Ministry for Pacific Peoples
Te Manatū mō ngā Iwi ō te Moana-nui-ā-Kiwa

14 November 2025

s9(2)(a)

Mālō e lelei s9(2)(a)

RESPONSE TO AN OFFICIAL INFORMATION ACT REQUEST (REF: DOIA016-2025/26)

On 16 October 2025, you contacted the Ministry for Pacific Peoples (the Ministry) requesting under the Official Information Act 1982 (OIA), information related to the use of Approved Artificial Intelligence Tools. I have outlined your specific request and my responses below.

This is a request made under the Official Information Act 1982. To better understand the government's use of artificial intelligence (AI), I request the following information:

1. *A list of all AI tools that are currently approved for use by staff at your agency.*

The AI tools currently approved for use by Ministry staff is Microsoft (MS) Copilot – specifically MS Copilot Edge and MS Copilot Teams.

2. *Any documentation outlining the conditions, guidelines, or policies attached to the approval and use of these tools.*

I have appended to this letter a copy of the Ministry's guideline titled "Use of Generative Artificial Intelligence (GenAI) Tools". Refer to **Appendix One**.

3. *For each approved tool that is not free to use, please provide the number of paid licenses or subscriptions the agency currently holds. I confirm that I do not require any commercially sensitive information (e.g. licence costs), merely the number of authorised users.*

The Ministry's MS Copilot tooling is provided as part of the Ministry's MS 365 Enterprise E5 subscription. We have 110 E5 licences.

Auckland
9 Ronwood Ave, Manukau
PO Box 97005,
South Auckland Mail Centre 2240
P: 09 265 3200

Wellington National Office
Level 7, 1 Bowen House
Wellington, 6011
PO Box 833, Wellington 6143
P: 04 473 4493

Christchurch
Level 1, BNZ Centre
120 Hereford St
Private Bag 4741,
Christchurch 8011

4. *Copies of all completed Cloud Risk Assessments and Privacy Impact Assessments (or equivalent documents) for each of the approved AI tools. If any part of this request is declined, please provide the specific grounds for refusal under the Act. I would prefer to receive this information in a machine-readable electronic format. Thank you for your assistance.*

I have appended to this letter a copy of the Ministry's completed Cloud Risk Assessment. Refer to **Appendix Two.**

With regard to copies of Privacy Impact Assessments, no such assessments have been completed. Therefore, I am refusing this part of your request under section 18(e) of the OIA, as the information you have requested does not exist.

In line with standard OIA practice, the Ministry proactively publishes some of its responses to OIA requests. As such, this letter may be published on the Ministry for Pacific Peoples' website. Your personal details will be removed, and the Ministry will not publish any information that would identify you or your organisation.

Should you wish to discuss this response with us, please feel free to contact the Ministry at: oia_requests@mpp.govt.nz.

If you are dissatisfied with this response, you have the right, under section 28(3) of the OIA, to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Mālō 'aupito

Danilo Coelho de Almeida
Deputy Secretary
Corporate & Support Services

Ministry for Pacific Peoples
Te Manatū mō ngā Iwi ō te Moana-nui-ā-Kiwa

Appendix One

Ministry for Pacific Peoples

Use of Generative Artificial Intelligence (GenAI) Tools

Guidelines

Deputy Secretary, Corporate & Support Services

April 2024

Document

This document contains the guidelines for the use of Generative Artificial Intelligence (AI) tools at the Ministry for Pacific Peoples (MPP).

Version History

VERSION	DATE	AUTHOR	KEY CHANGES
1.0	05 April 2024	Kate Brewer	First draft
2.0	24 April 2024	Kate Brewer	Updated based on feedback (Transitional Director IT, Director Operations Corporate Services, Principal Advisor Risk and Assurance).
3.0	September 2020	Principal Advisor, People & Culture	Annual review and amendments
5.0	December 2024	Director, People & Capability	Updated in line with legislation. Procedural aspect moved to guidelines

Note: Do not make unauthorised electronic copies or new versions (drafts) of this corporate policy. Contact the Director, People and Capability to have new drafts initiated and recorded in the appropriate manner.

Status

CONTACT	Chief Information Security Officer
STATUS	In effect from May 2024
APPROVED DATE	May 2024
POLICY OWNER	Ministry for Pacific Peoples
BUSINESS OWNER	Deputy Secretary Corporate & Support Services
REVISION CYCLE	Every two years or as needed
NEXT REVIEW	December 2025

Signoff

NAME	ROLE	SIGNATURE	DATE
Danilo Coelho de Almedia	Deputy Secretary, Corporate & Support Services		3 December 2024

Table of Contents

1. Introduction

This document sets out MPP's expectations on the responsible use of Generative Artificial Intelligence (GenAI) at MPP.

MPP has undertaken an IT Security Assessment of Microsoft's Co-pilot GenAI tool.

MPP'S CURRENT POSITION IS:

- **Co-pilot has been approved as MPP's enterprise GenAI tool;**
- **MPP staff can use Co-pilot in accordance with the Guidance Principles below;**
- **Use of any other GenAI tool is not permitted without an IT Security Assessment and approval from MPP's Chief Security Officer, Chief Information Security Officer and Chief Privacy Officer; and**
- **Personal or sensitive information must not be inputted into Co-Pilot AI tool.**

.

2. Guidance Principles

Don't use Co-pilot for any MPP data classified as SENSITIVE or above	The risks for security and potential impacts if Government SENSITIVE or above datasets were to be compromised could be extremely serious. Do not input these types of datasets into Co-pilot.
Don't input personal information into Co-Pilot	In situations where it isn't possible to use non-personal information, a Privacy Impact Assessment must be conducted, all potential risks must be identified and addressed, and the Assessment must be approved by MPP's Chief Privacy Officer.
Don't use any other GenAI tool	This could create a risk of technologies being used in ways that could result in privacy or security breaches or disrupt the organisation's current and approved technology environment. If staff require use of an AI tool other than Co-pilot, an IT Security Assessment must be conducted, and approval of the tool must be provided by MPP's Chief Security Officer, Chief Information Security Officer and Chief Privacy Office. A Privacy Impact Assessment may also need to be conducted if the tool is intended to be used to input personal information.
Don't input any information into Co-Pilot that would be withheld under the Official Information Act	The risks for the integrity of the public service and potential impacts if redacted information were to be accessed and or inappropriately used could be extremely damaging for public trust and confidence.
Don't use Co-pilot for Ministry decision-making processes.	MPP is required to understand its own decision-making processes and to be able to explain those decisions when questioned to do so. Using GenAI for essential systems and services uses AI algorithms which are extremely complex to understand and very difficult to explain how the output was reached.

3. Why do we need a GenAI Guide?

- GenAI, when used appropriately, can improve services provided by organisations and Government agencies. GenAI is currently being integrated into cloud, security and other services around the world and so is no longer something organisations can or necessarily should avoid using.
- However, New Zealanders have concerns about the use of AI, and they have expectations that any use of it by Government agencies will be done so carefully, ethically and securely.
- This guidance is intended to support staff at MPP to understand the benefits and risks and to be aware of the Ministry's expectations regarding the proper use of the approved GenAI tool, Co-pilot.

4. Benefits of GenAI

- AI assists with mechanical and tedious tasks (i.e. counting or data matching) that people might not want to or be able to do. Those tasks are likely better suited to automation such as offered by AI tools.
- AI can save time. GenAI can be used to create a first draft of documents, but the GenAI outcomes are limited in their ability to create new critical content, and any output requires careful review.
- By using algorithms AI can detect patterns in large volumes of data and can interpret their meaning. Analytics created by AI in this way can use and access more data, are more detailed, and the models improve over time.

5. Risks of GenAI

- As AI models are created off training data which is often publicly sourced or sourced from the input of others using the AI tool, information specific to minority groups may not be well represented in the data drawn from the AI tool and results can be discriminatory or unfair.
- Inputting personal or sensitive information into the AI model without consent or authority may lead to a privacy and / or security breach by the organisation.
- Hackers may manipulate AI models to facilitate cyber-attacks. AI tools can be used to impersonate real people, create fake identities and to assist with online hacking and phishing scams.
- Some AI tools can leak sensitive information that increases security risks. AI models have been known to suggest real passwords.
- AI makes it easier to exploit illegally obtained information from data breaches, to re-identify people in published datasets, and to combine any sources of data to build detailed profiles of people which are more or less accurate.
- Poorly considered prompts used in the AI model may lead to inaccurate responses from it.

6. Definitions

TERM	DEFINITION
Artificial Intelligence	AI is software that learns from data. AI tools are built on 'training data' (see definition below) and examples of AI tools include software used to review and summarise legal documents using language matching; the predictive text function on your laptop or phone; and content creating tools (see definition below) such as Co-pilot.
Generative AI	Is one type of Artificial Intelligence technology that can produce content – such as text, images or audio – by matching the prompts or questions it receives to patterns in the data that it has. On the basis of probability, the technology then uses that matched data to 'fill in the blanks' and create or generate text or images that closely resemble human-related content.
Publicly available AI tools	These sit outside an agency's own environment as third-party AI platforms or software. Apart from Microsoft's Co-pilot, these tools have not been risk assessed by MPP to the standard expected for NZ Government agencies. Open AI's ChatGPT, Microsoft's Bing search and Google's Bard are the most well-known examples of free and publicly available GenAI.
Personal Information	Information about a living individual. Examples include a person's name, telephone number, address, date of birth, ethnic origin and financial information. Even if a person's name is not recorded, but there is a reasonable chance that they could be identified from other information or a combination of pieces of information, it can still be personal information for the purposes of the Privacy Act.
Training data	is an extremely large dataset that is used to teach machine learning models of AI. The data is often publicly sourced or sourced from the input of others using the AI tool and can take various forms, such as images, audio, or text.

7. Further Resources

- Privacy Policy.docx
- Privacy Act 2020
- Summary of Guidance from Office of Privacy Commissioner on GenAI.docx
- Office of the Privacy Commissioner I Generative Artificial Intelligence.
- Interim GenAI guidance for the public service — Full guidance (PDF 193 KB)
- Interim GenAI guidance for the public service — Summary (PDF 230 KB)

This document is a first effort by MPP to provide help to staff to use this new class of technology. It will be updated as the technology evolves, and the risks and impacts are better understood.

Appendix Two

Ministry for Pacific Peoples
Te Manatū mō Ngā Iwi ō te Moana-nui-ā-Kiwa

Ministry for Pacific Peoples

Microsoft Copilot Cloud Security Assessment

12 September 2024

IN-CONFIDENCE

Document Properties

Project Name	Microsoft Copilot Cloud Security Assessment
Client	Ministry for Pacific Peoples
Author	Matthew Haselton
Date	12/09/2024
Version	0.5
Document Status	Draft

Version History

Version	Date	Author	Changes Made
0.1	05/08/2024	Matthew Haselton	Initial Draft
0.2	26/08/2024	Sashi Douché	Peer Review
0.3	27/08/2024	Matthew Haselton	Updates Based on Peer Review
0.4	12/09/2024	Peter Jakowetz	Quality Assurance
0.5	18/09/2024	Peter Jakowetz	Released Draft

Distribution List

Name	Role
Nicholas Carter	Chief Information Security Officer
Mathew So'otaga	Director Operations, Corporate Services and Office of the Secretary

Document Sign-Off

Certification

- I accept the findings of the system audit and all areas of non-compliance, along with the required and recommended remediation actions as documented in the below document.
- I acknowledge that the operation of the service complies with the Ministry's standards and business security requirements and that the certification audit findings are within the Ministry's risk tolerance.
- The outstanding residual risks identified during the certification process do not preclude the solution from being certified, providing they are remediated within the specified timeframes and are formally validated as being addressed.
- I acknowledge my responsibility to ensure agreed remediations are actioned within the specified timeframes and to escalate any areas of non-compliance to the Accreditation Authority in a timely manner.
- I therefore recommend the system for accreditation for use by the Ministry.

Name	Role
Mathew Sootay	Director Operations Corporate Support Services
Caveats:	
Signature	Date: 26/9/24
	CERTIFY / DOES NOT CERTIFY

Accreditation

- I acknowledge the role and responsibility of Accreditation Authority.
- I acknowledge the residual risks outlined in this document associated with the solution.
- I acknowledge the business owner's responsibility to resolve outstanding remediation items within the noted timeframes.
- I confirm that the operation of the solution represents an acceptable level of residual risk to the Ministry.

Name	Role
Danilo Coelho de Almeida	Dep Sec Corporate and Support Services
Caveats:	
Signature	Date 26/09/24
	ACCREDIT / DOES NOT ACCREDIT

Table of Contents

Executive Summary

Introduction

This report presents the findings of an information security risk assessment of the Ministry for Pacific Peoples (MPP) implementation of Microsoft's Copilot. The risk assessment followed the AoG risk assessment process based on the AS/NZS ISO 31000:2009 and ISO/IEC 27005:2011 risk management standards.

Background

The report assesses the security risks associated with using Microsoft's Copilot. Microsoft Copilot is an artificial intelligence tool that supports Microsoft 365 users working with apps like Excel, PowerPoint, Outlook, etc. It combines large language models (LLMs) and uses the Microsoft Prometheus Artificial Intelligence (AI) model using AI tools from OpenAI, such as ChatGPT-4, ChatGTP-4o and DALL-E 3. It also relies on the large web-scraping database from the Bing search engine, Microsoft Natural Language Processing, Text to Speech (TTS), Retrieval Augmentation Generation to ground and add context and Azure cloud services.

Summary

The NZ Government has released interim guidance on the usage of AI[1] within the public service. Summarised this covers:

- Don't use generative AI for data classified at Sensitive or above.
- Don't input or use personal data in generative AI tools if they are external to your environment (in cases such as the use of Copilot).
- Avoid inputting personal data into generative AI tools.
- Prevent AI from being used as shadow IT.
- Avoid inputting generative AI tools any information that would be withheld within OIA requests.
- Avoid using generative AI tools for business critical channels.

Keeping generative AI to a trusted set of tools such as Copilot helps mitigate a number of these recommendations along with working alongside guardrails such as the AI policy within MPP. Ensuring that the following controls are in place and effective over time will help manage the ongoing risks of usage of Copilot specifically:

- User education - ensure AI related training is available, as such that which is planned within KnowBe4.
- Account Security – ensure account security is maintained within M365. This is currently in an appropriate state with the recent work undergone by MPP.
- Consider blocking copilot access to specific sensitive documents or SharePoint folders[2] if deemed necessary to provide additional protection.

[1] https://www.digital.govt.nz/assets/Standards-guidance/Technology-and-architecture/Generative-AI/Joint-System-Leads-tactical-guidance-on-public-service-use-of-GenAI-summary-September-2023.pdf
[2] https://practical365.com/block-access-to-content-services/

Issues Summary

The following issues were identified when reviewing the service:

Table 1 – Issues

Finding ID	Summary	Related Risks
F01	Personal Information (PI) may be used when using Copilot which could be disclosed to the wider learning model.	COP.R01, COP.R02
F02	Personal email addresses may be used for Copilot which may lead to leakage of information.	COP.R01, COP.R02
F03	Use of more than one Generative AI tools by MPP users which may have a weaker security posture.	COP.R01, COP.R02, COP.R04
F04	Incorrect information may be returned by Copilot which may then be further used by MPP staff.	COP.R04
F05	Sensitivity labels on documents in the M365 is incorrectly applied	COP.R03
F06	M365 products and services may not be hardened appropriately	COP.RO5
F07	Insufficient logging and monitoring capabilities	COP.R06

Recommendations Summary

The following recommendations were highlighted relating to the service:

Table 2 - Recommendations

Rec ID	Summary	Related Finding/s	Status

REC01	**Human Review and Moderation of Data**
	• Ensure there are procedures in place that make sure the accuracy and appropriateness of data transferred in and out of Copilot:
	  ○ Reviews of data that is input into Copilot.
	  ○ Review of data that is output from Copilot.
	  ○ Appropriate data sanitisation steps and release management processes developed.
		F01	Open

REC02	**Use only Ministry of Pacific People (MPP) email addresses** • Ensure that MPP staff only use their work email addresses. • Ensure that MPP staff only use Copilot and not any additional AI tools with personal emails.	F02, F03	Open
REC03	**Ensure Staff Adhere to MPP AI Policies** • Develop guidelines and use cases for what types of usage of Copilot can be used within MPP. • Ensure that users don't claim work that is not their own. • Ensure that appropriate user training and adherence to MPP's Guidance on Use of Generative AI tools.	F01, F03, F04	In Progress

Rec ID	Summary	Related Finding/s	Status
REC04	**Appropriate M365 Security, Privacy, Identity and Compliance Policies and Labels** • Ensure that Restrict SharePoint Search is enabled. This prevents Copilot from accessing all SharePoint sites and only restricted to ones that are allowed. • Ensure the correct users have the correct access to information and data. • Ensure that Microsoft Purview information protection is utilised so sensitivity labels can be used, Copilot integrates sensitivity labels into the user interactions to keep labelled data protected.	F04	To be confirmed
REC05	**Logging of Copilot** • Enable comprehensive logging of Copilot tools, such as access logs, data processing logs and output logs.	F07	To be confirmed
REC06	**Ensure Incident Response and Privacy Breach Notifications are in Place** • Ensure that all MPP staff are aware, appropriately trained and know when, where and how to report a breach or disclosure of information.	F01, F06, F07	Closed
REC07	**Develop an Incident Response Playbook** • Ensure an Incident Response Playbook has been developed for MPP to response to incident on Co-Pilot. Such as accidental disclosure of Personal Information or Sensitive MPP information. This may include actions such as notifying users whose date was disclosed.	F01, F06	Open
REC08	**Appropriate Hardening and Management of M365 Tenancy** • Ensure that appropriate hardening is completed for M365 products and services.	F06	Closed

Detailed Findings

This section provides details of the risks identified during the risk assessment for the Microsoft Copilot.

Table 3 – Risk Details

Risk ID	Risk Summary	Gross Risk			Recommendations	Residual Risk		
		Likelihood	Impact	Risk Rating		Likelihood	Impact	Risk Rating
COP.R01	**Disclosure of Sensitive Data** A user intentionally or unintentionally discloses Personal Information (PI) when using Copilot leading to information disclosure.	Possible	Moderate	13	• **REC01** – Human Review and Moderation of Data • **REC02** – Use only Ministry of Pacific People (MPP) email addresses • **REC06** – Ensure Incident Response and Privacy Breach Notifications are in Place • **REC07** – Develop an Incident Response Playbook	Possible but Unlikely	Moderate	9
COP.R02	**Storage of User Prompts** A user intentionally or unintentionally includes sensitive ministry information in the prompt to Copilot which results in information disclosure.	Likely	Moderate	17	• **REC01** – Human Review and Moderation of Data • **REC03** – Adhere to MPP AI Policies	Possible but Unlikely	Moderate	9
COP.R03	**Permission Management of M365** Copilot is able to access/read, and leverage information contained in documents and M365 applications, due to a user have exessive access and permissions, which results in sensitive information being exposed unintentionally.	Possible	Moderate	13	• **REC04** – Appropriate M365 Security, Privacy, Identity and Compliance Policies and Labels	Possible but Unlikely	Moderate	9

Risk ID	Risk Summary	Gross Risk			Recommendations	Residual Risk		
		Likelihood	Impact	Risk Rating		Likelihood	Impact	Risk Rating
COP.R04	**Inaccurate Data Returned by Copilot** Inaccurate information or data is returned by a prompt due to the generative nature of the Copilot model, which is reported in a ministry document. This impacts the integrity of the document which could be misleading or inappropriate.	Possible	Minor	8	• **REC01** – Human Review and Moderation of Data • **REC03** – Adhere to MPP AI Policies	Possible but Unlikely	Minor	5
COP.R05	**Security Vulnerability Exploited** A malicious actor is able to exploit a security vulnerability that is introduced to Copilot or M365 services/products. This leads to information disclosure, loss or modification.	Possible	Major	18	• **REC08** – Appropriate Hardening and Management of M365 Tenancy	Possible but Unlikely	Moderate	9
COP.R06	**Insufficient Logging and Incident Response** An incident occurs causing a breach as a result of insufficient logging of Copilot and the absence of incident response playbooks, it is unable to resolved in a timely manner. It leads to information disclosure, modification or loss.	Possible	Major	18	• **REC05** – Logging of Copilot • **REC06** – Ensure Incident Response and Privacy Breach Notifications are in Place	Possible but Unlikely	Major	9

Appendix A – Risk Assessment Guidelines

Risk Statements

It is important to clearly describe risks so that they can be assessed and evaluated. Assessing the likelihood and impact of a risk stated as *"Fraud may occur"* is difficult, if not impossible, as there is limited information on which to base the assessment. However, assessing the same a risk stated as *"An employee commits fraud resulting in financial loss and reputational damage as fraud detection processes within the information system and business processes are not robust"* is straightforward.

Therefore (where possible) the description of risks identified should use the following structure:

An <uncertain event> occurs, leading to <effect on objectives>, as a result of <definite cause>.

For example:

- "A malicious party gains unauthorised access to information stored in the system by performing a brute force password guessing attack as the organisations password and account lockout policies are not enforced"; or
- "The loss of a laptop leads to official information being disclosed to an unauthorised party, and reputational damage to the Minister and agency as a disk encryption solution has not been deployed to all laptop devices".

Risk identification phase should include an examination of the knock-on effects of the consequences of the identified risks, including their cascade and cumulative effects.

Rating Risk

The likelihood and impacts of the risks will be rated using the simple qualitative scales documented below. The identified risks should be assessed considering the existing controls in place. This will provide the current risk rating and enable the effectiveness of the proposed controls to be assessed.

Impact (Consequences) Assessment

The qualitative scale used to assign an impact rating is presented in the following table. All impacts need to be seen in a business context, and be informed by the business. Rating the impact of a risk should include a consideration of any possible knock-on effects of the consequences of the identified risks, including cascade and cumulative effects.

All impacts need to be seen in a business context, and be informed by the business. The effect of a risk event materialising must be assessed using the agency's approved risk rating scales. If a risk has multiple potential consequences, then the impact with the largest effect must be used to rate the risk. However, where multiple consequences for a single risk are assessed at the same level the impact may be evaluated as being higher than the individual impact statements (e.g., a risk that has two moderate impacts might be judged to have a significant impact when they are combined). Rating the impact of a risk should include a consideration of any possible knock-on effects of the consequences of the identified risks, including cascade and cumulative effects.

Table 4 – Impact Scale

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 SSC, GCDO or OPC. • The SSC and GCDO 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	**Major**	• 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, GCDO or OPC. • Communications and recovery can be managed internally with strong guidance from the SSC and GCDO.	• 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 GCDO.	• 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.

Likelihood (Probability) Assessment

The qualitative scale used to assign a likelihood rating is presented 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.

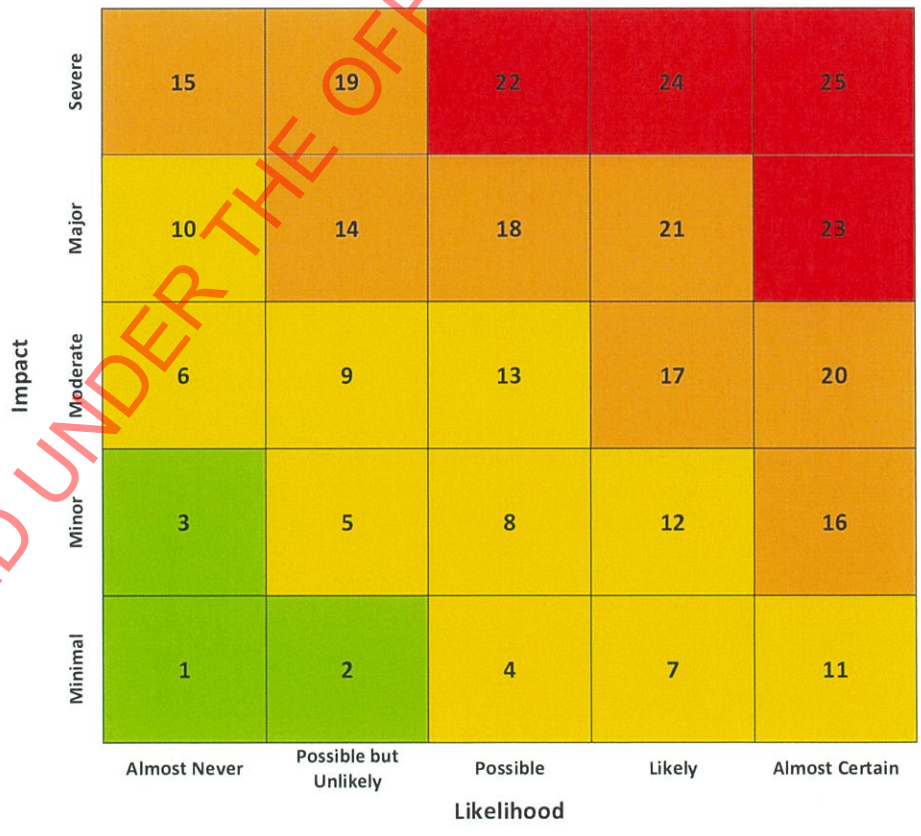
Table 12 – Likelihood Scale

		Likelihood risk rating criteria		
		Description	**Probability**	**Frequency**
Likelihood	**Almost Certain**	The event is expected to occur and is almost inevitable	Greater than 95% chance of occurring	< 1 year
	Likely	The event is expected to occur in most circumstances	60% to 95% chance of occurring	1-2 years
	Possible	The event might occur in some circumstances	30% to 60% chance of occurring	2-3 years
	Possible but Unlikely	The event is not expected but could occur in some circumstances	5% to 30% chance of occurring	3-20 years
	Rare	The event may occur but only in exceptional circumstances	Less than 5% chance of occurring	> 20 years

Risk Matrix

The following table 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 5 – Risk Matrix



Escalation of Risk

The table 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 6 – Risk Escalation and Reporting

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

Appendix C – Glossary

Term	Description
Availability	Ensuring that authorised users have timely and reliable access to information.
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.
Current Risk	The risk with existing risk treatment measures 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.
Probability	The chance of an event occurring.
Residual Risk	The risk remaining after the recommended 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.

Term	Description
Stakeholder	A person or organisation that can affect, be affected by, or perceive themselves to be affected by a risk eventuating.
Threat	A potential cause of a risk.
Vulnerability	A weakness in an information system or service that can be exploited by a threat.
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.
Acceptable Interruption Window (AIW)	The maximum period of time that an information system or service can be unavailable before compromising the achievement of the agency's business objectives.
HRMS	Human Resource Management System.
MPP	Ministry for Pacific Peoples