



**Government
Chief Digital Office**

**Microsoft 365
Security Risk Assessment
Report**

Issued by

*All of Government Service Delivery,
Digital Public Service Branch*



**Te Tari Taiwhenua
Internal Affairs**

New Zealand Government

Document Control

Document Information

Project ID/Name	Microsoft 365
Author	[REDACTED], Quantum Security Services Ltd.
Title	GCDO – Microsoft 365 Security Risk Assessment Report
Version	V0.6 dated 12 September 2022
Document Number	Cloud.Microsoft365.SRA.2022_096

Revision History

Version	Date	Author	Description of changes
0.1	29/06/2022	9(2)(a)	Initial Draft
0.2	30/06/2022	9(2)(a)	Peer Review
0.3	30/06/2022	9(2)(a)	Quality Assurance
0.4	04/07/2022	9(2)(a)	Draft Release
0.4.1	12/07/2022	9(2)(a)	Updates to include additions to scope.
0.5	13/07/2022	9(2)(a)	Draft Release
0.5.1	08/08/2022	9(2)(a)	Incorporating feedback from participating Agencies
0.6	12/08/2022	9(2)(a)	Draft Release
1.0	28/09/2022	Katrina Banks	Finalised for sign-off

Document Approval

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

Acknowledged by	Signature	Date
Jane Kennedy General Manager AoG Service Delivery, Digital Public Service Branch Department of Internal Affairs Te Tari Taiwhenua	Original Signed	30/9/22

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

Acknowledged by	Signature	Date
Katrina Banks Manager Security AoG Service Delivery, Digital Public Service Branch Department of Internal Affairs Te Tari Taiwhenua	Original Signed	28 September 2022

Glossary of Terms

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.
Data	Facts about something that can be used in calculating, reasoning, or planning.
Effect	A positive or negative deviation from what is expected.
Gross Risk	The risk without any risk treatment applied.
Impact	The effect of consequences realised from a risk occurring.
Information	Processed, organised and structured data, providing context for data and enables decision making processes. In the context of this risk assessment information is either classified as RESTRICTED or below, or considered sensitive in nature.
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 risk treatment has been applied.
Risk	The effect of uncertainty on 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.
Vulnerability	A weakness in an information system or service that can be exploited by a threat.

Contents

Document Control	2
Document Information	2
Revision History	2
Document Approval	3
Glossary of Terms	4
Executive Summary	6
Introduction	6
Key Service Provider Risks to Agencies	7
Key Agency Risks	8
Summary of Cloud Service Risks	9
Gross Risk Position	10
Key Service Provider Recommendations	11
Key Consuming Agency Recommendations	11
Residual Risks	12
Business Context	13
Certification Approach	13
Stakeholders	13
Information Classification	13
Business Processes Supported	13
Business Impact	13
Security Requirements	14
Users	15
Legislation, Policy and Guidelines	16
Information Protection Priorities	16
Technical Context and Scope	16
Threat Actors	18
Detailed Risks	19
Generic Cloud Service Risks	36
Threat Assessment	51
Controls Catalogue	53
Appendix A – Consulted Stakeholders	67
Appendix B – Project Overview	68
Appendix C – Risk Assessment Guidelines	69
Rating Risk	69
Likelihood (Probability) Assessment	69
Impact (Consequences) Assessment	69

Executive Summary

Introduction

This report presents the findings of an information security risk assessment for the use and operation of Microsoft 365 (M365) by the Department of Internal Affairs (DIA) Digital Public Service (DPS) branch, in its role supporting the Government Chief Digital Officer (GCDO). The risk assessment followed the Government Chief Information Officer's (GCIO) risk assessment process, which is based on the AS/NZS ISO 31000:2009 and ISO/IEC 27005:2011 risk management standards.

M365, formerly Office 365 (O365), is a cloud-based, subscription suite that encompasses traditional Office 365 and other productivity apps, cloud services, device management, and security. It first emerged as an enterprise-level licensing bundle in 2017.

When consuming M365 and O365 services, Agencies can subscribe to various licencing arrangements. O365 can be consumed independently, whereas M365 refers to the wider platform and package of services.

The risk assessment covers the following scope for M365:

- Exchange Online (EXO);
- SharePoint Online (SPO);
- OneDrive for Business;
- Office 365 Applications (Word, Excel, PowerPoint Outlook, Visio, OneNote and the Teams Client);
- Teams Videoconferencing and Communications Services;
- Microsoft Viva;
- Yammer;
- Power Apps and Work Management Suite;
- PowerBI Online;
- Project Online;
- Planner;
- To Do;
- Endpoint Manager (E3); and
- Defender for Cloud Apps

Any external stakeholders, such as other Agencies using this solution, should review the risks identified in this report using their own risk management framework. This will ensure that the risks identified are relevant to the Agency's use of M365 and are within their business context and risk appetite.

Agencies may wish to perform service or application specific risks assessments based on various use cases, sensitivity of information, or an Agency's risk appetite for a particular service.

As this is a high-level risk assessment report, the risks identified, and ratings assessed, may be different and unique in the context of Consuming Agencies. Therefore, Agencies reading this report should review the risks using their own risk management framework. This will ensure that the risks identified are specific to the Agency's adoption of M365 service, are within their business context, and risk appetite.

Agencies may wish to perform service or application specific risks assessments based on various use cases, sensitivity of information, or an Agency's risk appetite for a particular service.

The details of the risk assessment scope can be found in *Appendix B – Project Overview*. Where **CA** and **SP** are used in this report, they refer to **Consuming Agency** and **Cloud Service Provider** respectively.

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



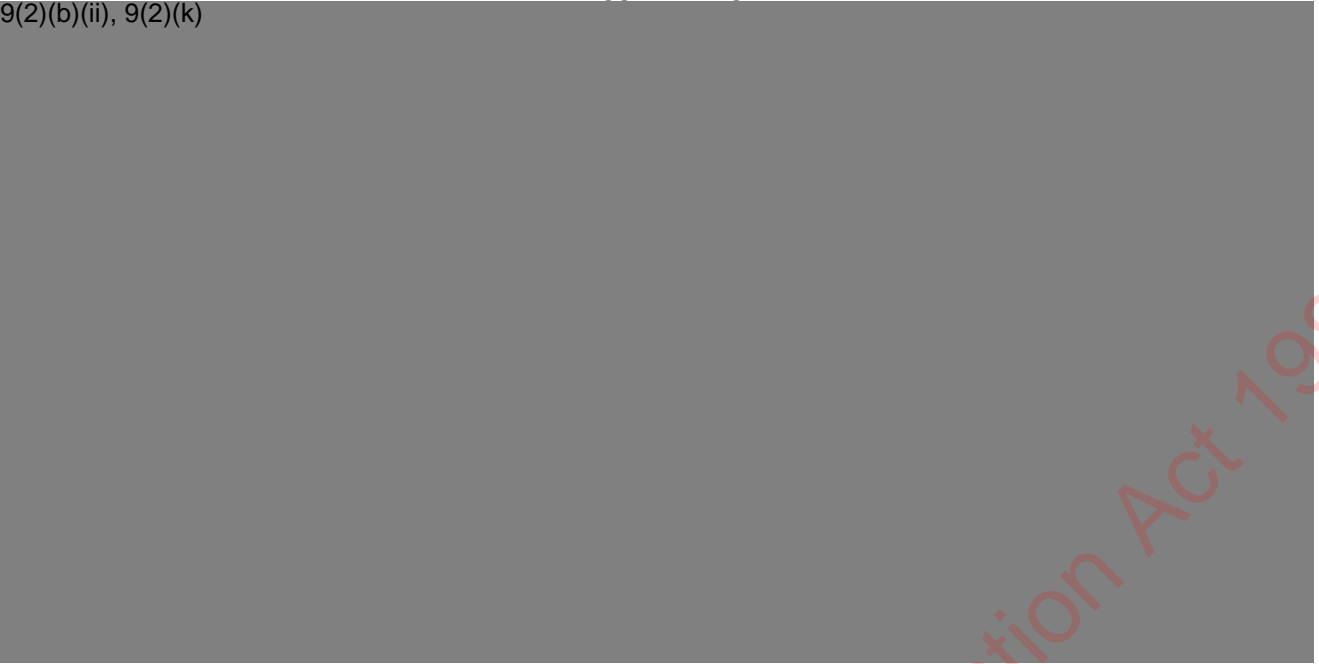
Released under the Official Information Act 1982

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



Released under the Official Information Act 1982

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



Released under the Official Information Act 1982

Gross Risk Position

Table 1 – Gross Risk Ratings illustrates the rating of each risk without any controls in place. The table below includes the gross risk positions of both M365 and generic cloud risks.

Table 1 – Gross Risk Ratings

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



Key Service Provider Recommendations

The risk assessment determined that the following key controls, if implemented, will help to address the identified risks. A controls catalogue was also developed to specify the recommended controls outlined in the risk assessment and is detailed in the Controls Catalogue section on page 53.

To mitigate and manage the identified gross risks rated as 9(2)(b)(ii), 9(2)(k), the following key recommendations should be undertaken:

1. Vulnerability Management and Intrusion Detection and Prevention

Microsoft should implement standardised scheduled patching and vulnerability management practices to ensure software services are not vulnerable to known vulnerabilities. This should be combined with intrusion detection and prevention systems to detect intrusion attempts to M365 services to prevent attackers from gaining unauthorised access to M365 services.

2. Security Incident Response, Logging and Auditing, and Business Continuity Planning

Microsoft should maintain continuous logging and monitoring across services. This allows for the detection and investigation of security incidents associated with these services with accurate and detailed logs. This includes ensuring sufficient logging and monitoring on the management console combined with tested and documented incident response plans which detail the actions to be taken following a significant security event.

3. System Redundancy

Microsoft should implement clustering, load balancing, network redundancy and system redundancy to reduce the strain on M365 servers and minimise the likelihood of service outages. With this, regular backups should be made to allow for the effective recovery of the service should service outages occur.

Key Consuming Agency Recommendations

1. Governance, Security Planning, Billing and Resource Management

Consuming Agencies should ensure that an appropriate governance structure is in place for providing oversight and effective risk mitigation. When procuring cloud services, Agencies should also be aware of the licencing arrangements and what security controls are available to them by default versus what they need to subscribe to additionally for adequate protection from threats. It is recommended Agencies consume E5 licences for M365 and O365. Further details on the comparisons for M365 plans can be found in Microsoft's document library - [Microsoft 365 guidance for security & compliance](#).

2. Access Management, Least Privilege and Role Based Access Control

Consuming Agency users that require access to the M365 services should only be provisioned with the minimum permissions required to perform the duties required of their role in the Agency. A robust process that defines user access management can ensure that permissions are appropriate and updated in a timely manner. The use of strong password polices, and multifactor authentication also reduces the likelihood of unauthorised access to services.

3. Business Continuity Plans

Consuming Agencies should have detailed, documented business continuity plans which detail the actions that should be taken in the event of a service outage. This will minimise the impact of significant service outages and allow for the Consuming Agency to continue to carry out Business as Usual (BAU) practices that would require the service.


Residual Risks

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

Table 2 – Residual Risk Ratings Service Provider

Table 3 – Residual Risk Ratings Consuming Agency

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



Business Context

This section provides an overview of the business context for the Microsoft 365 services that are in scope of this Information Security Risk Assessment.

Certification Approach

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

- Shared security responsibility model when consuming the M365 services;
- Key stakeholders involved when consuming M365 services;
- Classification of the information stored, processed, and transmitted by the M365 services;
- Different types of users with access to M365 services;
- Information Security requirements for the M365 service in terms of confidentiality, integrity, availability, privacy, and any other relevant legislation; and
- Information protection priorities when consuming the M365 services.

Consuming Agencies consuming the Risk Assessment must ensure that they:

- Review the business context assumptions made during the Risk Assessment and ensure that they accurately reflect the Agency's own context;
- Define the business process that will be supported by M365 services;
- Identify and document the business impact should an Information Security or privacy incident occur; and
- Consider the Agency's use context and risk appetite and evaluate assigned risk ratings.

Stakeholders

The following stakeholders for M365 have been identified:

- Department of Internal Affairs;
- Consuming Agencies; and
- Microsoft, their subcontractors, and third parties that assist in delivering M365 services.

Information Classification

Based on the assessment performed during the business context workshop, the information that is stored, processed, and transmitted by M365 was classified **RESTRICTED** and below.

Business Processes Supported

Each CA will be using different M365 services to support different types of business processes. Therefore, it is important for each Agency to understand what business processes will be supported and define the security requirements for the service. This will ensure that Agencies understand the security requirements that the service needs to meet.

Business Impact

Consuming Agencies will use M365 services to support different business processes, therefore transmitting, storing and processing different types of information. It is important for each Agency to identify the information that will be transmitted, stored and processed via Services and understand

IN-CONFIDENCE

the business impact if the confidentiality, integrity and availability of the information were compromised.

In the event of a security breach occurring on one or more M365 services, the most significant business impact for the stakeholders would be on Reputation and Trust, Strategy, and Stakeholders. This has been identified as **5 – Critical**. The following consequences are expected:

- Potential political or reputational damage caused by the disclosure of sensitive Risk Management, Privacy, Procurement and Security information.
- The New Zealand Government's strategic decisions being misinformed by misleading or missing information.
- Agencies' core systems are compromised with released information used to either gain access to Agency data or disrupt the service delivery of Agencies.
- Loss of confidence by the stakeholders, New Zealand citizens and Portfolio Ministers.

Security Requirements

The Confidentiality, Integrity and Availability requirements for M365 have been defined as follows:

Confidentiality

The confidentiality of the information transmitted, stored or processed by M365 is considered as **5 – Critical**. This is largely driven by the **RESTRICTED** classification of information that will be transmitted, stored or processed by M365.

If the confidentiality of information stored or processed by M365 was compromised, the following consequences are expected:

- Restricted information is disclosed to unauthorised parties;
- The New Zealand Government's reputation is damaged;
- The strategic objectives of the New Zealand Government are compromised;
- Loss of confidence by the stakeholders and Portfolio Ministers; and
- Increased workload for Agency staff to solve the security incident.

Integrity

The integrity of the information transmitted, stored or processed by M365 services is considered as **5 – Critical** for consuming Agencies. It is assumed that consuming Agencies will be using the cloud service to store and process information that business processes rely on for decision-making. Inaccurate or corrupted information can cause consuming Agencies to lose their data source of truth and affect business outcomes.

If the integrity of information stored or processed by M365 were to be compromised, the following consequences are expected:

- Modification of sensitive information by unauthorised personnel leading to inaccurate or corrupted data;
- Government decisions are misinformed;
- The New Zealand Government's reputation is damaged;
- The strategic objectives of the New Zealand Government are compromised;
- Loss of confidence by the stakeholders, New Zealand citizens and Portfolio Ministers; and
- Increased workload for DIA and other Lead Agency staff to assess the accuracy of the information and provide corrective actions.

Availability

The availability of the information transmitted, stored or processed by M365 is considered of 4 – Highly Important. This is due to the solution not supporting any business–critical processes, delays in reporting being manageable and Agency capability to use paper–based manual processes being acceptable.

If the availability of information stored or processed by M365 was compromised, the following consequences are expected:

- Agency users may not be able to access the service;
- Lead Agencies' users may not be able to access the service;
- Data may not be accessible;
- Government Strategic decisions may be delayed;
- Increased workload for Agency and Lead Agency users as they rely on manual fallback processes;
- Increased workload for DIA staff to solve the security incident; and
- Loss of confidence by the stakeholders.

Privacy

Personal information may be transmitted, stored, or processed by M365. Therefore, the Privacy of the information transmitted, stored, or processed by M365 service is considered as 5 – Critical.

If personal information will be transmitted, stored, or processed by M365, consuming Agencies must ensure that the privacy of the information is adequately protected from unauthorised access, disclosure, or modification during storage and in transit. Consuming Agencies should also ensure that the service is configured and operating to help Agencies meet the requirements from the Privacy Act 2020.

Users

Users of M365 have been defined as follows:

Table 4 – M365 User roles

Role	Description
Agency Administrators	Agency staff with privileged access to M365 services. Responsible for managing and configuring the Agency's M365 services, user accounts and permissions.
Agency Users	Agency users with role-based access to M365 services. Responsible for using the service to deliver and meet its associated Agency business outcomes.
Microsoft Administrators	Microsoft staff supporting M365 services. They are responsible for the supporting infrastructure and the management on the service maintenance and continuity.
Third-Party Contractors	Third-parties provisioned temporary access to M365 services to assist Agencies in meeting their business outcomes or maintaining M365 services.
External Users	External parties who may be given access to applications or files shared by Agencies.

Legislation, Policy and Guidelines

Government Agencies must ensure that they can demonstrate compliance with applicable legislation, policies, guidelines and any other external requirements when using or operating M365.

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

- Health information privacy code 2000;
- Health information security framework; and
- New Zealand Government Web Accessibility Standard 1.1 and Web Usability Standard 1.31;
- New Zealand Information Security Manual (NZISM V3.5)²;
- Official Information Act 1982;
- Privacy Act 2020;
- Public Records Act 2005;
- The New Zealand Government Protective Security Requirements (PSR)³.

Information Protection Priorities

For purposes of completing this risk assessment, the Table 5 represents the information protection priorities for M365:

Table 5 – Information Protection Priorities

Attribute	Priority Rating
Confidentiality	5 – Critical
Integrity	5 – Critical
Availability	4 – Highly Important
Privacy	5 – Critical

Table 6 represents the scale used to define the information protection priorities shown in Table 5.

Table 6 – Information Protection Priority Scale

0 Not Applicable	1 Unimportant	2 Some Importance	3 Important	4 Highly Important	5 Critical
---------------------	------------------	----------------------	----------------	-----------------------	---------------

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

¹ <https://www.digital.govt.nz/standards-and-guidance/nz-government-web-standards/>

² <https://www.nzism.qcsb.govt.nz/ism-document/>

³ <https://www.protectivesecurity.govt.nz/>

Released under the Official Information Act 1982

Threat Actors

The following threat actors were identified when performing a high-level threat assessment relating to M365 Services. The threat actors relate to threat sources within the detailed Risk Assessment in Table 9 presents the risks associated with use of M365 and O365 applications and services.

Table 9 and Table 10, with further analysis and scenarios in the Threat Assessment in Table 12.

Table 8 – Threat Descriptions

Role	Description
Determined Thief or Vandal	An individual or group that has formulated a plan to breach the logical perimeter(s) of the cloud SP and gain or elevate privileged access to information resources.
Hostile Intelligence Agencies	Hostile foreign intelligence Agencies may target M365 services to gain access to government information. A likely avenue of attack is network (Internet) based, particularly for RESTRICTED classified information and below. Such parties may conduct technical attacks from outside the cloud SP perimeter(s), which will be more challenging to detect if using passive techniques. Hostile intelligence Agencies may seek to subvert other authorised parties within the cloud SP with a view to conducting an insider attack i.e., a threat within a threat.
Interested or Informed Outsiders	An individual or group outside the cloud SP that attempts to gain unauthorised access to user accounts and/or infrastructure to retrieve sensitive information. Motivation for this may be the type of data the cloud SP stores on behalf of Consuming Agencies or information learned from a member of staff within, or SP to, the cloud SP.
Internal Threat	<ol style="list-style-type: none"> 1. A party that has authorised access within the cloud SP and abuses this privilege to steal information and/or media and/or disrupt services for personal gain. 2. A party that has authorised access within the cloud SP and unintentionally performs actions that result in unauthorised access to cloud SP resources and/or disrupts services. 3. An internal threat actor party within the cloud SP with anti-government or anti-establishment political or personal views, and who manipulates their role within the cloud SP.
Issue Motivated Group	A party that has a grievance or issue with the cloud SP or one of their customers (which may be government) and seeks to disrupt operations of the cloud SP to draw attention to their cause. This may directly or indirectly affect Consuming Agencies.
Natural Disaster or Person-Made Hazard	A natural disaster or person-made hazard impacts the infrastructure behind the cloud SP, such as a datacentre, or the people working remotely for the cloud SP, resulting in loss of data and/or disruption to service and/or Business as Usual (BAU) processes.
Organised Crime	These groups may target the cloud SP if they consider they can gain something of value from doing so.

Detailed Risks

Table 9 presents the risks associated with use of M365 and O365 applications and services.

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

Released under the Official Information Act 1982

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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

0/0/0/0/0/0

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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



Released under the Official Information Act 1982

Generic Cloud Service Risks

Table 10 presents the risks associated with use of a Generic Cloud Service that may be applicable when consuming the M365 SaaS service.

Table 10 – Generic Cloud Services Risk Assessment

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

Released under the Official Information Act 1982

Risk ID	Risk Description
	9(2)(k)
GC-R03	Māori Data is Relocated Outside of New Zealand 9(2)(k)
GC-R04	Information Disclosure, Modification or Loss due to Data Distribution 9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description
	9(2)(k)
GC-R05	Information Disclosure, Modification or Loss due to Data Lock In 9(2)(k)
GC-R06	Information Disclosure, Modification or Loss due to Insider Threats 9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description
	<p>9(2)(k)</p>
GC-R07	<p>Information Disclosure, Modification or Loss due to Ineffective Security Incident Response and Management</p> <p>9(2)(k)</p>
GC-R08	<p>Information Disclosure, Modification or Loss due to Inappropriate Use of Cloud Service</p> <p>9(2)(k)</p>

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

9(2)(k)

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

Released under the Official Information Act 1982

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



9(2)(k)

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

Released under the Official Information Act 1982

9(2)(k)

Risk ID	Risk Description
GC-R16	Information Disclosure, Modification or Loss due to Social Engineering Attacks 9(2)(k)
GC-R17	Information Disclosure due to Incomplete Segregation of SP Management Networks 9(2)(k)

Released under the Official Information Act 1982

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



Risk ID	Risk Description	9(2)(k)
GC-R19	Information Disclosure, Modification or Loss due to Compromised SP User Credentials 9(2)(k)	9(2)(k)

Released under the Official Information Act 1982

Risk ID	Risk Description
GC-R20	<p data-bbox="290 338 765 401">Information Disclosure, Modification or Loss due to SP System Misconfiguration</p> <p data-bbox="290 407 765 1039">9(2)(k)</p>
GC-R21	<p data-bbox="290 1136 765 1199">Ineffective Security Incident Management due to Inadequate Logging and Monitoring</p> <p data-bbox="290 1205 765 1627">9(2)(k)</p>

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

Threat Assessment

This section provides details of the threats identified during the high-level threat assessment. The threat assessment has been performed to assist the DIA in understanding key threats relating to the M365 Services from the SP. The STRIDE framework has been used to determine threats relating to key area: Spoofing, Tampering, Information Disclosure, Denial of Service and Elevation of Privilege.

Table 11 – Detailed Threat Scenarios

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

Released under the Official Information Act 1982

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

Threat Actor	[Redacted Content]	STRIDE Category
		Repudiation
Issue Motivated Group		Tampering Information Disclosure Denial of Service
Natural Disaster or Person-Made Hazard		Tampering Denial of Service
Organised Crime		Denial of Service Information Disclosure Denial of Service

Released under the Official Information Act 1982

Controls Catalogue

Table 8 presents the security controls to effectively manage the risks recorded in Table 9 presents the risks associated with use of M365 and O365 applications and services.

Table 9

Table 8 – Security Controls

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C01	Contracts and SLAs	<p>Ensure that contracts and associated Service Level Agreements (SLAs):</p> <ul style="list-style-type: none"> Clearly define the legal jurisdiction for contractual disputes relating to the use and function of the service; Clearly define the ownership of the data stored, processed and/or transmitted by the service; Define in which jurisdiction official information can and will be stored, processed and/or transmitted by the service; Ensure that official and/or private information is appropriately protected to accepted Information Security standards in SP's environment, including backups and other environmental copies; Ensure that the time to return to full service after a failure or outage, including data restoration, meets the organisation's business continuity requirements; Require that all access to the organisation's information and systems be monitored; Require and specify means to notify to the organisation of any actual or possible unauthorised access; Require engagement with the organisation in resolution of any information access incidents or issues; Require regular reports be delivered from SP on their performance against the SLA's; Require the organisation to be allowed to carry out regular audits to ensure compliance with its requirements or provide a full copy of all relevant independent third-party audit reports; Require sufficient resiliency from SP in its own and its network provider's infrastructures to minimise the impact of infrastructure failures, denial of service and other Internet based attacks; and Ensure the contract with SP outlines clearly the services in scope and that the organisation is alerted when there are any changes to services in scope.. 	Likelihood	2.2.5.C.01 2.3.20.C.01 2.3.23 3.2.9 3.2.11 3.3.7 3.3.11 4.4.8 6.4 22.1 22.1.18
C02	Due Diligence	<p>Ensure that adequate due diligence is undertaken across the service, specifically:</p> <ul style="list-style-type: none"> Defining the Information Security requirements of the service; Assessing whether the defined Information Security requirements are met by the service; Identifying and assessing any third-party dependencies that the SP may have; and Ensuring Third Parties can meet New Zealand security requirements as contractor. <p>For higher handling requirements Agencies must ensure that assurance checks are conducted on cloud providers.</p>	Likelihood	2.2.4 4.4.8 12.7
C03	Non-Disclosure and Confidentiality Agreements	<p>Identifying, articulating and regularly reviewing the organisation's requirements for confidentiality or non-disclosure agreements reflects the organisation's needs for the protection of its information. Ensuring contracts with SPs, Vendors and authorised Third Parties incorporate appropriate non-disclosure and confidentiality agreement provides the organisation with the assurance that its information will be safe from disclosure.</p>	Likelihood	4.4.8.C.02 4.4.8.C.03
C04	Risk Management	<p>Ensure that system undertakes risk identification and assessment, selection and implementation of baseline and other appropriate controls and the recognition and acceptance of residual risks relating to the operation of the system. Systems should be accredited before they are used operationally.</p> <p>Ensure that a Security Risk Management Plan (SRMPs) is developed to identify associated security risks for the system and address appropriate treatment measures including physical environments.</p>	Likelihood, Impact	2.3.27.C.02 3.3 12.7.14 4.4 4.5 5.1.8 5.1.9 5.3 22.1.21 22.2.13

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C05	Human Resources Security	<p>Ensure that all employees and contractors understand their responsibilities and are suitable for the roles which they are employed for, including:</p> <ul style="list-style-type: none"> • Security vetting all new staff before beginning employment and on a regular basis thereafter; • Undertaking an induction process that covers their responsibilities for Information Security; • Acknowledging the Code of Conduct and Information Security policy; • Acknowledging the employee's Terms and Conditions of Employment; • Receiving regular security awareness training; • Monitoring and management of changes in employee circumstances and behaviour; and • Removing access rights when their employment or contract ceases. 	Likelihood	3.2 3.3 3.5 5.1.7 9.2 19.1.18 22.1.27
C06	Security Vetting	<p>Ensure that authorised users of a system or service are vetted by an approved vetting service such as that provided by the Ministry of Justice. Only appropriately, authorised, cleared and briefed personnel are allowed access to the systems.</p>	Likelihood	3.5 9.2 9.4
C07	Security Awareness Training	<p>Ensure that all employees and contractors are provided with ongoing awareness training. Topics such as Information Security responsibilities (e.g., email security and using the internet), legislation and regulation, consequences of non-compliance with Information Security policies and procedures and potential security risks and counter measures should be covered.</p>	Likelihood	3.2 3.3 5.6.3.C.01 9.1 9.3 15.0 19.1.18 22.1.27
C08	User Training	<p>Ensure that all users of an information system are well trained in the correct use of the system to reduce the likelihood of inappropriate use or mistakes.</p>	Likelihood	3.2 9.1 22.1.27
C09	Access Control	<p>Ensure that users are only provided with access to the service that have been specifically authorised to use, including:</p> <ul style="list-style-type: none"> • Documenting of an access control policy that defines business requirements for access, principles for access (e.g., need to know, role based) and access control rules that will ensure these requirements are met; and • Implementing specific policies for access control based on business functions, processes or user roles and responsibilities, such as administrator access, user access, system access, remote access, network access, and discretionary and mandatory access. 	Likelihood, Impact	5.5.5 9.2 11.7 16.1 16.2 16.3 16.4 16.5 22.1.24 22.2.16
C10	Separation of Duties	<p>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.</p>	Likelihood, Impact	16.2.6
C11	Role Based Access Control	<p>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.</p>	Likelihood, Impact	9.2 9.4 11.7 16.2.6 16.3
C12	User Account Lifecycle Management	<p>Ensure that user accounts are managed through their lifecycle process, including:</p> <ul style="list-style-type: none"> • Assigning access rights aligned with the defined access control policy; • Reviewing access rights on a regular basis; • Disable accounts when a user leaves an organisation; • Disable accounts when a user no longer requires access; and • Remove or update access rights (e.g., when a user change roles within an organisation). 	Likelihood, Impact	5.5.5 9.2.7 16.1 16.3

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C13	Least Privileges	Ensure that only the minimum required access rights are granted to a user or system when accessing a system, preventing the assignment of excessive user permissions. Privileged access rights are controlled through formal authorisation process and implemented in accordance with the defined access control policy.	Likelihood, Impact	16.3 16.4.31.C.01 22.1.24
C14	Password Policy	Ensure the use of a robust password policy including: <ul style="list-style-type: none"> • Enforcing the use of individual user IDs and passwords to maintain accountability; • Allowing users to select and change their own passwords; • Enforcing a choice of quality passwords (what quality passwords are should be explained in the password policy), including minimum password length and complexity requirements; • Forcing users to change their passwords at the first log-on or if reset; and • Enforcing regular password changes (at least every 90 days) and as needed. 	Likelihood	16.1.40 16.1.41
C15	Secure Password Distribution	Ensure that user passwords should be protected against unauthorised access when distributed initially. Distribution methods may include: <ul style="list-style-type: none"> • Encrypted email; • A secure password reset mechanism that positively authenticates the user (such as a challenge question or multifactor authentication); • A text message to a verified mobile number; and • A telephone call. 	Likelihood	16.1.40 16.1.41
C16	Identity Management and Authentication	Identity management and authentication is the identification and authentication processes that verify the identity of a user or device. Secure authentication controls are implemented as physical or logical controls, and reduce the likelihood of unauthorised access to information, services or systems in accordance with an access control policy.	Likelihood	9.2.6 16.1 22.2.16
C17	Multi-Factor Authentication	Where strong authentication and identity verification is required (e.g., privileged users, administrators) additional forms of authentication can be used (e.g., tokens, digital certificates, biometrics). Multi-factor authentication provides the strongest level of authentication, as it requires a combination of at least two of the following forms of identification: <ul style="list-style-type: none"> • Something you know (e.g., username and password (one-time password (OTP) or reusable), personal identification number (PIN)); • Something you have (e.g., hardware or software token, digital certificate, smartcard); and • Something you are (e.g., biometric fingerprint). For higher handling requirements Agencies must ensure multifactor authentication is enabled.	Likelihood	16.1.13 16.1.14 16.1.16 16.1.17 16.4.10 16.5 16.7 19.1.20 21.4.11
C18	Secure Management	Ensure that servers and information systems are administered and managed securely from a suitably hardened and configured central point such as a jump server. Access to the central point should be restricted with access and activities logged. Administrators should be issued with unique accounts that are different to the account used for daily activities such as email or web browsing. A dedicated management network isolated from production networks should also be deployed to reduce the likelihood of management data being intercepted and disclosed, and to reduce the attack surface area of information systems.	Likelihood	18.1.14
C19	Data Backup	Ensure that backups of business-critical information, configurations, logs etc. are recoverable to assist in meeting the defined Recovery Point Objective (RPO), Recovery Time Objective (RTO) and the Maximum Tolerable Downtime (MTD). The data backup process may include appropriate controls required to protect the highest classification of information included in the backup as well as regular restoration tests to confirm its effectiveness. An offline encrypted copy of all backup's may be required and maintained in a location that meets the physical and environmental security requirements for back-up media. Consideration should be given to ensuring a local copy of backup data is held to support business continuity in case of failure of the service. Ensure a backup, recovery and archiving plan is developed, implemented, and incorporated into the Disaster Recovery and Business Continuity plans.	Impact	5.5.5 6.4 6.4.6 13.3.5 16.3.7 16.5 17.1.45 22.2.15.C.03 22.1.26

IN-CONFIDENCE

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

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C24	Encryption of Data in Transit	Ensuring business sensitive, private, or otherwise classified information that flows over the public or untrusted network such as the Internet or internal networks is protected using approved cryptographic protocols, reducing the likelihood of information being disclosed to, or captured by, an unauthorised person. For higher handling requirements Agencies must ensure that data is encrypted in transit.	Likelihood, Impact	8.3.5 16.1.37 17.2 17.3 17.4 21.4.13.C.01 22.1.24.C.04
C25	Encryption of Data at Rest	Ensuring business sensitive, private, or otherwise classified information stored on media is encrypted using approved encryption algorithms and protocols, reducing the likelihood of unauthorised disclosure. For higher handling requirements Agencies must ensure that data is encrypted at rest.	Likelihood, Impact	17.1 17.2 17.3 22.1.24.C.04
C26	Physical Security	Ensuring that all critical facilities such as datacentres, communication rooms, security containers, servers, networks, telecommunication equipment and other important assets are physically protected against accident, natural disaster, attacks and unauthorised physical access. This also involves ensuring environmental controls such as Air Conditioning, Uninterrupted Power Supplies (UPS), and fire suppression are in place to protect the facility. For higher handling requirements Agencies must ensure appropriate physical security controls are in place.	Likelihood	8.1 8.2 8.3 9.2 9.4 16.1.45.C.01 11.4.12 11.5.15 11.7.32
C27	Equipment Security	Ensure that equipment or assets supporting the service are protected against loss, damage, theft and unauthorised access. The considerations for equipment security includes: <ul style="list-style-type: none"> • Ensuring IT equipment always reside in an appropriate class of secure room; • Storing IT equipment during non-operational hours in an appropriate class of security container or lockable commercial cabinet; • Using IT equipment with removable non-volatile media which is stored during non-operational hours in an appropriate class of security container or lockable commercial cabinet as well as securing its volatile media; • Using IT equipment without non-volatile media as well as securing its volatile media; • Using an encryption product to reduce the physical storage requirements of the non-volatile media as well as securing its volatile media; and • Configuring IT equipment to prevent the storage of classified information on the non-volatile media when in use and enforcing scrubbing of temporary data at logoff or shutdown as well as securing its volatile media. 	Likelihood, Impact	8.4 9.2 10
C28	Secure Decommissioning and Disposal	Ensure that IT systems are safely decommissioned and that software, system logic and data are properly transitioned into new systems or archived in accordance with the organisation, legal and statutory requirements. IT systems no longer required should be sanitised and disposed of in an approved manner that reduces the likelihood of data recovered by an unauthorised party. Ensure that a policy and procedures is developed and implemented for the decommissioning and disposal of IT equipment, media, and other important assets. For higher handling requirements Agencies must ensure they have a decommissioning process defined.	Likelihood	11.7.35 12.6 13.1 13.4 13.5 13.6 22.1.26
C29	Media Handling	Ensure that media containing information are protected against unauthorised access, misuse or corruption. This includes classifying, labelling and registering the media and clearly indicates the required handling instructions and level of protection to be applied.	Likelihood	13.2 13.3

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C30	Documentation	<p>Ensure that Information Security documentation is produced for systems, to support and demonstrate good governance. The following documents should be documented:</p> <ul style="list-style-type: none"> • Information Security Policies (SecPol) – setting the strategic direction for Information Security; • Systems Architecture – illustrates the structural design of the system including any outsourced services; • Security Risk Management Plans (SRMPs) – identifying security risks and appropriate treatment measures for systems; • System Security Plans (SecPlan) – specifying the Information Security measures for systems; • Standard Operating Procedures (SOPs) – ensuring security procedures are followed in an appropriate and repeatable manner; • Incident Response Plans (IRPs) – outlining actions to take in response to an Information Security incident; • Emergency Procedures – ensuring classified information and systems are secured before personnel evacuate a facility in the event of an emergency; and • Independent Assurance Reports – provides assurance to System Owners, Certifiers, Practitioners and Accreditors and to assist system designers, enterprise and security architects where assurance reviews cannot be directly undertaken on SPs. 	Likelihood, Impact	3.2 3.3 4.3.18 5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8 9.2.5
C31	Change Management	<p>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:</p> <ul style="list-style-type: none"> • An upgrade to, or introduction of, IT equipment; • An upgrade to, or introduction of, software; • Environment or infrastructure change; and • Major changes to access controls. 	Likelihood	3.3 6.3 16.3.5
C32	Performance and Capacity Management	<p>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.</p>	Likelihood, Impact	3.2 3.3 12.7.19 22.1
C33	Malware Protection	<p>The installation of malware protection software on all endpoints and devices will reduce the likelihood of malicious code infecting the service. Configuring the protection to perform real-time checks for malware, automatically update its definition database, quarantine any infected files and automatically alert System Administrator(s) will ensure any infection is managed. Additional controls that detect and/or prevent the use of known malicious websites may also be considered.</p>	Likelihood, Impact	14.1
C34	Configuration Management	<p>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.</p>	Likelihood, Impact	5.5 12.2 14.1 18.1 22.2.14
C35	Release Management	<p>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.</p>	Likelihood	14.4.4
C36	Patch and Vulnerability Management	<p>Ensure that security patches are applied in a timely fashion to manage software and firmware corrections, vulnerabilities, and performance risks. Critical patches must be applied within two days of the release of a patch, and other patches should be applied as soon as possible or as per vendor recommendations. For higher handling requirements Agencies must ensure that appropriate patching and maintenance of software is undertaken.</p>	Likelihood	6.2 12.4
C37	System Hardening	<p>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.</p>	Likelihood	14.1 14.2
C38	Security of Network Services	<p>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:</p> <ul style="list-style-type: none"> • Using structured Internet and network addressing and naming schemas (e.g., Ipv4/6, DNS); • Identifying and creating network trust domains based on business security requirements (e.g., Guest networks, user networks, etc.); • Limiting access to network services and security domains (e.g., Management zones); and • Protecting network records using secure protocols and cryptographic technologies (e.g., DNSSEC, secure routing). 	Likelihood	18.0

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C39	Intrusion Detection and Prevention	Intrusion Detection and Prevention monitors network and/or system activities for malicious activity. The main functions are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. They can be deployed in four ways: <ul style="list-style-type: none"> • Network-Based Intrusion Prevention System (NIPS): monitors the entire network for suspicious traffic by analysing protocol activity; • Wireless Intrusion Prevention Systems (WIPS): monitor a wireless network for suspicious traffic by analysing wireless networking protocols; • Network Behaviour Analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations; and • Host-Based Intrusion Prevention System (HIPS): an installed software package which monitors a single host for suspicious activity by analysing events occurring within that host. For higher handling requirements Agencies must ensure that IDP/ IDS is implemented, along with appropriate supporting processes.	Likelihood, Impact	3.2 3.3 7.1.7 8.3 18.4
C40	Tenant Segregation	Tenant Segregation is achieved through the implementation of the appropriate multi-layered controls that considers the deployment (e.g., private, hybrid, public, etc.) and service model (SaaS, PaaS, and IaaS). Segregation (separation) between tenants' domains ensures that tenant information and services are isolated within enforced boundaries. Proper segregation also provides assurance that incidents are contained and only affect the affected tenant and do not extend to co-tenants. Effective tenant segregation ensures that one tenant cannot deliberately or inadvertently interfere with the security of the other tenants.	Likelihood, Impact	22.2
C41	Segregation of Networks	Ensure that the network is separated adequately, including the incorporation of security domains (Demilitarised zones and virtual local area networks) to segregate information systems with specific security requirements or different levels of trust. Where appropriate, isolation controls such as switch port isolation and private VLANs are used to isolate hosts within the same security domain.	Likelihood, Impact	18.1.13 19.1.14 22.3
C42	Separation of Non-Production Environments	To prevent unauthorised access or changes to the operational environment, non-operational environments such as development, test and training environments must be separated from operational ones. Consider the following to ensure effective separation of environments: <ul style="list-style-type: none"> • All changes must be tested in a non-operational environment before being transferred into the operational environment; • Testing must not be done in operational environments; • Rules for the transfer or installation of software into operational environments from non-operational environments; • Users must have different accounts for operational and non-operational environments; and • Operational or production data must not be used in non-operational environments unless the same security controls are in place in the non-operational environment. 	Likelihood, Impact	14.4
C43	Firewalls	Firewalls are deployed to monitor and control connections and information flows between security domains. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a firewall before granting access to internal systems. Configure the firewall rule-base to limit the inbound and outbound (ingress and egress) connections, protocols and ports required to support the service, and ensure firewalls are VoIP-aware.	Likelihood and Impact	14.1 14.4 14.5 18.1 19.1 19.3 19.5.26 21.1.5 21.4.10.C.14
C44	Business Continuity Plan	Ensure that Business Continuity Plans are established to assist in meeting business requirements, minimise disruption to the availability of information and systems and assist recoverability. By defining the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for the Service, business owners can ensure that continuity objectives are able to be achieved. Developing and testing a plan confirms that appropriate measures to ensure the continuity of critical business services are identified and implemented.	Impact	6.4
C45	Disaster Recovery Plan	Ensure that Disaster Recovery Plans are established to assist in meeting business requirements, minimise disruption to the availability of information and systems and assist recoverability. Defining, implementing, and testing a Disaster Recovery Plan supports the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirements defined in the Business Continuity Plan. For higher handling requirements Agencies must ensure that Disaster Recovery plans cater for cloud based services.	Impact	3.2.17 3.3.12 6.4
C46	System Redundancy	Ensure that sufficient redundancy exists within the system to protect against system outages. This can be done by including the following controls in system designs: <ul style="list-style-type: none"> • Clustering; • Load balancing; • Network redundancy; and • System redundancy. 	Likelihood, Impact	3.3 6.4.5

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C47	Information Security Review	<p>Ensure Information Security reviews are conducted at least annually to maintain the security of systems and detect gaps and deficiencies, including:</p> <ul style="list-style-type: none"> Identifying any changes to the business requirements or concept of operation for the subject of the review; Identifying any changes to the security risks faced by the subject of the review; Assessing the effectiveness of the existing countermeasures; Validating the implementation of controls and countermeasures; and Reporting on any changes necessary to maintain an effective security posture 	Likelihood	3.2 4.1 4.2 4.3 4.4 4.5 6.1
C48	Architecture and Design Review	<p>Reviewing the architecture and design of the service ensures that it meets the functional and non-functional business requirements including adequate controls to protect the confidentiality, integrity and availability of information stored, processed, or transmitted by the service.</p> <p>An Architecture and Design review will also assess the organisation's adoption of, and integration with, the service to ensure that the organisation's own security controls will meet the businesses requirements.</p> <p>Architecture and Design Reviews should be regularly conducted to verify that changes in the threat landscape and NZISM requirements are considered.</p>	Likelihood, Impact	4.3 5.1.8 6.1 14.2 14.3 14.4 14.5 18.1 19.1 19.3 21.4 22.2.14
C49	Security Tests and Controls Audit	<p>Ensure that information assurance activities such as controls audit and technical security assessments are conducted against systems to demonstrate that due consideration has been paid to risk, security, functionality, business requirements and as a fundamental part of information systems governance and assurance. The assurance activities should focus on validating whether:</p> <ul style="list-style-type: none"> Security posture of the organisation has been incorporated into its system security design; Controls are correctly implemented and are performing as intended; Changes and modifications are reviewed for any impact or implications; and Effectiveness of Information Security measures for systems is periodically reviewed and validated. <p>Penetration tests (when allowed), also provide assurance that exploitable information system weaknesses are identified, controls are configured and enforced to protect against real world attack scenarios.</p>	Likelihood	3.3 4.1 4.2 4.3 6.1 6.2
C50	Data Loss Prevention	<p>Depending on the solution and the risk posture of information leakage, Data Loss Prevention (DLP) and/or Cloud Access Security Broker (CASB) technologies and techniques are implemented to safeguard sensitive or critical information from leaving the organisation. They operate by identifying unauthorised use and data exfiltration and take remedial action by monitoring, detecting, and blocking unauthorised attempts to exfiltrate data. For DLP to be effective, all data states (processing, transmission, and storage) are monitored.</p> <ul style="list-style-type: none"> Agency managed and/or unmanaged devices with an ability of information upload to 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 or information disclosure; Data loss protection rules shall be configured in protection mode; Rules Shall be reviewed and modified on a regular basis, and upon related security incident/breach; and Administrative access to these tools is restricted to authorised personal only. 	Likelihood, Impact	7.3.7 7.3.8 14.1.13.C.03 21.4.5 21.4.14.C.02 21.1.24
C51	Application Security	<p>Establishing rules for the development of software and systems will ensure that the developers use secure development practices such as those defined and documented by Microsoft and the Open Web Application Security Project (OWASP).</p> <p>Functional testing is primarily used to verify that a service or a piece of software is providing the functionality required by the business. Typically, functional testing involves evaluating and comparing each service or software function with the business requirements (including security).</p> <p>By implementing an application proxy at web-based interfaces, the service will be protected against a wide range of Layer 3 – 7 attacks including DoS (e.g., SYN Flooding, Smurf, ICMP Ping Flood, Fraggle attacks), SQL Injection and Cross Site Scripting (XSS). Inspecting external traffic (inbound and outbound), messages and attachments for malicious content at the gateway will reduce the likelihood of malicious code entering the service. The content filter can be configured to quarantine any suspicious files and automatically alert the System Administrator(s) when malicious content is detected. It may also be configured to restrict the file types that can be transferred into and out of the Organisation's environment to only those that are required by the business.</p>	Likelihood, Impact	12.2 12.7.19 12.7.20 14.3 14.4 14.5 19.0 20.3
C52	Data Management	<p>Ensure data transfers are performed in accordance with the policy and processes and are approved by a trusted source.</p> <p>All classified information that are stored within a database are labelled appropriately with protective markings and database files are protected from access that bypasses the database's normal access controls.</p>	Likelihood, Impact	20.0 22.1

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C53	Governance	Ensure an appropriate governance structure is in place for providing oversight to make sure that risks are adequately mitigated, and controls are implemented to mitigate risks.	Likelihood, Impact	3.0 4.1 4.4 4.5 5.1 6.1 16.4 16.7 19.5 22.1
C54	Asset Management	Ensure physical measures are applied to facilities, IT equipment and communication devices so to protect systems and their infrastructure.	Likelihood	7.3.2 8.0 11.2.16.C.01 11.4 11.4.12 22.2.16.C.01
C55	Billing and Resource Management	To develop and manage Information Security budget projections and resource allocations based on short-term and long-term goals and objectives. When procuring cloud services Agencies should be aware of the licencing arrangements and what security controls are available to them by default versus what they need to subscribe to additionally for adequate protection from threats. It is recommended Agencies consume E5 licences for Microsoft 365 ad Office 365 services. Further details on the comparisons for M365 plans can be found here .	Likelihood	3.3 3.3.9.C.01
C56	Location of the Cloud Service	Services may be hosted inside or outside of New Zealand, and it may be possible to choose what locations Agencies can choose to house their services. If a SP has a global presence, data may transit, or be backed up in foreign datacentres which may not be transparent to CA. Support services for services hosted in a country may be provided from another jurisdiction, which should be considered when purchasing cloud services.	Impact	22.1.22
C57	Privacy Impact Assessment	To assess the privacy impacts of a project and where necessary (e.g., application, platform, database, a service, procedure), a privacy impact assessment (PIA) must be conducted in order to comply with the Privacy Act, the privacy of individuals, and assist in making decisions about how to mitigate and manage privacy risks.	Impact	3.2 3.3 3.1.9.C.01 5 22.1.22
C58	Dedicated Network Connectivity	Dedicated network connectivity, or dedicated private networks, allow customers to attach their networks to SPs directly. This allows them to bypass network providers through a direct connection physically and reduces capacity and internet routing issues.	Impact	18.2 19.1
C59	Denial of Service Protection	To protect a virtual environment from being exploited by a Denial of Service (DoS) attack, develop, and implement a Denial of Service (DoS) response strategy that includes: <ul style="list-style-type: none"> To identify the source of DoS, either internal or external; How to diagnose the incident or attack type and attack method; and How to minimise the effect of a DoS attack. Ensure a Virtual Machine (VM) migration and decommissioning policy and related SOPs are in place.	Impact	16.1.14 18.3 19.2 19.5 21.4 22.2.15
C60	Content Delivery Network	A content delivery network, or content distribution network (CDN), is a geographically distributed network of proxy servers and their datacentres. The goal is to provide high availability and performance by distributing the service spatially relative to end users.	Impact	N/A
C61	Exit Strategy	A planned approach to terminating a service in a way that will maximise benefit and minimise damage to the organisation. This may include considering termination and early-withdrawal fees, cancellation notification, data extraction mechanisms, and use of common information types that can be easily transferred.	Impact	N/A
C62	Out-of-band Administration	Administration of the servers has to be conducted through a dedicated network to prevent management data being intercepted and the network capacity being saturated by the users' activity or DoS attacks. This could be implemented by either a dedicated hardware network interface, dedicated VPN or by implementing traffic throttling at all the required stages to ensure enough network capacity is available for the administration access. Access to console information like system logs, system command line and the ability to restart systems that are unresponsive should also be available independently of the ability to access the applications on the system.	Likelihood, Impact	18.6 22.3

IN-CONFIDENCE

Number	Title	Description	Reduces	NZISM Reference(s) v3.5
C63	Information Classification and Labelling	Information is properly classified, labelled and registered in order to clearly indicate the required handling instructions and degree of protection to be applied.	Likelihood, Impact	13.2
C64	Service Roadmap	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	N/A

Released under the Official Information Act 1982

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

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

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



Released under the Official Information Act 1982

Appendix A – Consulted Stakeholders

The following stakeholders were consulted to inform the risk assessment:

Table 6 – Consulted Agencies

Attendee	Agency Name
Dayton Hight	Ministry of Education
Diane Simpson	Ministry of Education
Geoff Barnard	Tauranga City Council
Ian Henry	Electoral Commission
Kee Chin	Financial Markets Authority
Mae Koh	Department of Internal Affairs
Matthew Dean	Canterbury District Health Board
Michael de Ruiter	Canterbury District Health Board
Nick Wakefield	Canterbury District Health Board
Paul Headland	Department of Internal Affairs
Paul Hume	Transpower
Rhyse Gibson	Tertiary Education Council
Syed Hussaini	Wellington District Health Board
Tiaan de Klerk	Tertiary Education Commission
Tom Stewart	Reserve Bank of New Zealand

Appendix B – Project Overview

The risk assessment was undertaken in accordance with the statement of work dated 22 February 2022.

Scope

The Department of Internal Affairs (DIA), as Government Chief Digital Officer (GCDO) performed an information security risk assessment of the use and operations of M365.

Approach

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

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

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 7 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 that risk occurring.

Table 13 – 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 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 – 24 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 24 – 48 months.
1	Almost Never	It is difficult for the threat to exploit the vulnerability or it is not expected to occur within 4 years.

Impact (Consequences) Assessment

The qualitative scale used to assign an impact rating is presented in Table 14. 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 any cascade and cumulative effects.

Table 14 – AoG DIA All-of Government Risk Consequence Guide

Scale	Description	Reputation and Trust	Investment / Fiscal	Strategy	Delivery	Stakeholders
5	Severe	<ul style="list-style-type: none"> Severely affects the international reputation of NZ The Government suffers severe negative reputational impact The Prime Minister loses confidence in the Minister(s) and/or DIA's senior management Severe and potentially irrecoverable loss of confidence in GCIO DIA suffers severe political and/or reputational damage that is not easily recovered from External or independent investigation is commissioned 	<ul style="list-style-type: none"> Long-term and severe negative impact to the national economy Inability to attract on-going investment from Government for ICT Functional leadership & change Impact cannot be managed without major additional funding from Government. Sustainability of multiple key vendors severely compromised Systemic major project failures Widespread loss of benefits for key AoG activities 	<ul style="list-style-type: none"> Severe compromise of the strategic objectives of the NZ Government Key AoG outcomes not achieved Unintended significant change to AoG Strategy Abandonment of key strategy or platform Severe compromise of the strategic objectives and goals of multiple Agencies 	<ul style="list-style-type: none"> Severe and simultaneous loss of organisational capability in multiple Agencies Severe adverse impact of large numbers of end users / clients Severe adverse impact on multiple key vendors or wider supply chain 	<ul style="list-style-type: none"> Severe multiple Agency / sector wide adverse impact on business outcomes Treasury or SSC intervention with control removed from DIA Sustained media interest Withdrawal of key Vendors Successful legal action by multiple affected stakeholders Death or permanent incapacity or ill health
4	Significant	<ul style="list-style-type: none"> Significant change to the role of ICT Functional Leadership (or DIA's involvement) Significant loss of confidence and trust in DIA by Portfolio Minister Public Inquiry or long-term and widespread loss of confidence in DIA Significant political and/or reputational damage to both DIA and Portfolio Minister Loss of confidence in the AoG Governance frameworks and DIA / GCIO ability to manage Media interest is sustained with criticism levelled at the GCIO and DIA 	<ul style="list-style-type: none"> Widespread withdrawal of Agency participation Significant system level fiscal impact on multiple Agencies Vendor investment willingness significantly compromised Inability to attract on-going investment for key business cases Weak commercial or legal position resulting in unintended cost to the sector Impact cannot be managed without major re-prioritisation across the sector Loss of return 	<ul style="list-style-type: none"> Beneficial change across the system is significantly impaired or halted Significant compromise of the strategic objectives and goals of multiple Agencies Withdrawal of key Agency participation GCIO/ GCPO led AoG Policy outputs heavily criticised 	<ul style="list-style-type: none"> Delivery capability of other Agencies impacted Significant loss of quality to deliverables across sector Widespread Inability to attract or loss of critical skills Significant on-going impact on day-today service delivery across multiple Agencies 	<ul style="list-style-type: none"> Isolated but significant adverse impact on key vendor(s) Minister(s) and Chief Executive need to be briefed and regularly updated Communications and recovery in crisis mode with significant input and external guidance from SSC Successful legal action by single affected stakeholder Lack of participation interest from new vendors Significant, highly visible and sustained OIA attention Major injury(s) or illness resulting in long-term incapacity or ill health
3	Moderate	<ul style="list-style-type: none"> Minister has heightened concern with possible strained relationship between Minister of Internal Affairs and other key Ministers Questions raised about DIA's decision making or strategic choices Limited and contained political and/or reputation damage Media interest with some minor criticism levelled at the GCIO or DIA Independent investigation is commissioned internally 	<ul style="list-style-type: none"> Withdrawal of individual Agency participation Reduced Vendor investment willingness Loss of return on investment or poor benefits realisation in isolated cases/ Negative impact on ability of Agencies to make medium / long-term investment decisions Fiscal impact can be managed with some re-planning and additional financial input Economies of scale to transformation threatened 	<ul style="list-style-type: none"> Some compromise of the strategic objectives and goals of individual participating key Agencies Some impact on AoG Strategy & outcomes 	<ul style="list-style-type: none"> Loss of organisational capability in single Agencies Limited loss of quality to deliverables across a number of Agencies Moderate impact on service delivery across one or more related business lines 	<ul style="list-style-type: none"> Other dependent parties resourcing decisions impacted negatively Minister(s) is (are) being actively briefed The Chief Executive and senior management briefed and regularly updated Non-compliance with legal obligations Most communications and recovery can be managed internally with some external guidance New vendors reluctant to participate in supplier market Notifiable health & safety event – Significant injury or illness requiring medical treatment or counselling
2	Minor	<ul style="list-style-type: none"> Senior management believe that the GCIO and or DIA reputation has been damaged Senior management needs to be briefed The Chief Executive needs to be advised Minor or short-lived media interest 	<ul style="list-style-type: none"> Agencies threaten withdrawal of participation Reduced appetite for uptake of common capabilities Impact can be managed within current resources, with some re-planning Poor benefits management 	<ul style="list-style-type: none"> Minor impact on AoG Strategy & outcomes 	<ul style="list-style-type: none"> Customer complaints Agency level design flaws Decline in quality Isolated or intermittent user impacts Minor impact on vendors or wider supply chain 	<ul style="list-style-type: none"> Minister(s) may be informed in some cases Little interest from stakeholders but key stakeholders need to be informed. Communications and recovery can be managed internally Minor injury or illness – first aid treatment required
1	Minimal	<ul style="list-style-type: none"> GCIO or DIA reputation is not visibly affected Minimal impact of level trust in the Department 	<ul style="list-style-type: none"> Some indications of fragmentation of collective Agency support 	<ul style="list-style-type: none"> Minimal impact on strategic direction and AoG outcomes largely unaffected 	<ul style="list-style-type: none"> Isolated outages or business interruption evidenced 	<ul style="list-style-type: none"> End user inconvenienced All communications and recovery can be managed internally Minimal impact on vendor / market Event leading to minor injury not requiring first aid

Table 15 – Risk Matrix

Table 15 presents a 5x5 matrix for assigning a risk rating to a risk. It is used by mapping the likelihood and impact ratings. The rating being the point where the likelihood and impact ratings intersect.

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

Escalation of Risk

Table 16 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 16 – 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