version 2.3. The controls that are underlined and in bold letters are key controls.

Table 11 – Connectivity Services Risks

Risk ID	Risk Description	9(2)(k) [redacted]
CS-R01	**Human Error (R32)** 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
CS-R02	**Unmanaged Endpoint (R34 & R38)** 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
CS-R03	**Connectivity Failure (R35)** 9(2)(k) [redacted]	
CS-R04	**Shared GNet Services (R37)** 9(2)(k) [redacted]	

[9] Host protection on agency managed devices/endpoints (e.g. desktop, laptop, phone, tablet etc.) to detect and act on any information breaches.

Risk ID	Risk Description	92)(k)
	9(2)(k)	
CS-R05	**Private / GNet Network Design** 9(2)(k	

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	

Detailed Findings – Unified Communication Services

Error! Reference source not found.below presents the Unified Communications Services Risks (UC-R) associated with the use of TaaS (Any product under UC tower). The risk IDs mentioned in the bracket and in bold letters are from earlier TaaS Risk A ssessment Report version 2.3. The controls that are underlined and in bold letters are key controls.

Table 12 – Unified Communications Services Risks

Risk ID	Risk Description	9(2)(k [redacted]
UC-R01	**Data Transfer using UC Client (R40)** 9(2)(k) [redacted]	[redacted]
UC-R02	**Shared collaboration tools (R41)** 9(2)(k) [redacted]	[redacted]

[10] In addition to standard access and authentication controls, the controls related to federation with other agency is the most important control to implement. Subscribing agency should also implement the content sharing controls/policies available within their UC subscription (e.g. Configuring Microsoft Teams with three tiers of protection using information classification).

Risk ID	Risk Description	9(2)(k [redacted]
	9(2)(k) [redacted]	
UC-R03	**Malware Infections (R43)** 9(2)(k) [redacted]	

9(2)(k)

[redacted]

Risk ID	Risk Description
	9(2)(k) [redacted]

Risk ID	Risk Description	9(2)(k [redacted]
UC-R04	**Malicious Party (R44)** 9(2)(k) [redacted]	
UC-R05	**Agency Site Physical Security Breach (R45)** 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	
UC-R06	Technical Attacks (R46, R47)	
	9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	[redacted]

Detailed Findings – Contact Centre Services

Table 13 below presents the Contact Centre Services Risks (CC-R) associated with the use of TaaS (Any product under Contact Centre tower). The risk IDs mentioned in the bracket and in bold letters are from earlier TaaS Risk Assessment Report version 2.3. The controls that are underlined and in bold letters are key controls.

Table 13 – Contact Centre Services Risks

Risk ID	Risk Description	9(2)(k [redacted]
CC-R01	**Customer Message Integrity (R48)** 9(2)(k) [redacted]	[redacted]
CC-R02	**Incorrect PCI Process or NC (R52)** 9(2)(k) [redacted]	[redacted]

Risk ID	Risk Description
	9(2)(k) [redacted]
CC-R03	**Breach of Privacy/Legal requirements (R53)** 9(2)(k) [redacted]

9(2)(k) [redacted]

Risk ID	Risk Description	9(2)(k [redacted]
	9(2)(k) [redacted]	
CC-R04	Payment Phishing	
	9(2)(k) [redacted]	

Detailed Findings – Managed Security Services

Table 14 below presents the Managed Security Services Risks (MS-R) associated with the use of TaaS (Any product under Managed Security Services tower). The risk IDs mentioned in the bracket and in bold letters are from earlier TaaS Risk Assessment Report version 2.3. The controls that are underlined and in bold letters are key controls.

Table 14 – Managed Security Services Risks

Risk ID	Risk Description	9(2)(k) [redacted]
MS-R01	**False Positives (R56)** 9(2)(k) [redacted]	
MS-R02	**False Negatives (R57)** 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	
MS-R03	Unmanaged digital Keys (R58) 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	[redacted]
MS-R04	**Compromised PKI (R59 & R60)** 9(2)(k) [redacted]	[redacted]

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	
MS-R05	**Poor performance and/or Availability of Identity Brokerage & CASB (R61 & R67)** 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
MS-R06	**Compromised Identity Brokerage (R62 & R63)** 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
MS-R07	**SIEM Integration Errors (R64)** 9(2)(k) [redacted]	[redacted]
MS-R08	**Lost Stolen Agency Device (R65)** 9(2)(k) [redacted]	[redacted]

9(2)(k)

Risk ID	Risk Description	[redacted]
	9(2)(k) [redacted]	
MS-R09	**Information Interception (R66, R68)** 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	
MS-R10	**Single Point of Failure (R69)** 9(2)(k) [redacted]	
MS-R11	**Lack of Security Architecture and Risk Management (R70)** 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k)
	9(2)(k)	

Detailed Findings – Aggregation Services

Table 15 below presents the Aggregation Services Risks (AS-R) associated with the use of TaaS (Any product under Aggregation Services tower). The risk IDs mentioned in the bracket and in bold letters are from earlier TaaS Risk Assessment Report version 2.3. The controls that are underlined and in bold letters are key controls.

Table 15 – Aggregation Services Risks

Risk ID	Risk Description	9(2)(k) [redacted]
AS-R01	**Poor Change Management (R71)** 9(2)(k) [redacted]	[redacted]

Risk ID	Risk Description	9(2)(k)
	9(2)(k)	
AS-R02	**Poor Incident Management (R72 & R73)** 9(2)(k)	

Risk ID	Risk Description	9(2)(k [redacted]
	9(2)(k) [redacted]	[redacted]
AS-R03	**Poor Asset Management (R74)** 9(2)(k) [redacted]	[redacted]

Risk ID	Risk Description	9(2)(k [redacted]
	9(2)(k) [redacted]	
AS-R04	**Agency information is modified or disclosed (New Risk)** 9(2)(k) [redacted]	

Detailed Risks – Management Platform

Table 16 below presents the risks associated with a TaaS Platform provided by Service Providers for hosting TaaS Services.

Table 16 – TaaS Platform Risk Assessment

Risk ID	Risk Description	9(2)(k [redacted]
MP-R01	**Malicious Parties** 9(2)(k) [redacted]	[redacted]
MP-R02	**Technical Attacks** 9(2)(k [redacted]	[redacted]

Risk ID	Risk Description	9(2)(k [redacted]
	9(2)(k) [redacted]	
MP-R03	**Malware Infections** 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	[redacted]
MP-R04	**Service Management** 9(2)(k) [redacted]	[redacted]

Risk ID	Risk Description	9(2)(k) [redacted]
MP-R05	9(2)(k) [redacted]	[redacted]
MP-R06	Insider Threat 9(2)(k) [redacted]	[redacted]

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	
MP-R07	**Incident Management** 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k [redacted]
MP-R08	Information and Service Assurance 9(2)(k) [redacted]	[redacted]
MP-R09	Service Resiliency 9(2)(k) [redacted]	[redacted]

Risk ID	Risk Description	9(2)(k [redacted]
	9(2)(k) [redacted]	
MP-R010	Governance and Assurance 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
	9(2)(k) [redacted]	[redacted]

Risk ID	Risk Description	9(2)(k) [redacted]
MP-R011	Jurisdictional / Cloud Adoption Risk 9(2)(k) [redacted]	

Risk ID	Risk Description	9(2)(k) [redacted]
MP-R012	**Incident Management** 9(2)(k) [redacted]	[redacted]
MP-R013	**Supply Chain Introduces Undetected Vulnerabilities** 9(2)(k) [redacted]	[redacted]

Risk ID	Risk Description
	9(2)(k) [redacted]

9(2)(k) [redacted]

Controls Catalogue

Table 17 below presents the recommended controls to effectively manage TaaS risks. **Error! Reference source not found.**

Table 17 – Recommended Controls

Control Number	Control Title	Description	Reduces	NZISM Reference (V3.4, Dec 2020)
C01.	Information Security Governance	• Information Security Policies form part of an information security framework that establishes the baseline set of policies, standards and guidelines that are required for the organisation to effectively manage its security risks, in line with its business requirements. The framework is designed to be flexible and extensible to: o Enable development of new policy artefacts whilst minimising the need to revise or redevelop the security policy. o Establish a structured, consistent and robust approach to the development, implementation and review of the policy artefacts. o Ensure that staff are provided with access to information that is relevant to their roles. • Establishing an information security management framework to implement, manage, control and regulate the organisation's security activities and initiatives will help protect information to enable the organisation to achieve its business objectives. This should include, but is not limited to, the following: o Information security roles and responsibilities are defined and allocated. o How information security fits into the organisation's IT governance and enterprise risk management structure. o How the security objectives should align with the organisation's business objectives. o How security requirements are incorporated with the business requirements. o Legal, regulatory and contractual obligations and other compliance demands and requirements. • Ensuring project management methods incorporate information security and ensure they are addressed as part of the project.	Likelihood, Impact	GOV1 GOV2 GOV3 GOV4 GOV5 GOV8 GOV9 GOV10 INFOSEC1 INFOSEC2 INFOSEC3 PERSEC1 PHYSEC2 PHYSEC4 3 5.1 5.2
C02.	Segregation 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
C03.	Human Resource Security	• Ensure that all employees and contractors understand their responsibilities and are suitable for the roles, which they are employed, including: o Security vetting all new staff before beginning employment and on a regular basis thereafter. o Undertaking an induction process that covers their responsibilities for information security. o Acknowledging the Code of Conduct and information security policy o Acknowledging the employee's Terms and Conditions of Employment o Receiving regular security awareness training. o Monitoring and management of changes in employee circumstances and behaviour. o Removing access rights when their employment or contract ceases. • Ensure that organisation and third-party staff that are users or administrators receive formal training on how to perform the tasks that are relevant to their role before they are granted access to the information services. • 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. • Ensure that all employees and contractors are provided with ongoing security / privacy awareness training. Topics such as information security responsibilities, legislation and regulation, consequences of non-compliance with information security policies and procedures and potential security risks and counter measures should be covered. • Subscribing Agencies should ensure that all users of their systems are provided with, and acknowledge, the Terms of Use. These should outline the acceptable use of the service. These terms of use can either be in the form of a banner produced when the user logs on, or a hard copy document provided to a staff member.	Likelihood	3.5 9.1 9.2 9.4 19.1.18

Control Number	Control Title	Description	Reduces	NZISM Reference (V3.4, Dec 2020)
C04.	Asset & Information Lifecycle Management	• A defined and implemented Asset Lifecycle Management process will ensure that all software and hardware components are upgraded or replaced in a timely manner, when the cessation of support is announced, extended support options would incur excessive costs, or the vendor no longer intends to support the product. • This may incorporate an inventory of assets and cover ownership, reissue, return, recycling, decommissioning and destruction of organisation-owned hardware, software, mobile devices and any other removable media. • Ensure that IT systems and Agency information 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. • Manage and protect information as an asset, in any format, throughout its lifecycle through the implementation of Information Lifecycle Management policies and procedures. • Include procedures for the labelling, categorisation and/or classification of information, as well as identifying, implementing and maintaining controls to effectively protect information during the various stages of its existence, including: o Creation and receipt. o Use. o Distribution. o Maintenance. o Storage and archive. o Disposal. • 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. • Classifying information in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification will ensure it is handled and protected correctly, and advise employees on the correct procedures for creation, duplication, destruction and disposal. The Protective Security Requirements provide clear instruction on how to classify official information, as well as how it should be subsequently handled. • Ensure that import, export, copying of information are hygiene checked, protected in transit and at rest (securely transfer) from one system to another for the purpose of testing, migration transition or archival with their appropriate classification.	Likelihood	1.1.11 12.3 12.4.7 12.6 13.1 13.2 13.3 13.4 13.5 13.6 20.2 20.3 22.1.26
C05.	Documentation	Ensure that information security documentation is produced for systems, to support and demonstrate good governance. The following documents should be documented: • Sufficient design and technical documentation supports the rebuilding of information services and systems. • Security Risk Management Plans – identifying security risks and appropriate treatment measures for systems. • System Security Plans – specifying the information security measures for systems. • Standard Operating Procedures – ensuring security procedures are followed in an appropriate and repeatable manner. • Emergency Procedures – ensuring classified information and systems are secured before personnel evacuate a facility in the event of an emergency.	Likelihood, Impact	5.1 5.2 5.3 5.4 5.5 5.6 5.7

Control Number	Control Title	Description	Reduces	NZISM Reference (V3.4, Dec 2020)
C06.	Access, Authentication & Authorisation	• 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. • Ensure that users are only provided with access to the service that have been specifically authorised to use, including: o 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. o 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. • 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. • Ensure that user accounts are managed through their lifecycle process, including: o Assigning access rights aligned with the defined access control policy. o Reviewing access rights on a regular basis. o Disable accounts when a user leaves an organisation. o Disable accounts when a user no longer requires access. o Remove or update access rights (e.g. when a user changes role within an organisation). • 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. • Ensure that user passwords should be protected against unauthorised access when distributed initially. Distribution methods may include: o Encrypted email. o A secure password reset mechanism that positively authenticates the user (such as a challenge question or multifactor authentication). o A text message to a verified mobile number. o A telephone call. • 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 [redacted] 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. • User and Device Access Management ensures information, services and systems are only accessed by users and devices who are explicitly authorised. Access management reduces the likelihood of unauthorised access to information, services and systems through formalised and controlled procedures including: o The registering of users and devices (so that they are uniquely identifiable, accountable for their actions, and be assigned access rights). o Provisioning of access rights for users and devices, in line with the access control policy. o Restricting and controlling of privileged access rights, in line with the access control policy. o Securely allocating user and device credential information (e.g. unique identifiers, secret authentication information). o Reviewing user and device access rights on a regular basis. o Removing or adjusting access rights of users and devices (e.g. change of a user's role or responsibilities). o De-registering or removing access rights of users and devices (e.g. upon termination or a change of their responsibilities or relationship). • Ensure that any services that provide identity federation functionality is securely configured. These services need to ensure that any client accessing a service is properly authenticated, and authorised, and that appropriate trust is established between two different organisations. • Web-standards based protocols should be used for exchanging authentication and authorisation data between organisations (e.g. SAML 2.0, OAuth 2.0, OpenID).	Likelihood, Impact	5.5.5 9.2.6 9.2.7 16.1 16.2 16.3 16.4 16.5 18.1.14 19.1 22.1 22.2.16
C07.	Multi-Factor Authentication	• Secure 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. • 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: o Something you know (e.g. username and password). o Something you have (e.g. hardware or software token, digital certificate). o Something you are (e.g. biometric fingerprint). • The identity and authentication information of users and devices need to be kept confidential, ensuring that it is not disclosed to other parties and securely stored (e.g. locked in a safe, password vault).	Likelihood, Impact	16.7

Control Number	Control Title	Description	Reduces	NZISM Reference (V3.4, Dec 2020)
C08.	Cryptographic Policy & Encryption	• 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. • Ensuring business [redacted] 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. • Ensuring business [redacted] private, or otherwise classified information stored on media is encrypted using approved encryption algorithms and protocols, reduces the likelihood of unauthorised disclosure.	Likelihood, Impact	16.1.35 16.1.36 17.1 17.2 17.3 17.4
C09.	Physical & Environmental Security	• Ensure that all critical facilities such as data centres, communication rooms, servers, networks, telecommunication equipment and other important assets are physically protected against accident, natural disaster, attacks and unauthorised physical access. • Ensure that equipment or assets supporting the service are protected against loss, damage, theft and unauthorised access. The considerations for equipment security includes: o Ensuring IT equipment always reside in an appropriate class of secure room. o Storing IT equipment during non-operational hours in an appropriate class of security container or lockable commercial cabinet. o 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. o Using IT equipment without non-volatile media as well as securing its volatile media. o Using an encryption product to reduce the physical storage requirements of the non-volatile media as well as securing its volatile media. • 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	8.1 8.2 8.3 8.4 9.4 10 11.7.32
C10.	System & Service 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: o An upgrade to, or introduction of, IT equipment. o An upgrade to, or introduction of, software. o Environment or infrastructure change. o Major changes to access controls. • 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: o All changes must be tested in a non-operational environment before being transferred into the operational environment. o Testing must not be done in operational environments. o Rules for the transfer or installation of software into operational environments from non-operational environments. o Users must have different accounts for operational and non-operational environments. o 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. • 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. • Provide a Service Roadmap plan that outlines short and long-term service upgrades and updates. This ensures that service users and integrating vendors are aware of planned improvements and/or changes to the service. This facilitates the adoption of updated service features and provides an opportunity to address any integration issues before a service upgrade or update occurs.	Likelihood, Impact	12.7.19 14.1 14.4

Control Number	Control Title	Description	Reduces	NZISM Reference (V3.4, Dec 2020)
C11.	Host Protection	• The installation of malware protection software on all applicable systems, 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. • 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. • 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. • Access to Web content is implemented in a secure and accountable manner via web Proxy for and content filtering. • Only approved applications are used on agency-controlled systems via application white listing. • Endpoint/hosts are regularly monitored and maintained for the up-to-date Patches and regular vulnerability scans. • Use of Data loss protection clients on the endpoint where appropriate. • Mobile telephone systems and devices are prevented from communicating unauthorised classified information via MDM. • Wearable devices are prevented from unauthorised communication or from compromising secure areas. • Devices and systems are protected from unauthorised external media connectivity and usage. • Strong identity access and authentication methods are enforced on the endpoints/hosts via centrally managed directory service. • The development of a Mobile Device Policy will ensure those staff members that are provided with a mobile device (or those who utilise BYOD) for the organisation's purpose, are provided with clear direction on correct use of the device and reminded of the need to comply with the policy. It will ensure that appropriate precautions are taken to protect against theft, damage and accidental disclosure of information.	Likelihood, Impact	7.1 7.3 9.3 11.4 11.5 12.1 13.3.6 14.1 14.2 14.3 16 20.1 21 GOV04
C12.	Backup & Restore	• 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 back up as well as regular restoration tests to confirm its effectiveness. An offline encrypted copy of all back-up 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.	Impact	6.4 13.3 16.3 16.5 17.1 22.1.26 22.2
C13.	Logging & Incident Monitoring (SIEM)	• Ensure that information systems are configured with adequate logging, archived and retained for a defined appropriate period. Events to be logged includes: ○ 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). ○ IT equipment location/identification. • Ensure that security related event logs are analysed regularly using automated security information and event management (SIEM) tools or equivalent to help identify anomalies. • Clock/Time synchronisation across all connecting services will ensure a definitive time source is used, which will aid any information security investigation.	Likelihood, Impact	3.4 4.4 7.1 7.3 12.4 14.1 14.2 14.3 15.2 16.5 16.6.11 18.1.19 19.2 20 22.2
C14.	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. • Automate and orchestrate operational tasks and processes to increase the speed and accuracy of the deployment and maintenance of information services. Examples of Automation and Orchestration include: ○ Automated tasks (scripts, workflows, processes). ○ Orchestrated deployments (deployment scripts, build images, application packages.	Likelihood, Impact	5.5 12.2 14.1 18.1 22.2.14

Control Number	Control Title	Description	Reduces	NZISM Reference (V3.4, Dec 2020)
C15.	Patch & Vulnerability Management	• Ensure a patch management strategy is defined and implemented that involves vulnerability identification and proactive management through regular application of security patches and updates. • Ensure that security patches are applied in a timely fashion to manage software and firmware corrections, vulnerabilities and performance risks. • Technical vulnerabilities of information services and systems are continuously monitored. • Technical vulnerabilities are assessed, prioritised and applied accordingly. Severity 1 patches are applied as soon as they are available.	Likelihood	12.4
C16.	Network Security	• 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: o Using structured Internet and network addressing and naming schemas (e.g. IPv4/6, DNS). o Identifying and creating network trust domains based on business security requirements (e.g. Guest networks, user networks, etc.). o Limiting access to network services and security domains (e.g. Management zones). o Protecting network records using secure protocols and cryptographic technologies (e.g. DNSSEC, secure routing). • 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: o Network-Based Intrusion Prevention System (NIPS): monitors the entire network for suspicious traffic by analysing protocol activity. o Wireless Intrusion Prevention Systems (WIPS): monitor a wireless network for suspicious traffic by analysing wireless networking protocols. o 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. • 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. Separation and Segregation principles are also applied to SDNs. • Firewalls are deployed to monitor and control connections and information flows between security domains. For [redacted] 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. • Clock/Time synchronisation across all connecting services will ensure a definitive time source is used, which will aid any information security investigation. • The application of defence-in-depth to the protection of systems and infrastructure is enhanced using successive layers of security controls. All layers are designed to control and limit access to those with the appropriate authorisation for the site, infrastructure and system. • Additionally, the use of different brands or technologies to achieve the same control objective (e.g. use different firewall vendors for internet and backend firewalls), reduces the possibility of an attacker circumventing all controls by circumventing one vendor or type of technology.	Likelihood, Impact	7.1.7 10.8 14.1 14.4 14.5 16.6.11 18.1 18.3 18.4 19.1 19.3 22.3
C17.	DoS Protection	• Implement a solution to detect and prevent Denial of Service (DoS) and distributed denial of service (DDoS) attacks. These solutions need to work in conjunction with upstream network providers to be truly effective. • Services must be designed to protect against non-technical Denial of Service attacks that target business processes (e.g. submitting a large amount of false contact requests).		
C18.	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	20.1 22.1 22.2 22.3
C19.	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 out-bound), 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
C20.	Message Integrity	• Message Integrity is used to provide recipients with a method of authenticating the source of a message, the ability to verify the integrity of a message and non-repudiation by the sender or recipient (i.e., the sender cannot claim that they did not send the message, or, the sender can gain assurance that the recipient has received the message). • Message Integrity can be implemented as formal transfer policies, procedures and/or technical controls to ensure the integrity of information when being transferred. • Email messages have appropriate protective markings to facilitate the application of handling instructions.	Likelihood, Impact	15 17.6.7 17.7

Control Number	Control Title	Description	Reduces	NZISM Reference (V3.4, Dec 2020)
C21.	Due Diligence	• Ensure that contracts and associated Service Level Agreements (SLAs): o Clearly define the legal jurisdiction for contractual disputes relating to the use and function of the service. o Clearly define the ownership of the data stored, processed and/or transmitted by the service. o Define in which jurisdiction official information can and will be stored, processed and/or transmitted by the service. o 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. o Ensure that the time to return to full service after a failure or outage, including data restoration, meets the organisation's business continuity requirements. o Require that all access to the organisation's information and systems be monitored. o Require and specify means to notify to the organisation of any actual or possible unauthorised access. o Require engagement with the organisation in resolution of any information access incidents or issues. o Require regular reports be delivered from SP on their performance against the SLA's. o 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. o 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. o Ensure the contract with SP outlines clearly the services in scope and that the organisation are alerted when requiring services that are not within the scope • Ensure that adequate due diligence is undertaken across the service, specifically: o Defining the information security requirements of the service. o Assessing whether the defined information security requirements are met by the service. o Identifying and assessing any third-party dependencies that the service provider may have. • 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. • An exit strategy outlines the processes for leaving a current situation, either after a predetermined objective has been achieved or as a strategy to mitigate failure. At worst, an exit strategy will save face. At best, an exit strategy will peg a withdrawal to the achievement of an objective worth more than the cost of continued involvement. Exit strategies typically include the means to extract the organisation's settings, configurations and information from the Service Provider in a format that can be used by the organisation, to stand up the Service or use the information in a different setup.	Likelihood, Impact	2.2 2.3.16 2.3.23 3.2 3.3 4.4.8 22.1
C22.	ICT Supply Chain & Vendor Management	• Being aware of any reliance the Service Provider has on any third party, will allow the organisation to ensure these are identified and addressed in the contracts between them and the Service Provider. This ensures that the Service Provider can provide assurance and be held accountable that these third parties meet the organisation's security requirements. • To support contractual agreements, the implementation of a communication channel in the form of Vendor Management will allow the organisation to monitor the Service Provider's performance against the contract and SLAs..	Likelihood	12.7
C23.	Information Security Incident Management	• Ensure than an incident response plan is develop and defines what constitutes an incident, and to outline the systematic process that is to be followed should an incident occur. A 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: o Detecting security incidents to minimise impacts. o Reporting security incidents, assisting in documenting and understanding the risks and impacts. o Managing security incidents by identifying and implementing processes for incident analysis and selection of appropriate remediation. • Manage and respond to service management events that falls under the definition of an Information Technology Infrastructure Library (ITIL) incident, Specifically, any unplanned interruptions or reductions in quality of IT services. Having an effective ITIL Incident Management process ensures IT services are restored in a timely manner to minimise impact to the business and should be appropriately integrated with an Information Security Incident Management process to effectively respond to and manage security-related events.	Impact	5.1.11 5.1.12 5.6 7 22.1.25
C24.	Business Continuity	• 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. • Information Security Continuity is an integral component of disaster recovery and business continuity plans. Establishing, documenting, implementing and maintaining processes, procedures and controls ensures the required level of information security is achieved. This includes adequate management structure with the necessary authority and incident response teams to act in case of disasters, as well as all the necessary controls required. As with all information security documentation, these processes need to be periodically verified, reviewed, tested and evaluated to make sure it meets the outlined requirements.	Impact	6.4

Control Number	Control Title	Description	Reduces	NZISM Reference (V3.4, Dec 2020)
C25.	Disaster Recovery _& Fault Tolerance	- Ensure that disaster recovery processes 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. - 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: o Clustering. o Load balancing. o Network redundancy. o System redundancy.	Impact	6.4
C26.	Information Security Review & Audit	- 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. - Ensure information security reviews are conducted to maintain the security of systems and detect gaps and deficiencies, including: o Identifying any changes to the business requirements or concept of operation for the subject of the review. o Identifying and changes to the security risks faced by the subject of the review. o Assessing the effectiveness of the existing counter-measures. o Validating the implementation of controls and counter-measures. o Reporting on any changes necessary to maintain an effective security posture. - 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. - 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: o Security posture of the organisation has been incorporate into its system security design. o Controls are correctly implemented and are performing as intended. o Changes and modifications are reviewed for any impact or implications. o Effectiveness of information security measures for systems is periodically reviewed and validated. o 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, Impact	4.1 4.2 4.3 4.4 4.5 6.1 6.2 10.8 14.2 14.4 14.5 16.5 18.1 19.1 19.3 21.4 22.1.21 22.2.13
C27.	Cardholder Data Policy	- Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes. This policy should include at least the following: o Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements; o Processes for secure sanitisation and deletion of data when no longer needed; and o Specify and document information retention requirements for cardholder data. o A process for identifying and securely deleting stored cardholder data that exceeds defined retention.	Likelihood	**13.1.12** - Archiving ***PCI DSS v3.1 - Requirement 3.1: Protect stored cardholder data***
C28.	Database Security	Ensure classified database content is protected from personnel without a need-to-know. System user access to the database is [redacted] and logged for: o Attempted access that is denied. o Changes to system user roles or database rights. o Addition of new system users, especially privileged users. o Modifications to the data. o Modifications to the format or structure of the database.	Likelihood, Impact	16.6.10 17.7.30.C.01 20.4

Control Number	Control Title	Description	Reduces	NZISM Reference (V3.4, Dec 2020)
C29.	Communications Security	• Video & Telephony Conferencing (VTC), Internet Protocol Telephony (IPT) and Voice over Internet Protocol (VoIP) systems are implemented in a secure manner that does not compromise security, information or systems and that they operate securely. • Ensure the use of Session Border Controllers (SBCs) is integrated with the agency's security architecture and that use is consistent with other requirements for gateway security especially for the products like unified communications and contact centre. Ensure that communication media (Voice/Video/Chat) are protected by the gateways (SBCs) to: o Encrypt the media in transit/rest to maintain the confidentiality and integrity of an information while maintaining quality and performance of a service. o Ensure that service is protected from external attacks and threats to maintain confidentiality, integrity and availability. o Ensure strong client access mechanisms to securely communicate via devices (Desk phones, soft clients on the mobile, desktop, laptop, tablets). o Secure the connectivity between PSTN and IP telephony. o Use video and voice aware firewall mechanisms to allow [redacted] traffic. • Ensure the communications (Voice/Video over IP, instant messages) are protected from common risk and threats such as: o Reconnaissance scan. o Man in the middle attacks. o Eavesdropping. o Session hijack. o Session overload. o Protocol fuzzing. o Media injection. o Toll Fraud.	Likelihood, Impact	11 18.3 19.5
C30.	Information Spill Protection	• Depending on the SaaS 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 [redacted] 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. • 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.	Likelihood, Impact	14.1.13.C.03 21.4.5 21.1.24
C31.	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	10.1 22.1
C32.	Management of Privileged Access	• Controlling the allocation, maintenance and removal of privileged access rights will ensure that the use of administrative privileges is [redacted] to only those activities that require them, and not for business as usual or day-to-day activities. Privileged access rights are controlled through formal authorisation processes and implemented in accordance with an access control policy.	Likelihood	PERSEC1 16.3 22.1

Control to Risk Mapping

Service Provider

Table 18 below details a mapping between the Service Provider controls and their associated risks.

Table 18 – Service Provider Controls to Risk Mapping

9(2)(k)

[redacted]

9(2)(k)

[redacted]

9(2)(k)

[redacted]

Subscribing Agency

Table 19 below details a mapping between the Subscribing Agency controls and their associated risks. Controls listed below must be reviewed by Subscribing agency for its effectiveness and determine the risk position based on their risk appetite for the use of TaaS services.

Table 19 – Subscribing Agency Controls to Risk Mapping

9(2)(k)

[redacted]

9(2)(k)

[redacted]

Appendix A – Consulted Agencies

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

Table 20 – Consulted Agencies

No.		Attendee	Role	Agency Name
1		Matthew Rounthwaite	Chief Information Security Officer	Accident Compensation Corporation
2		Simon Hide	Enterprise Architect	Ministry of Justice
3		Christian Hogg	Chief Information Security Officer	Inland Revenue
4		Jan Serfontein	Chief Architect	Kainga Ora – Homes and Communities

Appendix B – Project Overview

Scope

The Department of Internal Affairs (DIA), as Lead Agency for Telecom-as-a-Service (TaaS) have written this Risk Assessment Report for service providers and Subscribing Agencies, for the use of TaaS.

The objective was to create a Risk Assessment that is comprehensive and yet cost-effective for TaaS Subscribing Agencies. The assessment can then be used to frame and provide a basis for future Risk Assessments and control audits of TaaS.

This TaaS Risk Assessment focused on consolidating common risks and Tower specific risks for Subscribing Agencies consuming TaaS products approved under ICT common services.

TaaS is an AoG initiative that enables New Zealand businesses to offer their products and services directly to New Zealand government agencies. TaaS links business with government, making the procurement process easier for all. For more details please visit https://www.digital.govt.nz/products-and-services/products-and-services-a-z/taas/

TaaS has a list of approved products and suppliers that are offering services in Communications (including Unified Communications) Connectivity, Contact Centre, Managed Security Services and Aggregation Services tower for enterprise grade products. Suppliers of TaaS are required to perform formal security assurance with Lead Agency.

Minimum requirement for the scope of this Risk Assessment is depending on:

- Risk profile of the service.
- Use / delivery of TaaS products to deliver Managed Services.
- Reliance on Agency controls, particularly for people and process controls.
- Claims made by the Supplier in the service description.

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 TaaS services.
- Development of a Risk Assessment report in draft.
- Issuance of a final Risk Assessment report.

Documents Referenced

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

- TaaS Risk Assessment Report V2.3
- TaaS Control Objectives V2_0 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 21 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 21 – 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

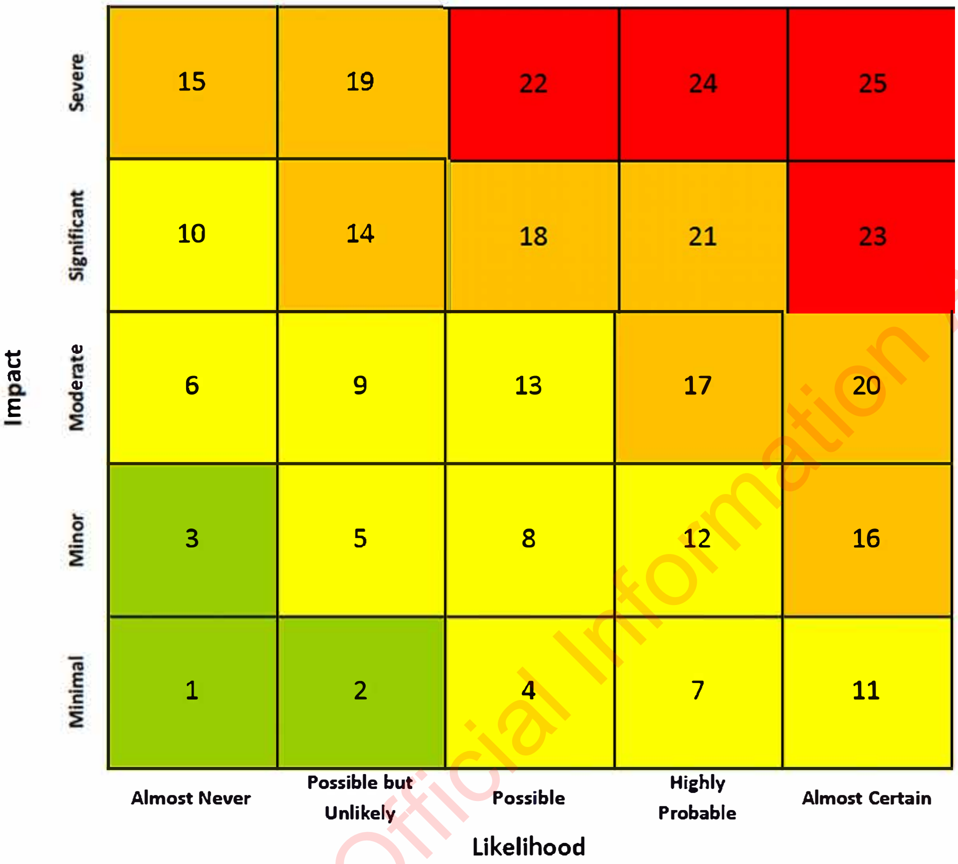
The qualitative scale used to assign an impact rating is presented in Table 22**Error! Reference source not found.**. All impacts were analysed in a business context. The impact of risks includes a consideration of any possible knock-on effects of the consequences of the identified risks, including cascade and cumulative effects.

Table 22 – 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**	• 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 Te Kawa Mataaho Public Service Commission (TKM/PSC), GCIO or OPC. • The TKM/PSC and GCIO manage the communications and recovery.	• 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.	• 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	• 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**	• 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 TKM/PSC and GCIO.	• 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.	• 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.	• 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**	• 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.	• 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.	• 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.	• 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**	• 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.	• 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.	• 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.	• 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**	• Reputation is not affected. • No questions from the Minister. • No media attention. • All communications and recovery can be managed internally.	• No loss or significant threat to health or life. • The agency's safety practices are questioned but are found to be appropriate.	• 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.	• 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 23 below 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.

Table 23 – Risk Matrix



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 24 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 24 – 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