ICT Shared Capabilities Marketplace Payroll Enterprise Software Provider Hosted

Security Risk Assessment Report

Issued by

Digital Public Services Branch

Te Tari Taiwhenua
Internal Affairs

Te Kāwanatanga o Aotearoa
New Zealand Government

Document Control

Document Name	Payroll Enterprise Software Security Risk Assessment
Author	9(2)(a) Director and Security Consultant, SafeStack
Title	ICT Shared Capabilities Marketplace – Payroll Enterprise Software - Security Risk Assessment
File name	ICT Shared Capabilities Marketplace – Payroll Enterprise Software – Security Risk Assessment Report.docx
Version	v1.5 dated 29 April 2022
Document Number	MKP.PES.RA.2022.050

Confidentiality

The information contained in this document is proprietary to the Department of Internal Affairs. This document must not be used, reproduced, or disclosed to others except employees of the recipient of this document who have the need to know for the purposes of this assignment. Prior to such disclosure, the recipient of this document must obtain the agreement of such employees or other parties to receive and use such information as proprietary and confidential and subject to non-disclosure on the same conditions as set out above.

The recipient by retaining and using this document agrees to the above restrictions and shall protect the document and information contained in it from loss, theft, and misuse.

Revision History

Version	Date	Author	Description of Change
0.1	12/07/2021	9(2)(a)	Initial draft.
0.2	21/07/2021	9(2)(a)	Updated with feedback from Mae Koh (Enterprise Security Assurance Consultant, AoG Services Delivery).
1.0	24/08/2021	9(2)(a)	Updated with feedback from consulted agencies and suppliers (refer to Appendix A), and internal quality assurance. Release to AoG SD for review and sign-off.
1.1	8/12/2021	Mae Koh	Comments provided by AoG SD.
1.2	9/12/2021	9(2)(a)	Comments addressed.
1.3	12/01/2022	Mae Koh	Minor updates.
1.4	02/03/2022	9(2)(a)	Updated to ensure consistent with revised certification process.
1.5	29/3/2022	Mae Koh	Formatting updates.

Document Approval

I approve this Risk Assessment report; it presents the information security risks introduced to Consuming Agencies using Marketplace Payroll Enterprise Software.

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

Name and Role	Signature	Date
Jane Kennedy General Manager AoG Service Delivery Digital Public Service Branch Department of Internal Affairs Te Tari Taiwhenua	Signed on Original	20/5/22

I acknowledge that this Risk Assessment has been completed in accordance with the Digital Public Services Branch's information security Risk Assessment process.

Name and Role	Signature	Date
Katrina Banks Manager Security AoG Service Delivery, Digital Public Service Branch Department of Internal Affairs Te Tari Taiwhenua	Signed on Original	13 May 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.
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.
Probability	The chance of an event occurring.
Recovery Point Objective (RPO)	The earliest point time that is acceptable to recover data from. The RPO effectively specifies the amount of data loss that is acceptable to the business.
Recovery Time Objective (RTO)	The amount of time allowed for the recovery of an information system or service after a disaster event has occurred. The RTO effectively specifies the amount of time that is acceptable to the business to be without the system.
Residual Risk	The risk remaining after the risk treatment has been applied.
Risk	The effect of uncertainty on the business objectives. The effect can be positive or negative. However, in the context of information security it is usually negative.
Risk Appetite	The amount of risk that the organisation is willing to accept in pursuit of its objectives.
Risk Owner	A person or entity with the accountability and authority to manage a risk. Usually, the business owner of the information system or service.
Stakeholder	A person or organisation that can affect, be affected by, or perceive themselves to be affected by a risk eventuating.
Threat	A potential cause of a risk.
Vulnerability	A weakness in an information system or service that can be exploited by a threat.

Contents

Executive Summary

Introduction

Payroll is a large, important, and complex part of an agency. To effectively run payroll services, the software used must integrate with many different systems. All these systems combined perform key business functions ranging from payroll, time and attendance, award interpretation, rostering, human resources, workforce management, self-service, and data management.

In the Marketplace, Payroll itself is made up of two channels:

- Managed Services, which includes both software and a range of associated business and supporting services; and
- Enterprise Software, which includes the software.

The Marketplace Payroll Enterprise Software catalogue includes both provider-hosted (or Software-as-a-Service, SaaS) and agency-hosted products.

This report includes the findings for the information security Risk Assessment for a provider-hosted Payroll Enterprise Software product used by Consuming Agencies (CAs). There will be multiple suppliers (or Providers) that will provide this product, and each CA will have their own unique context and risk appetite. Therefore, this report contains generic findings and the intent is that each CA will review them using their own risk management framework. This Risk Assessment also only considers the context that the data stored, transmitted, or processed by these products is classified as IN-CONFIDENCE or lower. If a CA stores, transmits, or processes data with a higher classification, they will need to re-assess these risks using their own information classification policy and risk management framework.

The details of the Marketplace structure and security risk assurance framework can be found in Appendix B.

The Risk Assessment performed 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.

9(2)(k)

9(2)(k)

9(2)(k)

Gross Risk Position

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

Table 1 – Gross Risk Ratings

9(2)(k)

Key Recommendations

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

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

1. **Provider and Vendor Due Diligence**
   The CA will be unable to control how the Provider manages the components of the software that are outside of the CA's control. The Provider is also unlikely to share any details about how they secure or manage those components as this is confidential information for a likely multi-tenancy environment. If the information were used against the Provider, it could result in risk events that affect more of their customers than just the CA.

   Although the CA will not be able to perform a full audit of the software, they can obtain information on what controls the software does provide and if the CA can use those controls to manage their own risks. For example, an important control for the CA to configure is role-based (and organisation-based for multi-agency payroll) access controls. If the Provider and software does not provide enough granular levels of configurations, it will not be possible for the CA to implement this control which would lead to higher risks.

   For the controls listed in this report and the CVP, the CA should verify which controls are available to be configured (which can be verified by the Provider) before attempting to implement the controls themselves. This includes controls such as: role-based access controls, organisation-based access controls, separation of duties, least privilege, logging and auditing, information and security incident management, data backups, encryption in-transit, identity management, and unused features.

2. **Access Management and Controls**
   There are high risks related to the misconfiguration by CA users or unauthorised access to CA user accounts. These risk events can lead to various impacts due to the value of data in the system. One of the most important set of controls for the CA to implement will be strong access management and controls.

   This includes controlling how users authenticate to reduce the likelihood of someone gaining unauthorised access to an account. It also includes making sure there are granular enough roles and permissions so the CA can properly separate responsibilities and follow the principle of least privilege.

3. **Logging and Incident Response**
   Since the higher risks faced by a CA are related to misconfiguration or unauthorised access, it will be important to have detective controls in place in the event the access controls (preventative controls) fail.

   Logging and auditing will depend on what is available from the Provider and the software, and will be a critical detection point for CA. These detection points will need to then feed into a security

incident management process. That way if risk events do occur, the CA can respond quickly and effectively to minimise the impact.

4. Additional Assessments

This Risk Assessment is expected to cover most of the use cases for a CA that wishes to use Provider-hosted payroll software. However, there will be a few edge cases that might apply that can have large impacts to security risk. This includes edge cases related to:

- Initial migration from the previous payroll system;
- Overseas legislation;
- Use or storage of Classification Removed data; and
- Limitations of software hosted overseas (i.e., jurisdictional, performance, operational risks).

A CA should consider if these edge cases apply to their context and perform additional risk or assessment work to fully understand how this context affects these risks.

Residual Risk Positions

Table 2 below illustrates the expected residual rating of each of the risks if all the recommended Provider controls are implemented and appropriately configured and managed.

Table 2 – Provider Residual Risk Ratings

9(2)(k)

Table 3 below illustrates the expected residual rating of each of the risks if all the recommended Consuming Agency controls are implemented and appropriately configured and managed.

Table 3 – Consuming Agency Residual Risk Ratings

9(2)(k)

Business Context

This section provides an overview of the generic business context for the Payroll Enterprise Software (Provider-hosted) products that are in scope of this generic information security Risk Assessment.

9(2)(k)

9(2)(k)

Pre-payroll Services Processes

Recording of pay data involves many factors:

- Salary or rostered wages;
- Schedules or work patterns (default, or custom); and
- Pay rules (award interpretation, or deductions and allowances).

Salary

Salaried employees have a pattern set in their work profiles that determines how pay is calculated, and this would be configured and set in the payroll system. There is a default pattern that represents a common, standard salaried employee (such as Monday to Friday, 8AM to 4PM).

This pattern can be changed and is often happens due to different pattern terms in the salaried employee's individual agreement or collective agreement, change in part-time or full-time status.

Rostering / Time and Attendance

Payees paid according to a roster can be full-time, part-time, or casual employees. If a payee is on rostered wages, the time that they are paid for is based on either rostering (hours recorded in *advance*) or a time and attendance (hours recorded *already worked*). Either could be performed:

- Manually, such as using spreadsheets and entering data into a system; or

- Using a system, either within a separate rostering system or within the payroll software (as an add-on feature).

There are common controls and processes followed to confirm the integrity of the hours before the payroll process kicks off:

- Default schedules and configurations – These are set in the rostering or time and attendance systems, and make sure the pay is correct and complies with the Holidays Act;
- Approval flows – Hours recorded would go through an approval flow and the approvers required would depend on either: delegation matrix, collective agreement, individual agreements, or multi-employer agreements; and
- Data integrity reports – These can be run in the payroll systems to confirm the pay calculated is accurate, complete, and reliable.

Pay Rules

Last part of recording pay correctly involves pay rules and this involves considering any award interpretation, allowances, and deductions that might apply to a specific payee.

Award interpretation involves the translation of worked hours into a paid value based off rules and regulatory requirements set in the system. This can include allowances, overtime, and penalties. The rules and requirements are configured in either:

- The separate rostering systems; or
- Within the payroll software (as an add-on feature)

Common deductions that need to be configured before payroll is run includes:

- Employment or contract status;
- Salary sacrifice (or a donation of part of their salary to a charity);
- Kiwisaver or superannuation contributions;
- Inland Revenue Department or Ministry of Justice fines;
- Student loan payments;
- Any other changes agreed (such as overpayments, payment of leave up-front); and
- Payroll tax.

Payroll Processes

The payroll process for each CA will vary, but there are some common steps taken including:

- Data integrity reporting and validation;
- Trial pay runs;
- Calculation of pay;
- Final pay run and generation of pay, bank, and other third-party files; and
- Repeat of process for multiple pay runs (i.e. multi-agency payroll).

Pay Calculations

Pay calculation may start off with the data that is imported in from other systems (9(2)(k) 9(2)(k) r it will start off with data based off the profile and rules that the payee is set up with in the payroll system.

These calculations are consistent across agencies due to required compliance with the Holidays Act, however they still need to be configured within the system. The CA can alternatively follow the

common process model, which helps the CA make sure the payroll rules configured meet good practice and legislative requirements.

Pay Runs

A CA may administer multiple pay runs before pay is finalised. It may involve a trial run, which checks if the CA is under or overpaying. Multiple checks take place including checking number of payees compared to number of employees, comparing of pay data to previous pay runs. These results are also needed for audit evidence.

When the final run is administered, multiple files will be generated and may include (but is not limited to):

- Bank files – which are transferred to the CA's bank for payment to payees;
- IRD files – which are transferred to IRD for tax and other compliance;
- Payees pay information – which includes a summary of their pay, allowances, and deductions;
- 3rd party files – for uploading of pay data into other systems the CA may use (such as financial management or accounting systems), or to other 3rd parties that deductions were made for (such as Ministry of Justice); and
- Union files – which includes a summary of union fees that have been paid.

These files may be manually transferred (by manually uploading the files to the other system) or there may be an integration or file transfer system used by the CA.

For CA that look after multiple agencies' payroll, this process would repeat for each agency they look after.

Post-payroll and Ongoing Processes

After the payroll run is complete, a CA will perform:

- Accounting and recording of the pay run; and
- Reporting and sharing of reports with groups within the CA or agencies they administer payroll for.

There will also be ongoing services that take place outside of the payroll run, such as:

- Software data management (such as configuration management of profiles, pay rules, and other payroll-related configurations, access management, and data management);
- Integration management (such as Rostering, Time and Attendance, HR, and bank system integration);
- Identity Provider integration (for authentication to the system);
- Software, infrastructure, and hardware management (which in the scope of this report is managed by the SaaS Provider); or
- Supporting procedural controls (such as incident response, disaster recovery, and business continuity).

Information Classification

The security classification of the information that will be stored, processed, or transmitted by the payroll software has been evaluated as IN-CONFIDENCE and below. This is because while the payroll

software and business processes contain personal information, this data would not cause an impact to diplomatic, economic wellbeing, safety, or operational effectiveness of New Zealand.

There is a risk that the payroll software may store Classification Remove information. The most common situations include:

- Data or documents uploaded related to leave taken that involves domestic violence, vulnerable children, or health information.

If CAs wish to consume the software for information classified to Classification Removed CAs will need to comply and confirm with controls detailed in the Protective Security Requirements (PSR).

Users and Stakeholders

Based off the business processes outlined above, a CA may have the following users or stakeholders involved:

User or Stakeholder Group	Description
Consuming Agency	
Payroll Administrators	CA users with access to the software to administer their payroll function. These users may have different roles based off the role structure within the system and their role in the payroll process.
Super Administrators	CA users with privileged access to the software that can make [redacted] changes (such as user, roles, configuration, or data changes).
Managers	CA users that are Managers and have access to approve requests and changes.
Employees or Payees	CA users with access to view their data, make changes to their bank or other details, and request leave.
Other System User Groups	CA will have other teams outside the payroll function that are key stakeholders, including the HR, Accounting and Finance, and Reporting teams.
SaaS Provider	
Administrators	Provider staff with privileged access to the software and underlying infrastructure. Responsible for managing the supporting infrastructure and systems that support the SaaS system.
Managed Service Provider or Other Third Parties	
Outsourced Administrators	CAs may have a Managed Service Provider who is responsible for either: • The payroll function and business processes; • Administrative management of the payroll software; or • Both. The Managed Service Provider may also act as just an escalation point and provide support only for higher-level issues. For example, a low-priority or 1st level request for administrative management may be taken care of by the CA. Any escalation would be sent to a Managed Service Provider (who may have specialised software experience).
Other Agencies	CAs may look after and administer payroll on behalf of other agencies, and they would be key stakeholders to this payroll function.
Third parties	The CA will have to file, report, and work with multiple third parties as part of this process, including: • CA's bank; • Inland Revenue Department; and • Agencies or groups that collect deduction payments (such as Ministry of Justice).

Legislation, Policy, and Guidelines

CA must ensure that they can demonstrate compliance with applicable legislation, policies, guidelines, and any other external requirements when using payroll software.

The following legislation, policy, and guidelines relate specifically to security requirements are considered relevant to most CAs:

- Protective Security Requirements (PSR); and
- New Zealand Information Security Manual (NZISM v3.4).

The following legislation, policy, and guidelines relate different aspects to the payroll function or the business processes they support:

- Holidays Act 2003;
- Privacy Act 2020;
- Employment Protection Act 1987;
- Public Records Act 2005;
- Official Information Act 1982;
- KiwiSaver Act 2006;
- Accident Compensation Act 2001;
- Child Support Act 1991;
- Datacom GSF Specifications;
- Domestic Violence Amendment;
- Employment Relations Act 2000;
- Equal Pay Act 1972;
- General Disposals Authority 6;
- Health and Safety at Work;
- Home and Community Support (Payment for Travel Between Clients) Settlement Act 2016;
- Human Rights Act 1993;
- Income Tax Act 2007;
- Live Organ Donors Act 2016;
- Minimum Wage Act 1983;
- Parental Leave and Employment Protection Act 1987;
- Public Finance Act 1989;
- Student Loan Scheme Act 2011;
- Support Workers (Pay Equity) Settlements Act 2017;
- Tax Administration (Correction of Errors in Employment Income Information) Regulations 2019;
- Tax Administration Act 1994;
- Volunteers Employment Protection Act 1973; and
- Wages Protection Act 1983.

Some CA may provide payroll services to payees who must comply with overseas legislation. There will be different requirements and impacts if these are not followed and were not considered in the context of this work. The CA should perform their own assessment when understanding their specific requirements under any legislation.

9(2)(k)

9(2)(k)

Service Owner and Experts

Each CA will have to use this Risk Assessment and apply it to the specific Provider and payroll software solution they selected from the Marketplace, and to their own internal risk framework and context. As part of that, the CA can get support from the following stakeholders:

- Senior Responsible Officer – or the officer responsible for the use and risk of the software in their agency;
- IT Security Manager – or the manager responsible for performing security assurance for the system;
- Solution Architect – or the architect responsible for identifying the technical components and features in the Provider and software chosen; and

- Payroll and other subject matter experts – or others in the CA who can assist with adjusting this Risk Assessment in the context of how the system will be used within the CA.

Security Requirements

The security requirements help inform the technical impact of the security risks captured, and the requirements vary based off the confidentiality, integrity, availability, and privacy requirements of the data used by the payroll system.

The exact security requirements will vary by CA and will require the CA to assess using their framework. In most cases, the impacts across CA will be similar. Those impacts have been defined below:

Confidentiality and Privacy

The payroll system will store, process, and transmit information that includes Personally Identifiable Information (PII), and limited Classification Removed information that may be included in their leave, allowance, and deduction requests. This information is considered IN-CONFIDENCE.

There are different ways this information's confidentiality or privacy could be compromised: an administrative or system user could accidently or intentionally share data exports, pay files, or reports; the system could be mis-configured which would allow other system users to see data they shouldn't be allowed to see; a CA's account could be inappropriately accessed leading to a data breach; the Provider could have a security incident relating to their staff or the system which leads to a data breach.

The impact of a confidentiality or privacy incident would vary, and it would depend on the amount of information involved. If there was a small amount of information involved, the impact to the CA would be **moderate**. If there was a large of amount of information, the impact would be **significant**. It could result in:

- Breach of laws, resulting in litigation and against the CA (and other agencies they provide payroll services for);
- Significant reputational and political damage;
- Loss of confidence in the security of the software;
- Significant ongoing operational and service delivery impact to the CA due to incident investigation and process changes;
- Significant financial impact due to the need for additional resources to assist with the investigation and resolve any issues, and for any litigation fees; and
- Minister and leadership briefing and updates.

Integrity

The payroll system is a key component of the overall payroll function within a CA. They rely on the accuracy and integrity of the data in the system for payroll processes as well as supporting business processing (such as financial reporting and HR).

There are different ways the information's integrity could be compromised, and most of those events come down to access controls (including user access and data separation). The impact would also vary and would depend on the amount of information that was modified. If there was a small amount of information involved, the impact to the CA would be **moderate**. If there was a large of amount of information, the impact would be **significant**. It could result in:

- Breach of laws (such as Holidays Act due to incorrectly calculated pay)
- Significant reputational and political damage;
- Loss of confidence in the security of the software;
- Significant ongoing operational and service delivery impact to the CA due to incident investigation and process changes;
- Moderate financial impact due to the need for additional resources to assist with the investigation and resolve any issues, and for any litigation fees; and
- Minister and leadership briefing and updates.

Availability

Payroll is a regularly occurring process and is heavily relied on by multiple stakeholders (as captured above under Users and Stakeholders).

There are different ways the availability of the system or the information could be compromised. It could be unavailable for a short period of time due to a breaking change or misconfiguration, or it could be unavailable for an extended period due to a prolonged Distributed Denial of Service (DDoS), Denial of Service (DoS), or security incident with the payroll software and Provider.

If the system were unavailable outside of the pay run part of the process (less busy period), the impact would be **moderate**. If the system were unavailable during the pay run part of the process, the impact would be **significant**. It could result in:

- The CA standing up an incident response or business continuity team to administer the pay run without the payroll software;
- Increased operational and service delivery impacts due to manual processing and post-incident system updates;
- Significant reputational and political damage;
- Financial impact due to additional resources needed to administer manual pay runs; or
- Leadership and Minister briefing and updates.

Information Protection Priorities

Information protection priorities allow CA to know how they should prioritise their security risks and control decisions. The security requirements captured below are specifically for payroll software and does not consider the requirements of the wider payroll function or organisational functions. This is a single, system view rather than a holistic organisational view.

Based on the security requirements above, the priorities are:

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

The scale used for this rating system is:

Priority Rating	Scoring
Critical	5
Highly Important	4
Important	3
Some Importance	2
Unimportant	1
Not Applicable	0

Out-of-Scope

The following items are out of scope of this Risk Assessment:

- Risks relating to agency-hosted Enterprise Payroll Software,
- Risks relating to Managed Services, including:
  - Administering the payroll function; and
  - Management of the CA's tenancy.
- Risks related to the implementation or onboarding of this service and software, and
- Detailed risks related to any public or private cloud hosting infrastructure or platform.

9(2)(k)

Table 4 – Risk Assessment

Risk ID	Risk Description
1. Security risks affecting the **payroll process configurations and data**	
R01	**A <u>CA user misconfigures the system</u> which impacts the integrity of the payroll function.** 9(2)(k)
R02	**A <u>Provider user misconfigures the system</u> which impacts the integrity of the payroll function.** 9(2)(k)

9(2)(k)

Risk ID	Risk Description
2. Security risks affecting the **tenancy configurations**	
R03	**The CA users are <u>not properly setup or maintained</u> which leads to a data leak, misconfiguration incidents, or financial loss.** 9(2)(k)
R04	**A <u>CA user misconfigures the system</u> which impacts the security of the system.** 9(2)(k)

9(2)(k)

Risk ID	Risk Description	9(2)(k)
R05	**A Provider user misconfigures the system which impacts the security of the system.** 9(2)(k)	
R06	**A CA user account is inappropriately accessed which leads to a data breach or misconfiguration incidents.** 9(2)(k)	

Risk ID	Risk Description
R07	**An integration with another CA system is not secured which leads to a data leak.** 9(2)(k)
R08	**An integration with a third-party system is not secured which leads to a data leak.** 9(2)(k)

Risk ID	Risk Description	9(2)(k)
R09	**Data sent to the payroll software via other system integrations is compromised which leads to an integrity incident.** 9(2)(k)	
3. Security risks affecting the **application configurations, system code, system components, or supporting infrastructure**		
R10	**A Provider user account is inappropriately accessed which leads to a data breach or misconfiguration incidents.** 9(2)(k)	9(2)(k)

Risk ID	Risk Description	9(2)(k)
R11	**The software or the supporting infrastructure has a vulnerability which leads to a data leak.** 9(2)(k)	
R12	**The system is unavailable due to an availability attack or a Provider mistake.** 9(2)(k)	
R13	**The Provider shuts down the product and the CA is unable to access the software.** 9(2)(k)	

Risk ID	Risk Description	9(2)(k)
R26	**The Provider has a physical security breach which leads to data loss or availability issues.** 9(2)(k)	
4. Security risks affecting **other aspects of the software (i.e. migration to new software, privacy, legislative risks)**		
R14	**The software has communication or file hosting features that can be misused and used to carry out social engineering or malware related attacks.** 9(2)(k)	9(2)(k)

Risk ID	Risk Description	9(2)(k)
R15	**The software is hosted overseas which can lead to performance, operational, and jurisdictional impacts.** 9(2)(k)	
R16	**Data is lost, modified, or destroyed when migrating to the new software.** 9(2)(k)	

Risk ID	Risk Description	9(2)(k)
R17	**Data is exported from the system and is therefore no longer protected by the security controls of the software.** 9(2)(k)	
R18	Classification Remo**data is entered into the software which can cause the technical and business impact of any other risk event to be higher.** 9(2)(k)	
R19	**A CA fails to comply with overseas legislation due to a misconfiguration, data leak, or other security event.** 9(2)(k)	
R20	**A CA has a different operating model which means this assessment might not accurately capture their risks and recommended controls.** 9(2)(k)	

Risk ID	Risk Description
R21	**A remote working user does not secure their device which leads to a data leak.** 9(2)(k)
R22	**A system that the Provider relies on has a breach which affects the CA and their data.** 9(2)(k)
5. Security risks affecting CA that administer **multi-agency payroll**	
R23	**A CA is onboarded a new agency to their payroll function and incorrectly imports the data or configured the agency's user access.** 9(2)(k)

9(2)(k)

Risk ID	Risk Description
R24	**An agency user is not properly setup which leads to the new user getting the wrong access and causing a data leak or misconfiguration incident.** 9(2)(k)
R25	**An agency user misconfigures or modifies the data in the payroll software which impacts the CA's ability to administer their payroll.** 9(2)(k)

9(2)(k)

Controls Catalogue

Table 5 presents the recommended controls to effectively manage the risks recorded in Table 4.

Table 5 – Recommended Controls

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
C01	Contracts and SLAs	Ensure that contracts and associated Service Level Agreements (SLAs) with the Provider: • 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 and have defined 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 the Provider's environment, including backups and other environmental copies; • Ensure that full service and 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 the Provider 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 the Provider 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 are alerted when requiring services that are not within the scope or when services are shutdown.	Likelihood	2.2 3.2 3.3 4.4.8 22.1
C07	Security Awareness Training	Ensure that all employees and contractors are provided with ongoing awareness training. Topics such as information security responsibilities, legislation and regulation, consequences of non-compliance with information security policies and procedures and potential security risks and counter measures should be covered.	Likelihood	9.1 9.4 22.1.17
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. Users are also award of the system classification, and what data should not be stored (i.e. [redacted] personal information). This especially applies to users who have privileged access, which includes users who can: • Change or delete payroll configurations; • Change or delete security configurations; • Override payee or payroll data; • Change or delete integrations; • Add, remove, or modify user access; and • Exporting of bulk data from the system.	Likelihood	9.1 22.1.27
C09	Access Control	Ensure that users are only provided with access to the service that have been specifically authorised to use, including: • Documenting of an access control policy that defines business requirements for access, principles for access (i.e. need to know, role based) and access control rules that will ensure these requirements are met; • Documenting of the mapping of user roles and permissions so it is clear which user roles have access to higher risk permissions, such as payroll or security configuration changes; • Implementing specific policies for access control based on business functions, processes or user roles and responsibilities, such as: employee, manager, payroll administrator, HR administrator, or super administrator; and • For multi-agency payroll: Implementing specific policies for access control based on each agency that the CA administers payroll for.	Likelihood, Impact	5.5.5 9.2.6 16.1 16.2 16.3 16.4 16.5 22.1.22 22.2.16

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
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. This includes: • Confirming the user roles and permissions that can be assigned within the software do not cause duty conflict; or • Confirming the CA can create their own user roles with customer permissions to avoid duty conflict. Permissions that should be separated include: • Ability to change or delete security configurations, such as logging configurations; and • Ability to change or delete payroll process configurations (i.e. schedules, patterns, rules), payee configurations (i.e., bank account details), or pay data.	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 allow access to be quickly, easily, and uniformly granted, changed, or removed for groups of users, without having to update the privileges for each user. Role-based access controls will be important to make sure privileged access is clearly assigned. Privileged access for payroll software should include the following permissions: • Change or delete payroll configurations; • Change or delete security configurations; • Override payee or payroll data; • Change or delete integrations; • Add, remove, or modify user access; and • Exporting of bulk data from the system.	Likelihood, Impact	16.2.6
C12	User Account Lifecycle Management	Ensure that user accounts are managed through their lifecycle process, including: • 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 (i.e. when a user changes role within an organisation).	Likelihood, Impact	5.5.5 9.2.7 16.1 19.1
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. Privileged access for payroll software should include roles with the ability to: • Change or delete payroll configurations; • Change or delete security configurations; • Override payee or payroll data; • Change or delete integrations; • Add, remove, or modify user access; and • Exporting of bulk data from the system.	Likelihood, Impact	16.3 22.1
C16	Identity Management and Authentication	Identity management and authentication is the processes that verify the identity of a user or device. Ideally, payroll software would integrate directly with the CA's main identity provider and would allow users to authenticate using their main identity provider credentials.	Likelihood	16.1.39 22.2.16
C17	Multi-Factor Authentication	Where strong authentication and identity verification is required (i.e. software accessible via the internet that has high risk data), additional forms of authentication can be used (i.e. 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: • Something you know (i.e. username and password); • Something you have (i.e. hardware or software token, digital certificate); and • Something you are (i.e. biometric fingerprint). This would either be enforced by the identity provider (C16), or by the software itself.	Likelihood	16.1.13 19.1.18

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
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 backups may be required and maintained in a location that meets the physical and environmental security requirements for backup 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. Backups for this software should be necessary if: • The Provider shuts down the service; or • The system is unavailable for an extended period.	Impact	6.4 13.3 16.3 16.5 17.1 22.1.26 22.2
C20	Logging and Auditing	Ensure that information systems are configured with adequate logging, archived, and retained for a defined appropriate period. Each log should capture the data and time of the event, and the time zone should be clear. Events to be logged includes: • Failed and successful user logins; • Failed or successful data transfers via third-party integrations or file transfer functions; • Viewed personal information and pay data; and • All privileged operations. Privileged operations include: • Change or delete payroll configurations; • Change or delete security configurations; • Override payee or payroll data; • Change or delete integrations; • Add, remove, or modify user access or roles; and • Ability to export bulk data.	Likelihood, Impact	3.4 7.1 7.3 12.4 14.1 14.2 14.3 15.2 16.5 19.2 20 22.2
C22	Information Security Incident Management	Ensure than an incident response plan is developed and defines what constitutes an incident and outlines the process that is to be followed should an incident occur. A communication plan should also be developed to provide guidance on how and when to share information relating to a security incident with outside parties such as customers, vendors, and the media. The incident response and management plan (or other supporting documents) should include: • The common incidents that are expected to occur; • How security events and incidents are detected; • How the Provider will notify the CA of any incidents or events; • How the CA Senior Responsible Officer or other stakeholders responsible are notified; • How users should report incidents; • How incidents should be recorded and documented; • How the incident should be managed to reduce impact; and • When and how the incident should be escalated (i.e. if the incident involves [redacted] data). For payroll software specifically, the security events that should be considered are: • User reported system or availability issues; • User reported data leaks or misconfigurations; • User reported information classification or privacy concerns; • Provider security incident or data breach; • Provider's third-party incident (i.e. supply chain incident); • Provider recommended disabling of features (due to unpatched weaknesses); or • Extended and unexpected system downtime.	Impact	5.1.12 5.6 7 22.1.25

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
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. This includes any API or other secret keys used for configuring integrations within the system.	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. This includes any data that is transmitted as part of any software third party integrations or file transfer features.	Likelihood, Impact	16.1.36 17.2 17.3 17.4
C26	Physical Security	Ensure that all critical facilities such as datacentres, communication rooms, servers, networks, telecommunication equipment and other important assets are physically protected against accident, natural disaster, attacks and unauthorised physical access.	Likelihood	8.1 8.2 8.3 9.4 11.7.32
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: • Change or delete payroll configurations; • Change or delete security configurations; • Override payee or payroll data; • Change or delete integrations; or • Add, remove, or modify user roles.	Likelihood	6.3
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, Impact	14.4.4
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. Plan for this software should be necessary if: • The Provider shuts down the service; • The system is unavailable for an extended period; or • The system is unavailable during the payroll cycle.	Impact	6.4
C52	Manual Checks and Reporting	Generate external reports or perform manual process checks to verify the data integrity of a payroll run. This helps the CA ensure that the data and system configurations are correct and are producing a valid payroll function outcome.	Impact	N/A
C53	Configuration Onboarding and Support	A new system may be unfamiliar, and the risk of misconfiguration can be higher. In addition to the other controls around user training, documentation, and access controls: The CA can get support from the Provider to understand how the system and its configurations works and get help with getting the initial configuration correctly. This applies for initial system migrations, large data or user onboarding, or large ad-hoc re-configurations of the system.	Likelihood	N/A
C54	Unused Features	Unused features in software can introduce unnecessary risk as these features could be misused and the actions would go unnoticed as the feature is not regularly used. Common misused features include messaging, email, or file hosting/sharing features. When these features are not in use, they should be disabled. If they cannot be disabled, access to these features should be limited. If access cannot be limited, training materials to users' needs to be clear how these features should be used and how to report misuse or concerns via the incident process.	Likelihood	N/A

Number	Title	Description	Reduces	NZISM Reference(s) v3.4
C55	Additional Assessments	There will be other context that a CA needs to consider when using this software, and this may include: • Limitations or risks associated with overseas software (i.e. performance, operational, and jurisdictional); • Risks introduced as part of a software migration (i.e. project-specific security risks); • Overseas legislation that may need to be met due to jurisdiction of payees overseas; or • Increased classification of Classification Removed based off the CA's own classification system or need to store Classification Removed data within the system. To consider the additional context of these situations, additional assessments or risk work will need to be performed.	Likelihood, Impact	N/A
C56	Securing Exported Data	Once data is exported from the system, it can no longer be controlled or secured by the system. The physical and digital copies of data is not covered within the scope of this assessment since it is leaving the system. It is still important to mention the need for the CA to consider the security of this data, and make sure there are other device, network, and physical controls to protect it. Exported data will happen often for this system as there may be multiple manual data transfers if the system is unable to digitally integrate with the internal or third-party systems.	Impact	N/A
C57	Organisation-based Access Controls	For CA that administer multi-agency payroll, they should be able to separate and restrict access to the agencies they can administer payroll for. This means that in addition to role-based access controls, they should be able to control which agency the user has a role and permissions to.	Likelihood, Impact	N/A

Table 6 – Controls to Risk Mapping

Table 6 shows which controls (that are recommended for both the Provider and CA) are related to each risk from Table 4.

9(2)(k)

Appendix A – Consulted Agencies and Suppliers

The agency stakeholders listed below were involved in group workshops or were consulted individually to inform the whole Risk Assessment. Suppliers listed below were involved to provide input into the technical context and controls catalogue.

Group workshops were held on:

- Workshop #1 held 22/06/2021, attended by payroll and technical specialists from: Ministry of Justice, Inland Revenue Department, Department of Corrections, Department of Internal Affairs;
- Workshop #2 held 8/07/2021, attended by payroll and technical specialists from: Ministry of Justice, Department of Corrections, Ministry of Health, Department of Internal Affairs; and
- Supplier Workshop #1 held 8/13/2021, attended by technical specialists from: Fusion5, SAP, and AMS.

Table 7 – Consulted Agencies and Suppliers

No.	Agency or Supplier	Attendee	Role in the Workshops	Org or Agency Name
1	Agency	Lachlan Neumann	Business context	Central Agencies Shared Services
2	Agency	Neill Flynn	Technical context	Department of Corrections
3	Agency	Trudi Amos	Business context	Department of Corrections
4	Agency	Sara Brownlie	Business context	Department of Internal Affairs
5	Agency (AoG)	Mae Koh	Observer	Department of Internal Affairs (All of Government)
6	Agency (AoG)	Liz Monrad	Observer	Department of Internal Affairs (All of Government)
7	Agency	Liberty Fernandez	Security	Department of Internal Affairs (Safety Security and Risk Team)
8	Agency	Richard Long	Business context	Inland Revenue Department
9	Agency	Chris Walley	Technical context	Ministry of Health
10	Agency	Victoria Bartram	Business context	Ministry of Health
11	Agency	John Cleveland	Technical context	Ministry of Justice
12	Supplier	9(2)(a)	Technical context	AMS
13	Supplier		Technical context	Fusion5
14	Supplier		Technical context	Fusion5
15	Supplier		Technical context	SAP

Appendix B – Project Overview

Scope

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

The Department of Internal Affairs (DIA), as Government Chief Digital Officer (GCDO), have performed and completed this Risk Assessment report and Controls Validation Plan (CVP) to support the CAs who plan to use this Marketplace-listed catalogue service.

The objective was to create a generic Risk Assessment and CVP that would cover most of the security risks and controls that would apply regardless of Supplier, technology, or specific context. The intent is that this would set a baseline for the CAs to use and then apply their own internal risk management frameworks and accredit the service for their own use.

Marketplace has a list of catalogue items and suppliers that are categorised in Tier 1, Tier 2, and Tier 3. The Tier 3 a is lower entry bar for small products and suppliers where, Tier 1 is for enterprise grade products and applier that requires highest assurance.

For the purposes of this work, it was assumed the Payroll Enterprise Software (provider-hosted) product would have a minimum Tier 1 rating.

The minimum Tier rating is based on:

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

Tier 3: Baseline Index — Suppliers respond to security questions which can include the Cloud Risk Assessment Tool (GCIO105). Assessment is based on self-assertions and not independent reviews. SaaS go through a Confidence and Risk Index (CRI) rating by McAfee MVision.

Tier 2: Design and Control Analysis — Suppliers must provide independent security assurance information that Consuming Agencies will be able to review. This can include ISO27001 or SOC2 Type 2 audit reports, and penetration testing reports. This information will be reviewed and confirmed appropriate by the GCDO before Tier-2 endorsement.

Tier 1: Design and Control Effectiveness — To obtain this rating, suppliers must provide additional information and receive Certification from the GCDO. Certification is based on Risk Assessment and demonstration of controls effectiveness can be supported from an organisation having ISO 27001 or SOC2 Certification or going through an audit by an auditor from the SRS panel.

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 provider-hosted Payroll Enterprise Software;
- Development of a Risk Assessment report in draft;
- Review of risks and ratings through a risk validation workshop; 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 8 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 8 – 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

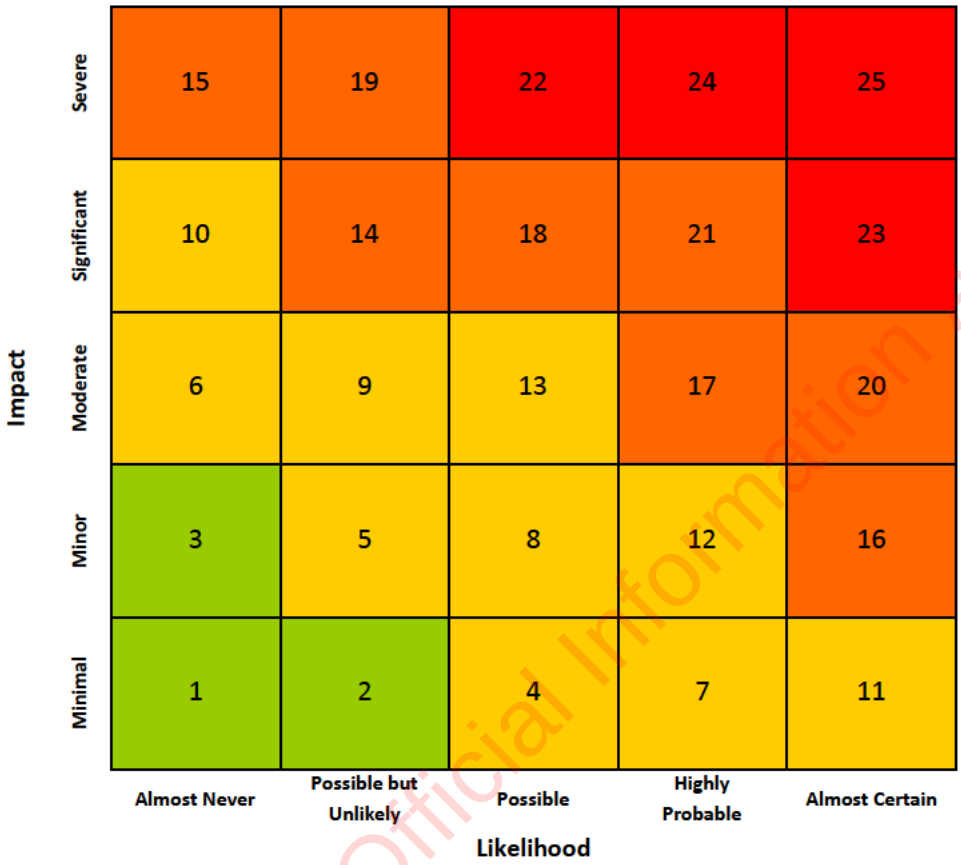
The qualitative scale used to assign an impact rating is presented in Table 9. All impacts were analysed in a business context. The impact of risks includes a consideration of any possible knock-on effects of the consequences of the identified risks, including cascade and cumulative effects.

Table 9 – AoG DIA All-of Government Risk Consequence Guide (choose the scale that best applies to you)

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

Table 20 – Risk Matrix

Table 10 presents an example 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.



Escalation of Risk

Table 311 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 31 – 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