|  |  |
| --- | --- |
| SOI cover image 2012 | Risk Assessment ProcessReport Template  |

Crown copyright ©. This copyright work is licensed under the Creative Commons Attribution 3.0 New Zealand licence. In essence, you are free to copy, distribute and adapt the work, as long as you attribute the work to the Department of Internal Affairs and abide by the other licence terms. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/3.0/nz/>. Please note that neither the Department of Internal Affairs emblem nor the New Zealand Government logo may be used in any way which infringes any provision of the [Flags, Emblems, and Names Protection Act 1981](http://www.legislation.govt.nz/act/public/1981/0047/latest/whole.html#dlm52216) or would infringe such provision if the relevant use occurred within New Zealand. Attribution to the Department of Internal Affairs should be in written form and not by reproduction of the Department of Internal Affairs emblem or New Zealand Government logo.

#  Glossary of Terms

|  |  |
| --- | --- |
| **Availability** | Ensuring that authorised users have timely and reliable access to information. |
| **Confidentiality** | Ensuring that only authorised users can access information. |
| **Consequence** | The outcome of an event. The outcome can be positive or negative. However, in the context of information security it is usually negative. |
| **Control** | A risk treatment implemented to reduce the likelihood and/or impact of a risk.  |
| **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. |
| **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. |
| **Recovery Point Objective (RPO)** | The earliest point time that is acceptable to recover data from. The RPO effectively specifies the amount of data loss that is acceptable to the business. |
| **Recovery Time Objective (RTO)** | The amount of time allowed for the recovery of an information system or service after a disaster event has occurred. The RTO effectively specifies the amount of time that is acceptable to the business to be without the system. |
| **Acceptable Interruption Window (AIW)** | The maximum period of time that an information system or service can be unavailable before compromising the achievement of the agency's business objectives. |

Contents

Glossary of Terms 3

1 Executive Summary 5

2 Business Context 7

3 Detailed Findings 9

4 Controls Catalogue 10

5 Controls to Risks Mapping 11

Appendix A – Risk Assessment Guidelines 12

*Impact (Consequences) Assessment* 12

*Likelihood (Probability) Assessment* 14

*Risk Matrix* 15

*Escalation of Risk* 15

Table of tables

[Table 1 – Gross Risks 3](#_Toc379271286)

[Table 2 – Residual Risks 3](#_Toc379271287)

[Table 3 – Risk Details 3](#_Toc379271288)

[Table 4 – Controls Catalogue 3](#_Toc379271289)

[Table 5 – Controls to Risk Mapping 3](#_Toc379271290)

[Table 6 – Impact Scale 3](#_Toc379271291)

[Table 7 – Likelihood Scale 3](#_Toc379271292)

[Table 8 – Risk Matrix 3](#_Toc379271293)

[Table 9 – Risk Escalation and Reporting 3](#_Toc379271294)

# Executive Summary

Introduction

This report presents the findings of an information security risk assessment of the *<information system or project name>*. The risk assessment followed the *<agency name>* Risk assessment process which is based on the AS/NZS ISO 31000:2009 and ISO/IEC 27005:2011 risk management standards.

Findings and Recommendations

A total of *<XX>* risks were identified during the risk assessment process. Table 1 illustrates the rating of each risk without any controls in place:

Table 1 – Gross Risks

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

<Provide a high-level overview of the findings and recommendations>

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

Table 2 – Residual Risks

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

# Business Context

This section provides an overview of the business context of the *<information system or service name>* that is in scope of this information security risk assessment.

Business Owner

The business owner of the service is:

*<Full Name>*

*<Job Title>*

*<Business Unit>*

*<Organisation>*

Technical Owner

The technical owner of the service is:

*<Full Name>*

*<Job Title>*

*<Business Unit>*

*<Organisation>*

Other Stakeholders

Additional business stakeholders for the service are:

*<Full Name>*

*<Job Title>*

*<Business Unit>*

*<Organisation>*

*<Full Name>*

*<Job Title>*

*<Business Unit>*

*<Organisation>*

Information Classification

*<Document the classification of the information stored, processed and/or transmitted by the information system/service based on the classification scheme presented in Security in the Government Sector (SIGS) 2002>*

Business Processes Supported

*<Provide an overview of the business processes supported by the information system/service>*

Business Impact

<Describe the business impact if the confidentiality, integrity, availability or privacy of the information stored, processed or transmitted by the information system/service were compromised. Define and document the maximum level of impact based on the impact rating table defined in Appendix X>

Users

<Document each user type and describe the access that they have to information with the information system/service>:

* <User Type A> – <description of how they access and use the service, together with the level of permissions that they have>.
* <User Type B> – <description of how they access and use the service, together with the level of permissions that they have>.
* <User Type C> – <description of how they access and use the service, together with the level of permissions that they have>.

Security Requirements

*<Document the business owner’s security requirements for the information system/service in terms of the Confidentiality, Integrity and Availability (CIA) requirements and any other relevant legislation etc.>*

Information Protection Priorities

*<Document the business owner’s information protection priorities for the information system/service based on the following scale:*

0: Irrelevant/not applicable

1: Unimportant

2: Some importance

3: Important

4: Highly Important

5: Critical*>*

|  |  |
| --- | --- |
| **Attribute** | **Priority Rating** |
| Confidentiality |  |
| Integrity |  |
| Availability |  |
| Privacy |  |

# Detailed Findings

This section provides details of the risks identified during the risk assessment for the *<information system/service name>*.

Table 3 – Risk Details

| **Risk ID** | **Risk Description** | **Key Risk Drivers** | **Consequence** | **Gross Risk** | **Recommended Controls** | **Residual Risk** |
| --- | --- | --- | --- | --- | --- | --- |
| **Likelihood** | **Impact** | **Risk Rating** | **Likelihood** | **Impact** | **Risk Rating** |
| 1.
 |  |  |  |  |  |  |  |  |  |  |
| 1.
 |  |  |  |  |  |  |  |  |  |  |

# Controls Catalogue

Table 4 – Controls Catalogue

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Number** | **Title** | **Description** | **Reduces** | **NZISM Reference(s)** |
| 1.
 |  |  |  |  |
| 1.
 |  |  |  |  |
| 1.
 |  |  |  |  |
| 1.
 |  |  |  |  |
| 1.
 |  |  |  |  |
| 1.
 |  |  |  |  |
| 1.
 |  |  |  |  |
| 1.
 |  |  |  |  |
| 1.
 |  |  |  |  |
| 1.
 |  |  |  |  |

#

# Controls to Risks Mapping

Table 5 – Controls to Risk Mapping

|  |  |  |
| --- | --- | --- |
| **No.** | **Control** | **Risk(s)** |
| C1 |  |  |
| C2 |  |  |
| C3 |  |  |
| C4 |  |  |
| C5 |  |  |
| C6 |  |  |
| C7 |  |  |
| C8 |  |  |
| C9 |  |  |
| C10 |  |  |

# Appendix A – Risk Assessment Guidelines

Risk Statements

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

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

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

For example:

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

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

Rating Risk

The likelihood and impacts of the risks will be rated using the simple qualitative scales documented below. The identified risks should be assessed with **no** controls in place. This will provide the gross risk rating and enable the effectiveness of the proposed controls to be assessed.

### Impact (Consequences) Assessment

The qualitative scale used to assign an impact rating is presented in Table 6. All impacts need to be seen in a business context, and be informed by the business. Rating the impact of a risk should include a consideration of any possible knock-on effects of the consequences of the identified risks, including cascade and cumulative effects.

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

Table 6 – Impact Scale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rating** | **Description** | **Reputation** | **Health and Safety** | **Service Delivery** | **Financial** |
| **5** | **Severe**  | * The agency suffers severe political and/or reputational damage that is cannot easily recover from.
* The Government suffers severe negative reputational impact, and the Prime Minister loses confidence in the Minister and/or the agency’s senior management.
* Minister and Chief Executive need to be briefed and regularly updated.
* Media interest is sustained for a prolonged period (i.e., over a week) with major criticism levelled at the Minister and/or the agency.
* The agency breaches multiple laws, which leads to legal action by affected stakeholders.
* External/independent investigation is commissioned by the SSC, 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 as a result of the risk eventuating.
 | * Impact can be managed within current resources, with no re-planning.
* Increase of less than 5% in yearly operating costs.
* One time financial cost of less than $10,000.
 |

###

### Likelihood (Probability) Assessment

The qualitative scale used to assign a likelihood rating is presented in Table 7 below. Where information is available about the frequency of an incident in the past it should be used to determine the likelihood of the risk eventuating. However, where such information does not exist it does not necessarily mean that the likelihood of the risk eventuating is low. It may merely indicate that there are no controls in place to detect it or that the agency has not previously been exposed to the particular risk.

Table 7 – 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 Likely | 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. |

### Risk Matrix

Table 8 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 8 – Risk Matrix

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

### Escalation of Risk

Table 9 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 9 – 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** |