# GCDO

# Desktop-as-a-Service (DaaS)

# Risk Assessment Report March 2022

*Issued by*

*Digital Public Service Branch*

Te Tari Taiwhenua
Internal Affairs

New Zealand Government

# Document Control

## Document Information

| | |
|---|---|
| Project ID/Name | GCDO – DaaS Security Risk Assessment |
| Author | 9(2)(a), Quantum Security Services |
| Title | 9(2)(a), Quantum Security Services Limited |
| File name | GCDO – DaaS Security Risk Assessment Report |
| Version | 30 November 2022 1.0 |
| Document Number | GCDO.DaaS.RiskAssessment.2022_113 |

## Revision History

| Version | Date | Author | Description of changes |
|---|---|---|---|
| 0.1 | 08/03/2022 | 9(2)(a) | Initial Draft |
| 0.2 | 08/03/2022 | 9(2)(a) | Peer Review |
| 0.3 | 11/03/2022 | 9(2)(a) | Quality Assurance (Quantum) |
| 0.4 | 11/03/2022 | 9(2)(a) | Draft Released to DIA |
| 1.0 | 23/03/2022 | Shaun Trewern | Document finalised by DIA |

# Document Approval

I approve this Risk Assessment report; it presents the Information Security risks introduced to Subscribing Agencies through the use and operation of Desktop-as-a-Service (DaaS).

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**<br>General Manager<br>All of Government Services Delivery<br>Digital Public Service Branch<br>Department of Internal Affairs Te Tari Taiwhenua | Original Signed | 05 December 2022 |

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

| Acknowledged by | Signature | Date |
|---|---|---|
| **Katrina Banks**<br>Manager Security<br>All of Government Services Delivery, Digital Public Service Branch<br>Department of Internal Affairs Te Tari Taiwhenua | Original Signed | 30 November 2022 |

## Glossary of Terms

**Availability** Ensuring that authorised users have timely and reliable access to information.

**API** A set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service.

**B2B** Business–to–business (B2B), also called B–to–B, is a form of transaction between businesses.

**Confidentiality** Ensuring that only authorised users can access information.

**Consequence** The outcome of an event. The outcome can be positive or negative. However, in the context of Information Security it is usually negative.

**Control** A risk treatment implemented to reduce the likelihood and/or impact of a risk.

**Gross Risk** The risk without any risk treatment applied.

**Impact** See Consequence.

**Information Security** Ensures that information is protected against unauthorised access or disclosure users (confidentiality), unauthorised or improper modification (integrity) and can be accessed when required (availability).

**Integrity** Ensuring the accuracy and completeness of information and information processing methods.

**Likelihood** See Probability.

**NIST** The National Institute of Standards and Technology (NIST) is a physical sciences laboratory and a non–regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness.

**Probability** The chance of an event occurring.

**POC** A proof of concept (POC) is a demonstration to verify that certain concepts or theories have the potential for real–world application.

**Recovery Point Objective (RPO)** The earliest point time that is acceptable to recover data from. The RPO effectively specifies the amount of data loss that is acceptable to the business.

**Recovery Time Objective (RTO)** The amount of time allowed for the recovery of an information system or service after a disaster event has occurred. The RTO effectively specifies the amount of time that is acceptable to the business to be without the system.

**Residual Risk** The risk remaining after the risk treatment has been applied.

**Risk** The effect of uncertainty on the business objectives. The effect can be positive or negative. However, in the context of Information Security it is usually negative.

**Risk Appetite** The amount of risk that the organisation is willing to accept in pursuit of its objectives.

**Risk Owner** A person or entity with the accountability and authority to manage a risk. Usually, the business owner of the information system or service.

**SRS Panel** The ICT Security and Related Services Panel (SRS Panel) are a group of industry experts contracted to provide government agencies with ICT services and advice on a range of security and privacy practices.

**Stakeholder** A person or organisation that can affect, be affected by, or perceive themselves to be affected by a risk eventuating.

**Threat** A potential cause of a risk.

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

## Contents

# Executive Summary

## Introduction

This report presents the findings of an Information Security Risk Assessment for the use and operation of the Desktop-as-a-Service (DaaS) service by the All-of-Government (AoG) Service Delivery (SD) business group of the Department of Internal Affairs (DIA)'s Digital Public Service (DPS) branch. The Risk Assessment followed the Government Chief Digital Officer's (GCDO) Risk Assessment process, which is based on the AS/NZS ISO 31000:2009 and ISO/IEC 27005:2011 risk management standards.

As this is a generic Information Security Risk Assessment report, the risks identified, and ratings assessed may be different and unique in the context of Subscribing Agencies (SAs) and the DaaS service being consumed. Therefore, agencies reading this report should review the risks using their own risk management framework. This ensures that the risks identified are specific to the agency's adoption of DaaS, are within their business context, and risk appetite.

It should be noted that this Information Security Risk Assessment only identifies risks related to the operations of the DaaS service. The information security risks associated with the DaaS service were previously assessed in 2016. Therefore, the approach taken in preparing this updated risk assessment was to use the previous assessment as a base and then consider:

1. Has anything changed in the environment or threat landscape that may affect the risk profile?
2. Are the previously identified risks and their controls still valid/relevant?
3. What is current good practice to ensure the products are safe, secure, and resilient?
4. Does DaaS align with Deputy Chief Executive (DCE) and General Manager (GM) priorities?
5. Have any new dependencies on the DaaS service come to light that may affect the risk profile?

Where **SA** and **SP** are used in this report, they refer to **Subscribing Agency (SA)** and **DaaS Service Provider (SP)** respectively.

9(2)(k)

9(2)(k)

[redacted]

9(2)(k)

[redacted]

## Gross Risks

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

**Table 1 – Gross Risk Ratings**

9(2)(k)

[redacted]

## Subscribing Agency Key Recommendations

The Risk Assessment included key controls that if implemented, helps to address the identified risks. A controls validation plan (CVP) was also developed to specify the recommended controls outlined in the Risk Assessment. The CVP has been detailed in the *GCDO Certification for Agencies Consuming DaaS*, within section *6.1 Controls Validation Plan.*

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

1. **Due Diligence**

   Before the consumption of the DaaS service, agencies should be informed and aware of the implicating risks associated with using the service. This can be done by performing a comprehensive Risk Assessment to identify the risks and controls associated with the service. It may also involve conducting a data impact assessment, privacy assessment, or jurisdictional Risk Assessment depending on the types of data to be stored. All identified risks should be understood and formally accepted with an appropriate risk management plan by the SA before consuming DaaS.

   The amount of due diligence performed should also extend to aspects related to supply chain risks and the ability to obtain appropriate security assurance from the supplier.

2. **Contracts and Service Level Agreements (SLAs)**

   DaaS agreements should define the agency's requirements for the service to ensure it is met by the DaaS SP. This should include the DaaS SP terms of service, associated SLAs, key performance indicators, and metric demonstrating service performance.

   Regular monitoring of the DaaS SP service performance should be carried out to ensure that expectations are continuously met. This includes any third parties contracted by the DaaS SP to provide services supporting DaaS.

3. **Use of Strong Encryption**

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

   Agencies should ensure that all requirements around protecting data in transit and at rest are well defined and included in contracts or SLAs, specifically for data backups and data in transit across untrusted networks.

4. **Access Controls**

   Ensure the identification, implementation and ongoing effectiveness of access controls is maintained. Specific policies for access control should be implemented based on business functions, processes, or user roles and responsibilities. User accounts should be managed through their lifecycle, ensuring that only the minimum required access rights are granted, preventing the assignment of excessive user permissions. Privileged access should be controlled through a formal authorisation process and implemented in accordance with the defined access control policy. Ensure the use of a robust password policy and implement multi-factor authentication where possible. IP whitelisting should be used to limit and control access to trusted users and locations only.

5. **User Awareness and Training**

   SA DaaS users should be provided with robust role-based training and have access to Standard Operating Procedures for essential tasks required by their role. All staff should also receive training in security practices to prevent social engineering attacks, ensure that unescorted visitors are challenged and that potential security incidents are detected and reported appropriately.

6. **Incident Management and Response**

   Effective incident management procedures are essential for the detection and resolution of security incidents. Response procedures should be formally documented, approved, and reviewed to be implemented and maintained effectively. Incident response training should be provided to staff, and response plans should be tested on a regular basis. Effective implementation of this risk will reduce the impact of security incidents, and the timeliness of resolution.

   The presence of adequate logging and regular monitoring of the DaaS environment can help the SA detect or investigate security incidents associated with DaaS should they occur. This includes enabling sufficient logging and monitoring on the DaaS infrastructure and virtual desktop applications.

## Service Provider Key Recommendations

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

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

2. **Use of Strong Encryption**
   SPs should ensure the use of strong encryption algorithms to protect data in transit and at rest in accordance with requirements defined in contracts or SLAs or in line with industry best practice.

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

4. **User Awareness and Training**
   DaaS SP users and third parties should be provided with robust role-based training and have access to Standard Operating Procedures for essential tasks required by their role. All staff should also receive training in security practices to prevent social engineering attacks, ensure that unescorted visitors are challenged and that potential security incidents are detected and reported appropriately.

5. **Configuration and Vulnerability Management of DaaS Virtualisation Platform**
   Change and vulnerability management procedures should be well defined and followed to ensure that the risks associated with misconfigurations and vulnerabilities that affect DaaS are addressed and mitigated, in particular to ensure muti-tenant segregation.

   A robust vulnerability management process should be followed. This includes regular vulnerability assessments, software patching and updating.

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

## Residual Risks

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

9(2)(k)

[redacted]

## Business Context

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

### Certification Approach

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

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

Subscribing agencies consuming the Risk Assessment must ensure that they:

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

### Stakeholders

The following stakeholders for DaaS have been identified:

- The DIA AoG SD team of the DPS branch;
- Subscribing Agency (SA) Business Owner; and
- SA Technical Owner.

### Information Classification

Based on the New Zealand Government Security Classification System[1], the information that will be stored, processed, or transmitted by the DaaS service has been classified Classification Removed and below. The compromise of information classified as Classification Removed and below can:

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

[1] https://www.protectivesecurity.govt.nz/information-security/classification-system-and-handling-requirements/classification-system/national-security-information/

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

## Business Processes Supported

DaaS delivers a managed virtual desktop environment for the use of New Zealand government agencies. DaaS enables agency staff to access their desktop operating system and desktop applications in a more efficient manner, as well as the flexibility for agencies to scale up or back service use and costs as required.

The DaaS service is integrated with the agency's existing IT infrastructure and delivered from within an approved government Infrastructure-as-a-Service (IaaS) datacentre.

## Business Impact

This section describes the business impact as it would apply to a SA should the confidentiality, integrity, availability, or privacy of the information stored, processed, or transmitted by the DaaS service be compromised.

Impacts may be different and unique for different SAs. Therefore, a SA must consider its own objectives and context when considering the consequences should a risk be realised.

## Security Requirements

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

### Confidentiality

The confidentiality of the information transmitted, stored, or processed by DaaS is considered as **4 – Highly-Important**. This is largely driven by the Classification Removed classification of information that will be transmitted, stored, or processed by DaaS.

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

- Classification Removed information is disclosed to unauthorised parties;
- The affected SA'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 DIA and other Lead Agency staff to solve the security incident.

## Integrity

The integrity of the information transmitted, stored, or processed by DaaS is considered as **4 – Highly-Important**. The DaaS information contained within its virtualised desktop environment must be stored and transmitted in a secure manner to prevent it from being modified by an unauthorised person. Inaccurate or corrupted information can cause the SA to lose their data source of truth. The SA is then unable to rely on the DaaS environment and this will affect business operations.

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

- Government decisions are misinformed;
- The affected SA's reputation is damaged;
- The strategic objectives of the New Zealand Government are compromised;
- Loss of confidence by the stakeholders and Portfolio Ministers;
- Increased workload for DIA and other Lead Agency staff to solve the security incident; and
- Increased workload for DIA and other Lead Agency staff to assess the accuracy of the information and provide corrective actions.

## Availability

The service availability requirement for DaaS is defined as 24/7 at 99.9% availability. If the availability of the DaaS service was compromised, the business impact would be **4 – Highly-Important**. 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 failback processes;
- Increased workload for DIA staff to solve the security incident; and
- Loss of confidence by the stakeholders.

## Privacy

Personally Identifiable Information (PII) may be included in the DaaS virtual desktop environment. It is highly important that the privacy of the information is adequately protected from unauthorised disclosure or modification during storage and in transit.

If the privacy of the DaaS service was compromised, the business impact will be **4 – Highly-Important**. The following consequences are expected:

- Disclosure of personal information to unauthorised parties, resulting in a privacy breach;
- Loss of key stakeholder confidence in DaaS service;
- Reputation damage for the affected SA; and
- Further investigation where required by law.

## Users

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

**Table 4 – User Groups & Descriptions**

| User Group | Description |
|---|---|
| New Zealand Government Agency Staff | Employees and contractors of the New Zealand government who require and are authorised to access virtualised desktop, laptop, and kiosk environments for the purposes of performing their day-to-day activities. |
| System Administrators | Employees and contractors associated with the DaaS solution provider, IaaS solution provider, and subscribed government agencies who perform system operational functions including software and platform management and patching. |
| Members of the Public | Users of DIA or other government agency kiosk PCs. |

## 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 DaaS.

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

- Public Records Act 2005;
- Official Information Act 1982;
- Privacy Act 2020;
- The New Zealand Government Protective Security Requirements (PSR)[2]; and
- New Zealand Information Security Manual (NZISM)[3].

## Information Protection Priorities

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

**Table 5 – Information Protection Priorities**

| Attribute | Priority Rating |
|---|---|
| **Confidentiality** | 4 – Highly Important |
| **Integrity** | 4 – Highly Important |
| **Availability** | 4 – Highly Important |
| **Privacy** | 4 – Highly Important |

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

**Table 6 – Information Protection Priority Scale**

| Priority Rating | Scoring |
|---|---|
| **Critical** | 5 |
| **Highly Important** | 4 |
| **Important** | 3 |
| **Some Importance** | 2 |

[2] https://www.protectivesecurity.govt.nz/

[3] https://www.nzism.gcsb.govt.nz/ism-document/

| Priority Rating | Scoring |
|---|---|
| **Unimportant** | 1 |
| **Not Applicable** | 0 |

## Detailed Risks

Table 7 presents the risks associated with use and operations of the DaaS Service. The Residual Risk Ratings do not consider additional controls or compensating controls as well as any additional Agency controls.

**Table 7 – DaaS Risks**

| Risk ID | Risk Description | 9(2)(k) [redacted] |
|---|---|---|
| R01 | **Desktop Service Outage due to Single point of Failure**<br>9(2)(k) [redacted] | [redacted] |

| Risk ID | Risk Description | 9(2)(k) [redacted] |
|---|---|---|
| R02 | **Supply Chain Risk**<br>9(2)(k) [redacted] | |
| R03 | **Weak Encryption of Data in Transit**<br>9(2)(k) [redacted] | |

| Risk ID | Risk Description | 9(2)(k) [redacted] |
|---|---|---|
| | 9(2)(k) [redacted] | |
| R04 | **Use of Non-AoG DaaS Provider**<br>9(2)(k) [redacted] | |

| Risk ID | Risk Description | 9(2)(k) |
|---|---|---|
| R05 | **Virtualisation Technology Vulnerabilities**<br>9(2)(k) | |
| R06 | **Insecure Virtual Desktops and Application Packaging**<br>9(2)(k) | |

| Risk ID | Risk Description | 9(2)(k) [redacted] |
|---|---|---|
| | 9(2)(k) [redacted] | [redacted] |
| R07 | **Incomplete Segregation of DaaS Management Networks**<br>9(2)(k) [redacted] | [redacted] |
| R08 | **Incomplete Segregation of DaaS SP Tenant Data**<br>9(2)(k) [redacted] | [redacted] |

| Risk ID | Risk Description | [redacted] |
|---|---|---|
| | 9(2)(k)<br>[redacted] | [redacted] |
| R09 | **Data Location and Third Party Access**<br>9(2)(k)<br>[redacted] | [redacted] |
| R10 | **Insecure SA End User Devices**<br>9(2)(k)<br>[redacted] | [redacted] |

| Risk ID | Risk Description | 9(2)(k) [redacted] |
|---|---|---|
| | 9(2)(k) [redacted] | |
| R11 | **Accidental Information Disclosure by DaaS Remote Access User**<br>9(2)(k) [redacted] | |

| Risk ID | Risk Description | 9(2)(k) [redacted] |
|---|---|---|
| R12 | **Inappropriate DaaS User Access Management**<br>9(2)(k) [redacted] | [redacted] |
| R13 | **Prolonged Desktop Service Outage due to Inadequate Data Backup and Recovery Procedures**<br>9(2)(k) [redacted] | [redacted] |

| Risk ID | Risk Description | 9(2)(k)<br>[redacted] |
|---|---|---|
| | 9(2)(k)<br>[redacted] | |
| **R14** | **Desktop Service Degradation or Outage due to Inadequate Network and Server Capacity Management**<br>9(2)(k)<br>[redacted] | |

| Risk ID | Risk Description | 9(2)(k) [redacted] |
|---|---|---|
| R15 | **DaaS Misconfiguration**<br>9(2)(k) [redacted] | [redacted] |
| R16 | **DaaS System Vulnerabilities**<br>9(2)(k) [redacted] | [redacted] |

| Risk ID | Risk Description | 9(2)(k) [redacted] |
|---|---|---|
| R17 | **Ineffective DaaS Security Incident Management due to Inadequate Logging and Monitoring**<br>9(2)(k) [redacted] | [redacted] |
| R18 | **Compromised DaaS User Credentials**<br>9(2)(k) [redacted] | [redacted] |

| Risk ID | Risk Description | 9(2)(k) [redacted] |
|---|---|---|
| | 9(2)(k) [redacted] | |
| **R19** | **Information Disclosure, Modification or Loss due to Insider Threat**<br>9(2)(k) [redacted] | |
| **R20** | **Desktop Service Outage due to Denial of Service (DoS) or Distributed Denial of Service (DDoS) Attacks**<br>9(2)(k) [redacted] | |

| Risk ID | Risk Description | 9(2)(k) [redacted] |
|---|---|---|
| | 9(2)(k) [redacted] | [redacted] |
| R21 | **Ineffective DaaS Security Incident Management due to Inadequate Incident Response Procedures**<br>9(2)(k) [redacted] | [redacted] |
| R22 | **Information Disclosure due to Insecure Data Backups**<br>9(2)(k) [redacted] | [redacted] |

| Risk ID | Risk Description | 9(2)(k) [redacted] |
|---|---|---|
| | 9(2)(k) [redacted] | [redacted] |
| R23 | **Information Disclosure, Modification, or Loss due to Insecure Facilities**<br>9(2)(k) [redacted] | [redacted] |
| R24 | **Disclosure of Information due to Incomplete Data Deletion**<br>9(2)(k) [redacted] | [redacted] |

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

## Controls Catalogue

Table 8 presents the recommended controls to effectively manage the risks recorded in use and operations of the DaaS Service. The Residual Risk Ratings do not consider additional controls or compensating controls as well as any additional Agency controls.

**Table 8 – Recommended Controls**

| Number | Title | Description | Reduces | NZISM Reference(s) v3.5 |
|---|---|---|---|---|
| **C01** | Contracts and SLAs | Contractual and Service Level Agreements are the only mechanisms that an organisation can use to ensure and enforce that a cloud-based and/or manage service will meet its requirements. Where a Service Provider retains direct control over ICT system operations, organisations need to ensure that contracts and associated SLAs:<br>• Clearly define the legal jurisdiction for contractual disputes relating to the use and function of the service;<br>• Clearly define the ownership of the data stored, processed and/or transmitted by the service;<br>• Define in which jurisdiction official information can and will be stored, processed and/or transmitted by the service;<br>• 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;<br>• Ensure that the time to return to full service after a failure or outage, including data restoration, meets the organisation's business continuity requirements;<br>• Require that all access to the organisation's information and systems be monitored;<br>• Require and specify means to notify to the organisation of any actual or possible unauthorised access;<br>• Require engagement with the organisation in resolution of any information access incidents or issues;<br>• Require regular reports be delivered from SP on their performance against the SLAs;<br>• 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;<br>• 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<br>• Ensure the contract with SP outlines clearly the services in scope and that the organisation is alerted when requiring services that are not within the scope. | Likelihood | 2.2.5.C.01<br>2.3.20.C.01<br>2.3.23<br>3.2.9<br>3.2.11<br>3.3.7<br>3.3.11<br>4.4.8<br>6.4<br>22.1<br>22.1.18 |
| **C02** | Due Diligence | Ensure that adequate due diligence is undertaken across the service, specifically:<br>• Defining the Information Security requirements of the service;<br>• Assessing whether the defined Information Security requirements are met by the service;<br>• Identifying and assessing any third–party dependencies that the service provider may have; and<br>• Ensuring third parties can meet New Zealand security requirements as contractor.<br>For higher handling requirements Agencies must ensure that assurance checks are conducted on cloud providers. | Likelihood | 2.2.4<br>4.4.8<br>12.7 |
| **C03** | Non–Disclosure and Confidentiality Agreements | Identifying, articulating, and regularly reviewing the organisation's requirements for confidentiality or non–disclosure agreements reflect 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. | Likelihood | 4.4.8.C.02<br>4.4.8.C.03 |
| **C04** | Risk Management | 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.<br>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. | Likelihood, Impact | 2.3.20.C.02<br>3.3<br>12.7.14<br>4.4<br>4.5<br>5.1.8<br>5.1.9<br>5.3<br>22.1.21<br>22.2.13 |

| Number | Title | Description | Reduces | NZISM Reference(s) v3.5 |
|---|---|---|---|---|
| **C05** | Human Resources Security | Documented Human Resource Security processes ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are employed. Some of the processes to be considered may include:<br>• Security vetting all new staff before beginning employment and on a regular basis thereafter;<br>• Undertaking an induction process that covers their responsibilities for Information Security;<br>• Acknowledging the Code of Conduct and Information Security policy;<br>• Acknowledging the employee's Terms and Conditions of Employment;<br>• Receiving regular security awareness training;<br>• Monitoring and management of changes in employee circumstances and behaviour; and<br>• Removing access rights when their employment or contract ceases. | Likelihood | 3.2<br>3.3<br>3.5<br>5.1.7<br>9.2<br>19.1.18<br>22.1.27 |
| **C06** | Security Vetting | Ensure that authorised users of a system or service are vetted by an approved vetting service such as that provided by the Ministry of Justice. Only appropriately, authorised, cleared, and briefed personnel are allowed access to the systems. | Likelihood | 3.5<br>9.2<br>9.4 |
| **C07** | Security Awareness Training | Ensure that all employees and contractors are provided with ongoing awareness training. Topics such as Information Security responsibilities (e.g., email security and using the internet), legislation and regulation, consequences of non–compliance with Information Security policies and procedures and potential security risks and counter measures should be covered. | Likelihood | 3.2<br>3.3<br>5.6.3.C.01<br>9.1<br>9.3<br>15.0<br>19.1.18<br>22.1.27 |
| **C08** | User Training | Ensure that all users of an information system are well trained in the correct use of the system to reduce the likelihood of inappropriate use or mistakes. | Likelihood | 3.2<br>9.1<br>22.1.27 |
| **C09** | Access Control | Ensure that users are only provided with access to the service that have been specifically authorised to use, including:<br>• 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<br>• 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<br>9.2<br>11.7<br>16.1<br>16.2<br>16.3<br>16.4<br>16.5<br>22.1.24<br>22.2.16 |
| **C10** | Separation of Duties | Ensure that all critical tasks that may be disrupted by human error or through malicious intent are designed in such a way that a single individual is unable to perform an action that results in such a disruption. | Likelihood, Impact | 16.2.6 |
| **C11** | Role Based Access Control | Ensure that access to the service is controlled based on the roles of the individuals requiring access. Role based access controls allows access to be quickly, easily, and uniformly granted, changed, or removed for groups of users, without having to update the privileges for each user. | Likelihood, Impact | 9.2<br>9.4<br>11.7<br>16.2.6<br>16.3 |
| **C12** | User Account Lifecycle Management | Ensure that user accounts are managed through their lifecycle process, including:<br>• Assigning access rights aligned with the defined access control policy;<br>• Reviewing access rights on a regular basis;<br>• Disable accounts when a user leaves an organisation;<br>• Disable accounts when a user no longer requires access; and<br>• Remove or update access rights (e.g., when a user change roles within an organisation). | Likelihood, Impact | 5.5.5<br>9.2.7<br>16.1<br>16.3 |

| 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<br>16.4.31.C.01<br>22.1.24 |
| **C14** | Password Policy | Ensure the use of a robust password policy including:<br>• Enforcing the use of individual user IDs and passwords to maintain accountability;<br>• Allowing users to select and change their own passwords;<br>• Enforcing a choice of quality passwords (what quality passwords are should be explained in the password policy), including minimum password length and complexity requirements;<br>• Forcing users to change their passwords at the first log–on or if reset; and<br>• Enforcing regular password changes (at least every 90 days) and as needed. | Likelihood | 16.1.40<br>16.1.41 |
| **C15** | Secure Password Distribution | Ensure that user passwords should be protected against unauthorised access when distributed initially. Distribution methods may include:<br>• Encrypted email;<br>• A secure password reset mechanism that positively authenticates the user (such as a challenge question or multifactor authentication);<br>• A text message to a verified mobile number; and<br>• A telephone call. | Likelihood | 16.1.40<br>16.1.41 |
| **C16** | Identity Management and Authentication | Identify management and authentication is the identification and authentication processes that verify the identity of a user or device. Secure authentication controls are implemented as physical or logical controls, and reduce the likelihood of unauthorised access to information, services, or systems in accordance with an access control policy. | Likelihood | 9.2.6<br>16.1<br>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:<br>• Something you know (e.g., username and password (one–time password (OTP) or reusable), personal identification number (PIN));<br>• Something you have (e.g., hardware or software token, digital certificate, smartcard); and<br>• Something you are (e.g., biometric fingerprint).<br>For higher handling requirements Agencies must ensure multifactor authentication is enabled. | Likelihood | 16.1.13<br>16.1.14<br>16.1.16<br>16.1.17<br>16.4.10<br>16.5<br>16.7<br>19.1.20<br>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 [redacted] with access and activities logged. Administrators should be issued with unique accounts that are different to the account used for daily activities such as email or web browsing.<br>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.<br>Ensure a backup, recovery and archiving plan is developed, implemented, and incorporated into the Disaster Recovery and Business Continuity plans. | Impact | 5.5.5<br>6.4<br>6.4.6<br>13.3.5<br>16.3.7<br>16.5<br>17.1.45<br>22.2.15.C.03<br>22.1.26 |

| Number | Title | Description | Reduces | NZISM Reference(s) v3.5 |
|---|---|---|---|---|
| **C20** | Logging and Auditing | Ensure that information systems are configured with adequate logging, archived, and retained for at least 18 months. Events to be logged includes:<br>- User login;<br>- All privileged operations;<br>- Failed attempts to elevate privileges;<br>- Security related system alerts and failures;<br>- System user and group additions, deletions, and modification to permissions;<br>- Unauthorised or failed access attempts to systems and files identified as critical to the Agency;<br>- Date and time of the event;<br>- Relevant system user(s) or processes;<br>- Event description;<br>- Success or failure of the event;<br>- Event source (e.g., application name); and<br>- IT equipment location/identification.<br>For higher handing requirements Agencies must ensure that logging and appropriate supporting processes are implemented. | Likelihood, Impact | 3.3<br>3.4<br>4.2.10<br>4.4<br>7.1<br>7.3<br>12.4<br>13.3.9.C.01<br>14.1<br>14.2<br>14.3<br>15.2<br>16.1.46<br>16.5<br>16.6<br>19.1.13.C.01<br>19.2<br>19.2.20<br>20.1.10.C.02<br>20.1.11.C.01<br>22.2 |
| **C21** | Security Incident and Event Management (SIEM) | Ensure that security related event logs are analysed regularly using automated security information and event management (SIEM) tools or equivalent to help identify anomalies. | Impact | 7.1 |
| **C22** | Information Security Incident Management | 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:<br>- Address clear definitions of the types of Information Security incidents are likely to be encountered and provide broad guidelines on what constitutes an Information Security incident;<br>- Information Security incident response and management training for all system users and administrators;<br>- Address authority responsible for initiating investigations of an Information Security incident;<br>- Detecting security incidents to minimise impacts;<br>- Reporting security incidents, assisting in documenting and understanding the risks and impacts; and<br>- Managing security incidents by identifying and implementing processes for incident analysis and selection of appropriate remediation. | Impact | 3.2<br>3.3<br>5.1.11<br>5.1.12<br>5.6<br>7.0<br>22.1.25 |
| **C23** | Cryptographic Policy and Key Management | Ensure that cryptographic keys are managed according to defined standards and procedures and protected against unauthorised access or destruction during their lifecycle, including creation, storage and protection, distribution, use, renewal, recovery, revocation, destruction.<br>Agencies must ensure they have complete visibility over all uses and access of their private keys when operating with cloud service providers (i.e., assured key management practices).<br>Agencies must be able to demonstrate that any third party holding, using, or managing Agencies private keys in order to ensure functionality of a service is not compromised, or to provide a greater level of assurance over the management and security of keys than an Agency itself may be able to provide, demonstrate (evidence-based) equitable credentials to that required of Agency staff or other government outsourced service providers.<br>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.<br>In cases where sole control of private keys (such as Hold Your Own Key [HYOK] approach) is impractical, Agencies must carefully consider the nature of information that they are entrusting to a cloud service provider, and the different threats, adversary motivations and mitigations that are applicable, in order to reduce the risk and information exposure.<br>For higher handling requirements Agencies must ensure they have sole control over associated cryptographic keys. | Likelihood | 17 |
| **C24** | Encryption of Data in Transit | Ensuring business [redacted] private, or otherwise classified information that flows over the public or untrusted network such as the Internet or internal networks is protected using approved cryptographic protocols, reduces the likelihood of information being disclosed to, or captured by, an unauthorised person.<br>For higher handling requirements Agencies must ensure that data is encrypted in transit. | Likelihood, Impact | 8.3.5<br>16.1.37<br>17.2<br>17.3<br>17.4<br>21.4.13.C.01<br>22.1.24.C.04 |

| Number | Title | Description | Reduces | NZISM Reference(s) v3.5 |
|---|---|---|---|---|
| **C25** | Encryption of Data at Rest | Ensuring business [redacted] private, or otherwise classified information stored on media is encrypted using approved encryption algorithms and protocols, reduces the likelihood of unauthorised disclosure.<br>For higher handling requirements Agencies must ensure that data is encrypted at rest. | Likelihood, Impact | 17.1<br>17.2<br>17.3<br>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.<br>This also involves ensuring environmental controls such as Air Conditioning, Uninterrupted Power Supplies (UPS), and fire suppression are in place to protect the facility.<br>For higher handling requirements Agencies must ensure appropriate physical security controls are in place. | Likelihood | 8.1<br>8.2<br>8.3<br>9.2<br>9.4<br>16.1.45.C.01<br>11.4.12<br>11.5.15<br>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:<br>• Ensuring IT equipment always reside in an appropriate class of secure room;<br>• Storing IT equipment during non–operational hours in an appropriate class of security container or lockable commercial cabinet;<br>• 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;<br>• Using IT equipment without non–volatile media as well as securing its volatile media;<br>• Using an encryption product to reduce the physical storage requirements of the non–volatile media as well as securing its volatile media; and<br>• 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<br>9.2<br>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.<br>Ensure that a policy and procedures is developed and implemented for the decommissioning and disposal of IT equipment, media, and other important assets.<br>For higher handling requirements Agencies must ensure they have a decommissioning process defined. | Likelihood | 11.7.35<br>12.6<br>13.1<br>13.4<br>13.5<br>13.6<br>22.1.26 |
| **C29** | Media Handling | Ensure that media containing information are protected against unauthorised access, misuse, or corruption. This includes classifying, labelling, and registering the media and clearly indicate the required handling instructions and level of protection to be applied. | Likelihood | 13.2<br>13.3 |
| **C30** | Documentation | Ensure that Information Security documentation is produced for systems, to support and demonstrate good governance. The following documents should be documented:<br>• Information Security Policies (SecPol) – setting the strategic direction for Information Security;<br>• Systems Architecture – illustrates the structural design of the system including any outsourced services;<br>• Security Risk Management Plans (SRMPs) – identifying security risks and appropriate treatment measures for systems;<br>• System Security Plans (SecPlan) – specifying the Information Security measures for systems;<br>• Standard Operating Procedures (SOPs) – ensuring security procedures are followed in an appropriate and repeatable manner;<br>• Incident Response Plans (IRPs) – outlining actions to take in response to an Information Security incident;<br>• Emergency Procedures – ensuring classified information and systems are secured before personnel evacuate a facility in the event of an emergency; and<br>• Independent Assurance Reports – provides assurance to System Owners, Certifiers, Practitioners and Accreditors and to assist system designers, enterprise, and security architects where assurance reviews cannot be directly undertaken on service providers. | Likelihood, Impact | 3.2<br>3.3<br>4.3.18<br>5.1<br>5.2<br>5.3<br>5.4<br>5.5<br>5.6<br>5.7<br>5.8<br>9.2.5 |

| Number | Title | Description | Reduces | NZISM Reference(s) v3.5 |
|---|---|---|---|---|
| **C31** | Change Management | Ensure that Information Security is an integral part of the change management process and incorporated into the organisation's IT governance and management activities. All changes to the configuration of a system should be documented and approved through a formal change control process. All changes should be reviewed whether successful or not. Examples of a system change includes:<br>• An upgrade to, or introduction of, IT equipment;<br>• An upgrade to, or introduction of, software;<br>• Environment or infrastructure change; and<br>• Major changes to access controls. | Likelihood | 3.3<br>6.3<br>16.3.5 |
| **C32** | Performance and Capacity Management | A Performance and Capacity Plan ensure that the service has adequate resources available to meet the agreed SLAs. It includes monitoring of the service and defining and implementing expected thresholds with automated alerts being generated when they are exceeded. Performance and capacity monitoring may also include periodic reports to ensure that SLAs and contractual agreements are being met. In addition, monitoring the performance and capacity of services and systems can provide early warning for potential security threats, as well as triggers when additional resources should be allocated to meet increased demands. | Likelihood, Impact | 3.2<br>3.3<br>12.7.19<br>22.1 |
| **C33** | Malware Protection | The installation of malware protection software on all endpoints and devices will reduce the likelihood of malicious code infecting the service. Configuring the protection to perform real–time checks for malware, automatically update its definition database, quarantine any infected files, and automatically alert System Administrator(s) will ensure any infection is managed. Additional controls that detect and/or prevent the use of known malicious websites may also be considered. | Likelihood, Impact | 14.1 |
| **C34** | Configuration Management | Configuration management is the process of controlling the configuration of the service's components to provide assurance that they have been deployed in accordance with the approved configuration and remain so throughout their lifecycle. It is used for establishing and maintaining consistency of a product's performance, functional and physical attributes with its requirements, design, and operational information throughout its life. Any changes to the system are proposed, evaluated, implemented, and documented using a standardized, systematic approach that ensures consistency, and proposed changes are evaluated in terms of their anticipated impact on the entire system. | Likelihood, Impact | 5.5<br>12.2<br>14.1<br>18.1<br>22.2.14 |
| **C35** | Release Management | A defined and implemented Release Management process will ensure software and firmware updates (including new releases) and configuration changes are deployed in a non–operational (e.g., development or test) environment prior to being deployed into production. It will also ensure that use cases, regression testing, and user acceptance testing is performed in line with the scope of the changes to the system. | Likelihood | 14.4.4 |
| **C36** | Patch and Vulnerability Management | Ensure that security patches are applied in a timely fashion to manage software and firmware corrections, vulnerabilities, and performance risks.<br>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.<br>For higher handling requirements Agencies must ensure that appropriate patching and maintenance of software is undertaken. | Likelihood | 6.2<br>12.4 |
| **C37** | System Hardening | Ensure standard operating environments (SOE) are hardened in order to minimise known vulnerabilities and attack vectors. Aligning with hardening standards (e.g., vendor guidelines or Centre for Internet Security [CIS] benchmark) limits the opportunity for a vulnerability in the service to be exploited. | Likelihood | 14.1<br>14.2 |
| **C38** | Security of Network Services | Ensure that network services (including those outsourced) are protected against malicious and accidental compromise by identifying and implementing appropriate security mechanisms and management processes. Means of securing network services include:<br>• Using structured Internet and network addressing and naming schemas (e.g., IPv4/6, DNS);<br>• Identifying and creating network trust domains based on business security requirements (e.g., Guest networks, user networks, etc.);<br>• Limiting access to network services and security domains (e.g., Management zones); and<br>• Protecting network records using secure protocols and cryptographic technologies (e.g., DNSSEC, secure routing). | Likelihood | 18.0 |
| **C39** | Intrusion Detection and Prevention | Intrusion Detection and Prevention monitors network and/or system activities for malicious activity. The main functions are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. They can be deployed in four ways:<br>• Network–Based Intrusion Prevention System (NIPS): monitors the entire network for suspicious traffic by analysing protocol activity;<br>• Wireless Intrusion Prevention Systems (WIPS): monitor a wireless network for suspicious traffic by analysing wireless networking protocols;<br>• 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<br>• 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.<br>For higher handing requirements Agencies must ensure that IDP/ IDS is implemented, along with appropriate supporting processes. | Likelihood, Impact | 3.2<br>3.3<br>7.1.7<br>8.3<br>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).<br>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<br>19.1.14<br>22.3 |

| Number | Title | Description | Reduces | NZISM Reference(s) v3.5 |
|---|---|---|---|---|
| **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:<br>• All changes must be tested in a non–operational environment before being transferred into the operational environment;<br>• Testing must not be done in operational environments;<br>• Rules for the transfer or installation of software into operational environments from non–operational environments;<br>• Users must have different accounts for operational and non–operational environments; and<br>• 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 [redacted] environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a firewall before granting access to internal systems.<br>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<br>14.4<br>14.5<br>18.1<br>19.1<br>19.3<br>19.5.26<br>21.1.5<br>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.<br>For higher handing requirements Agencies must ensure that Disaster Recovery plans cater for cloud-based services. | Impact | 3.2.17<br>3.3.12<br>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:<br>• Clustering;<br>• Load balancing;<br>• Network redundancy; and<br>• System redundancy. | Likelihood, Impact | 3.3<br>6.4.5 |
| **C47** | Information Security Review | Ensure Information Security reviews are conducted at least annually to maintain the security of systems and detect gaps and deficiencies, including:<br>• Identifying any changes to the business requirements or concept of operation for the subject of the review;<br>• Identifying and changes to the security risks faced by the subject of the review;<br>• Assessing the effectiveness of the existing countermeasures;<br>• Validating the implementation of controls and countermeasures; and<br>• Reporting on any changes necessary to maintain an effective security posture. | Likelihood | 3.2<br>4.1<br>4.2<br>4.3<br>4.4<br>4.5<br>6.1 |
| **C48** | Architecture and Design Review | Reviewing the architecture and design of the service ensures that it meets the functional and non–functional business requirements including adequate controls to protect the confidentiality, integrity and availability of information stored, processed, or transmitted by the service.<br>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.<br>Architecture and Design Reviews should be regularly conducted to verify that changes in the threat landscape and NZISM requirements are considered. | Likelihood, Impact | 4.3<br>5.1.8<br>6.1<br>14.2<br>14.3<br>14.4<br>14.5<br>18.1<br>19.1<br>19.3<br>21.4<br>22.2.14 |

| Number | Title | Description | Reduces | NZISM Reference(s) v3.5 |
|---|---|---|---|---|
| **C49** | Security Tests and Controls Audit | Ensure that information assurance activities such as controls audit and technical security assessments are conducted against systems to demonstrate that due consideration has been paid to risk, security, functionality, business requirements and as a fundamental part of information systems governance and assurance. The assurance activities should focus on validating whether:<br>• Security posture of the organisation has been incorporated into its system security design;<br>• Controls are correctly implemented and are performing as intended;<br>• Changes and modifications are reviewed for any impact or implications; and<br>• Effectiveness of Information Security measures for systems is periodically reviewed and validated.<br>Penetration tests (when allowed), also provide assurance that exploitable information system weaknesses are identified, controls are configured and enforced to protect against real world attack scenarios. | Likelihood | 3.3<br>4.1<br>4.2<br>4.3<br>6.1<br>6.2 |
| **C50** | Data Loss Prevention | Depending on the solution and the risk posture of information leakage, Data Loss Prevention (DLP) or Cloud Access Security Broker (CASB) technologies or and techniques are implemented to safeguard [redacted] or critical information from leaving the organisation. They operate by identifying unauthorised use and data exfiltration and take remedial action by monitoring, detecting, and blocking unauthorised attempts to exfiltrate data. For DLP to be effective, all data states (processing, transmission, and storage) are monitored.<br>• Agency managed and/or unmanaged devices with an ability of information upload in the cloud storage are proactively monitored to avoid accidental information disclosure in the cloud instance or on their personal cloud drives;<br>• Tools like DLP and CASB are installed on the endpoints and enabled with logging/monitoring to protect from security incidents of information disclosure;<br>• Data loss protection rules shall be configured in protection mode;<br>• Rules Shall be reviewed and modified on regular basis, and upon related security incident/breach; and<br>• Administrative access to these tools is [redacted] to authorised personal only. | Likelihood, Impact | 7.3.7<br>7.3.8<br>14.1.13.C.03<br>21.4.5<br>21.4.14.C.02<br>21.1.24 |
| **C51** | Application Security | Establishing rules for the development of software and systems will ensure that the developers use secure development practices such as those defined and documented by Microsoft and the Open Web Application Security Project (OWASP).<br>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).<br>By implementing an application proxy at web–based interfaces, the service will be protected against a wide range of Layer 3 – 7 attacks including DoS (e.g., SYN Flooding, Smurf, ICMP Ping Flood, Fraggle attacks), SQL Injection and Cross Site Scripting (XSS). Inspecting external traffic (inbound and outbound), messages and attachments for malicious content at the gateway will reduce the likelihood of malicious code entering the service. The content filter can be configured to quarantine any suspicious files and automatically alert the System Administrator(s) when malicious content is detected. It may also be configured to restrict the file types that can be transferred into and out of the Organisation's environment to only those that are required by the business. | Likelihood, Impact | 12.2<br>12.7.19<br>12.7.20<br>14.3<br>14.4<br>14.5<br>19.0<br>20.3 |
| **C52** | Data Management | Ensure data transfers are performed in accordance with the policy and processes and are approved by a trusted source.<br>All classified information that are stored within a database are labelled appropriately with protective markings and database files are protected from access that bypasses the database's normal access controls. | Likelihood, Impact | 20.0<br>22.1 |
| **C53** | Governance | Ensure an appropriate governance structure is in place for providing oversight to make sure that risks are adequately mitigated, and controls are implemented to mitigate risks. | Likelihood, Impact | 3.0<br>4.1<br>4.4<br>4.5<br>5.1<br>6.1<br>16.4<br>16.7<br>19.5<br>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<br>8.0<br>11.2.16.C.01<br>11.4<br>11.4.12<br>22.2.16.C.01 |
| **C55** | Billing and Resource Management | To develop and manage Information Security budget projections and resource allocations based on short–term and long–term goals and objectives. | Likelihood | 3.3<br>3.3.9.R.01 |
| **C56** | Location of IaaS Service | Services may be hosted inside or outside of New Zealand, and it may be possible to choose what locations Agencies can choose to house their services. If a SP has a global presence, data may transit, or be backed up in foreign datacentres which may not be transparent to CA.<br>Support services for services hosted in a country may be provided from another jurisdiction, which should be considered when purchasing IaaS services. | Impact | 22.1.22 |

| Number | Title | Description | Reduces | NZISM Reference(s) v3.5 |
|---|---|---|---|---|
| **C57** | Privacy Impact Assessment | To assess the privacy impacts of a project and where necessary (e.g., application, platform, database, a service, procedure), a privacy impact assessment (PIA) must be conducted in order to comply with Privacy Act's, the privacy of individuals, and assist in making decisions about how to mitigate and manage privacy risks. | Impact | 3.2<br>3.3<br>3.1.9.C.01<br>5<br>22.1.22 |
| **C58** | Dedicated Network Connectivity | Dedicated network connectivity, or dedicated private networks, allow customers to attach their networks to service providers directly. This allows them to bypass network providers through a direct connection physically and reduces capacity and internet routing issues. | Impact | 18.2<br>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:<br>• To identify the source of DoS, either internal or external;<br>• How to diagnose the incident or attack type and attack method; and<br>• How to minimise the effect of a DoS attack.<br>Ensure a Virtual Machine (VM) migration and decommissioning policy and related SOPs are in place. | Impact | 16.1.14<br>18.3<br>19.2<br>19.5<br>21.4<br>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.<br>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<br>22.3 |

9(2)(k)

[redacted]

9(2)(k)

[redacted]

# Appendix A – Consulted Agencies

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

**Table 10 – Consulted Agencies**

| Attendee | Role | Agency Name |
|---|---|---|
| Shaun Trewern | Enterprise Security Assurance Consultant, AoG SD | Department of Internal Affairs |

# Appendix B – Project Overview

## Scope

The Department of Internal Affairs (DIA), as Government Chief Digital Officer (GCDO) have written this Risk Assessment report and Controls Validation Plan (CVP) for service providers, for the use of Desktop-as-a-Service (DaaS) by Subscribing Agencies. The objective was to create a generic Risk Assessment and Controls Validation Plan (CVP) for the use of DaaS by Subscribing Agencies. The CVP has been detailed in the *GCDO Certification for Agencies Consuming DaaS*, within section *6.1 Controls Validation Plan.*

## Approach

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

- Consumption of documentation provided by DIA.
- Identification of risks and controls associated with the use of DaaS Services.
- Development of a Risk Assessment report in draft.
- Running workshops with Subscribing Agencies.
- Issuance of a final Risk Assessment report.

## Documents Referenced

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

- All of Government Cloud Computing: Information Security and Privacy Considerations April 2014.
- DaaS Risk Assessment Report, v1.1, 10/11/2016.

# Appendix C – Risk Assessment Guidelines

## Rating Risk

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

## Likelihood (Probability) Assessment

The qualitative scale used to assign a likelihood rating is presented in Table 11 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 11 – DIA Risk Likelihood Scale**

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

## Impact (Consequences) Assessment

The qualitative scale used to assign an impact rating is presented in Table 12. All impacts were analysed in a business context. The impact of risks includes a consideration of any possible knock–on effects of the consequences of the identified risks, including cascade and cumulative effects.

**Table 12 – GCDO All-of-Government Risk Consequence Guide**

| 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.<br>• The Government suffers severe negative reputational impact, and the Prime Minister loses confidence in the Minister and/or the Agency's senior management.<br>• Minister and Chief Executive need to be briefed and regularly updated.<br>• Media interest is sustained for a prolonged period (i.e., over a week) with major criticism levelled at the Minister and/or the Agency.<br>• The Agency breaches multiple laws, which leads to legal action by affected stakeholders.<br>• External/independent investigation is commissioned by the SSC, GCIO or OPC.<br>• The SSC and GCIO manage the communications and recovery. | • Loss of life.<br>• Major health and safety incident involving members of staff and/or members of the public.<br>• The injured party or parties suffer major injuries with long–term effects that leave them permanently affected.<br>• 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.<br>• Severe compromise of the strategic objectives of the NZ Government or other Agencies.<br>• Severe on–going impact on service delivery across NZ Government or multiple Agencies.<br>• Skills shortages severely affect the ability of the Agency to meet its objectives and goals.<br>• Staff work hours are increased by more than 50% (20 hours per week) for more than 30 days.<br>• 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.<br>• Impact cannot be managed without significant extra human resources.<br>• Yearly operating costs increase by more than 12%.<br>• One–time financial cost greater than $100,000. |
| 4 | **Significant** | • The Agency suffers significant political and/or reputational damage.<br>• Minister suffers reputational damage and loses confidence in the Agency's senior management.<br>• Minister and Chief Executive need to be briefed and regularly updated.<br>• Media interest is sustained for up to a week with minor criticism levelled at the Agency.<br>• Key stakeholders need to be informed and kept up to date with any developments that affect them.<br>• The Agency breaches the law, which leads to legal action by affected stakeholders.<br>• External/independent investigation is commissioned by the SSC, GCIO or OPC.<br>• Communications and recovery can be managed internally with strong guidance from the SSC and GCIO. | • A significant health and safety incident involving multiple members of staff and/or members of the public.<br>• The injured party or parties suffer significant injuries with long–term effects that leave them permanently affected.<br>• 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.<br>• Compromise of the strategic objectives of the NZ Government or other Agencies<br>• Significant on–going impact on service delivery across one or more business unit or multiple Agencies.<br>• Skills shortages affect the ability of the Agency to meet its objectives and goals.<br>• Staff work hours are increased by more than 38% (10 – 15 hours per week) for 30 days.<br>• 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.<br>• Impact cannot be managed without extra financial and human resources.<br>• Yearly operating costs increase by 10% to 12%.<br>• One–time financial cost between $50,000 and $100,000. |
| 3 | **Moderate** | • Agency suffers limited political and/or reputation damage.<br>• Minister is informed and may request to be briefed.<br>• The Chief Executive and senior management need to be briefed and regularly updated.<br>• The Agency breaches its compliance obligations.<br>• Media interest is sustained for less than a week with minor criticism levelled at the Agency.<br>• Key stakeholders need to be informed and kept up to date with any developments that affect them.<br>• External/independent investigation is commissioned by the Agency.<br>• Most communications and recovery can be managed internally with some guidance from the GCIO. | • Health and safety incident involving multiple members of staff or one or more members of the public.<br>• The injured party or parties suffer injuries with long–term effects and are not permanently affected.<br>• The Agency's safety practices are questioned and found to be inadequate. | • Compromise of the strategic objectives and goals of the Agency.<br>• Moderate impact on service delivery across one or more business unit due to prolonged service failure.<br>• Staff work hours are increased by less than 25% (8 – 10 hours per week) for a two–to–four–week period.<br>• 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.<br>• Yearly operating costs increase by 7% to 10%.<br>• 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.<br>• The Chief Executive needs to be advised.<br>• Senior management needs to be briefed.<br>• Media interest is short lived (i.e., a couple of days) and no blame is directed at the Agency.<br>• Key stakeholders need to be informed.<br>• Communications and recovery can be managed internally. | • Minor health and safety incident involving multiple members of staff or a member of the public.<br>• 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.<br>• Limited effect on the outcomes and/or objectives of more than one business unit.<br>• Staff work hours are increased by less than 15% (6 hours per week) for less than two weeks.<br>• 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.<br>• Increase of between 5% and 7% in yearly operating costs.<br>• One–time financial cost between $10,000 and $20,000. |
| 1 | **Minimal** | • Reputation is not affected.<br>• No questions from the Minister.<br>• No media attention.<br>• All communications and recovery can be managed internally. | • No loss or significant threat to health or life.<br>• 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.<br>• Staff work hours are increased by less than 5% (1 – 2 hours per week) for less than seven days.<br>• No increase in staff turnover as a result of the risk eventuating. | • Impact can be managed within current resources, with no re–planning.<br>• Increase of less than 5% in yearly operating costs.<br>• One–time financial cost of less than $10,000. |

Table 13 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 13 – Risk Matrix**

| Impact | Almost Never | Possible but Unlikely | Possible | Highly Probable | Almost Certain |
|---|---|---|---|---|---|
| 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 |

Likelihood

## Escalation of Risk

Table 14 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 14 – Risk Escalation and Reporting**

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

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

GCDO/GCSB guidance on Security Controls for Hosted Offshore Office Productivity Services[4] identifies baseline controls that Agencies needs to address to ensure compliance of relevant controls from the NZISM. Although not specifically targeted at addressing DaaS services, the controls identified in this document are directly applicable where Agencies need to address higher levels of handling requirements (i.e., Classification Removed ). Where appropriate, the controls below have been incorporated into this Risk Assessment to maintain alignment.

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

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

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