INTERNAL AFFAIRS
Te Tari Taiwhenua

New Zealand Government

Risk Assessment Process

Information Security

February 2014

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	The potential cause of a risk.
Threat Agent	An individual, group or event that can cause a threat to occur.
Vulnerability	A weakness in an information system or service that can be exploited by a threat.

Contents

Table of figures

Table of tables

1 Introduction

This document presents a risk assessment process this is designed to enable agencies to systematically identify, analyse and evaluate the information security risks associated with an information system or service together with the controls required to manage them.

Overview

This process is aligned with and based on the AS/NZS ISO 31000:2009 and ISO/IEC 27005:2011 risk management standards. Figure 1 below presents the risk management lifecycle as defined in AS/NZS ISO 31000. It also incorporates elements from the Carnegie Mellon OCTAVE Allegro and Sherwood Applied Business Security Architecture (SABSA) risk assessment methodologies.

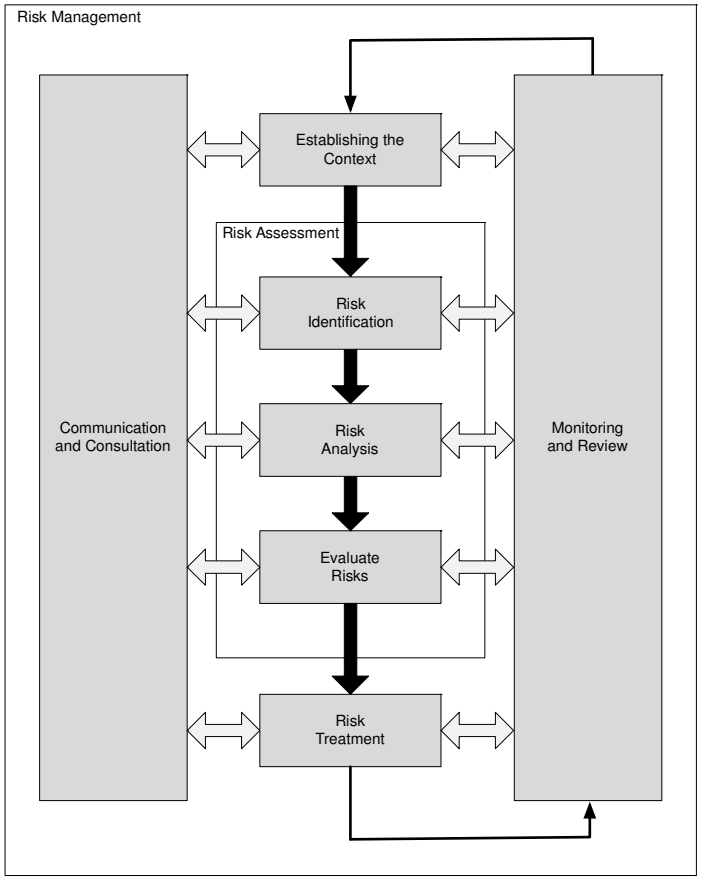


Figure 1 – ISO 3100:2009 Risk Management[1]

The process has been modified to incorporate the *Establish Context* phase into the risk assessment process. This ensures that risks are analysed and evaluated within the relevant business context.

The output of the risk assessment process is a report that captures the information security risks associated with the information system or service taking into consideration the agency's business context.

[1] **Source:** AS/NZS ISO 3100:2009 Risk management – Principles and guidelines

2 Risk Assessment Process

Establishing the Context

During a risk assessment it is essential to establish the business and technical context of the information system being reviewed. Establishing the context ensures that the businesses objectives are captured and that the internal and external factors that influence the risks are considered. It also sets the scope for the rest of the process.

Business Context

Meet with the business owner of the information system to establish the business context. During the meeting the business owner is responsible for identifying and defining the:

- **Information Classification** – the official information stored, processed and/or transmitted by the information system must be assigned an official classification based on Security in the Government Sector (SIGS).
- **Business Processes Supported** – the business processes and objectives supported by the information system. This should include any secondary, dependent or supporting processes.
- **Users of the System** – the different types of users of the information system. This should include the level of privileges they require to perform their duties or to use the system. Users may include business users, operations support staff and external users of services such as members of the public or another agency's staff.
- **Security and Compliance Requirements** – the confidentiality, integrity, availability (CIA) and privacy requirements of the system together with any relevant laws and/or regulations that need to be met by it.
- **Information Protection Priorities** – the business owner's prioritisation of the confidentiality, integrity, availability and privacy of the information stored, processed or transmitted by the information system.

Technical Context

Establish the technical context to provide a basic understanding of the security posture of the information system. A risk assessment may be performed for an information system that is already in production or as part of the development lifecycle of a new information system. The following provides guidance on who should be involved in establishing the technical context:

- **Service Owner** – the service owner (or their nominated delegate) is responsible for identifying the components and defining the boundaries of an information system that is scope of the risk assessment.
- **Enterprise or Solution Architect** – the Architect is responsible for identifying the components and defining the boundaries of an information system that is within the scope of the risk assessment.
- **Subject Matter Experts** – ICT operations staff responsible for the ongoing support and maintenance of the information system that is within the scope of the risk assessment.

The technical context discussions should focus on identifying the following attributes of the information system to provide an understanding of the overall security profile of the system:

- **Logical Architecture** – a system and component level view of the logical architecture of the information system. This should include the security domains where system components are located, the system interfaces and information flows (i.e., where and how data is stored, transmitted and processed).

- **System Components** – the hardware and software components that the information system is comprised of. This should include all direct and indirect components including servers, switches, firewalls, operating systems, applications and databases.

Risk Identification

The risk identification phase seeks to create a comprehensive list of events that may prevent, degrade or delay the achievement of the businesses objectives. Comprehensive identification is critical because a risk that is not identified at this stage will not be included in the risk analysis phase.

Although there are numerous tools and techniques that can be used to facilitate the identification and analysis of risks it is recommended that a multidisciplinary workshop discussion be used. The workshop should include the business and service owners (or their nominated delegates) and subject matter experts from both the business and ICT.

In order to manage risk, the potential threats to the information systems need to be identified. This is achieved by defining risk scenarios. Risk scenarios are methods of determining if any risks exist that could adversely affect the confidentiality, integrity or availability of the information system and therefore affect the business objectives. They generally consist of a threat exploiting a vulnerability resulting in an undesirable outcome. Appendix A – Threat Catalogue presents a sample list of threats that can be used to help discuss the potential risks to an information system. This approach can ensure that all the possible threats to the information system are considered, whilst ensuring that only those that are applicable are actually assessed.

The following provides an overview of the techniques that should be used to ensure that comprehensive lists of relevant risk are identified:

- People with the appropriate knowledge should be involved in identification of risks. Discussions must include the business owner and subject matter experts who can provide relevant and up-to-date information during the process; and

- Group discussions and workshops to facilitate the identification and discussion of the risks that may affect the businesses objectives.

When identifying risk, it is important to clearly describe it so that it can be assessed and evaluated. For example, assessing the likelihood and impact of a risk stated as: *"Fraud may occur"* is difficult if not impossible. However, assessing the same a risk stated as: *"An employee commits fraud resulting in financial loss and reputation damage as fraud detection processes are not robust"* is more straightforward. Therefore the description of risks identified should use the following structure (or a variation of it, providing that the three elements are included):

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

For example:

- A hacker gains unauthorised access to information stored in the system by performing a brute force password guessing attack. They use the information to commit identity fraud that leads to an investigation by the Privacy Commissioner, and reputational damage to the Minister and agency. The attack is successful because the system does not enforce strong passwords or account lockout policies and does not log failed logon attempts.

- The loss of a laptop leads to official information being disclosed to an unauthorised party, and reputational damage to the Minister and agency as disk encryption has not been enabled on all laptop devices.

Once the risk description has been defined and documented consideration should be given to the risk drivers. Capturing the risk drivers is useful when identifying and selecting controls to manage the risk.

The business and technical context normally inform the risk drivers, for example, a risk may only exist because the information system is Internet facing. It is important to also note that there may be multiple risk drivers related to a risk. The following provides some example risk drivers:

- The information system is deployed as an Internet facing service.

- The information system is an attractive target to criminals/hacktivists.

- Patches may not be applied in a timely manner.

- Default accounts/passwords are not changed or removed.

- User accounts are not disabled or removed in a timely manner when a staff member leaves the agency.

Although the risk statement captures the consequences (i.e., the effect on objectives) of the risk eventuating it is useful to document them separately as well. The consequences should be stated in business not technical terms. For example:

- Reputational damage to the agency;

- IN CONFIDENCE information is disclosed to an unauthorised party;

- Breach of the Privacy Act 1993;

- Service delivery is impacted due to a loss of productivity;

- Loss of confidence in the service by key stakeholders.

Risk Analysis

Once the relevant risks have been identified the likelihood and impact of them eventuating must be assessed and rated. Typically the likelihood and impact of a risk eventuating are rated using a qualitative scale. Appendix B – Example Risk Scales and Matrix presents a qualitative scale that can be used to assign a likelihood rating.

Note: the Risk Rating Scales and Matrix are only provided to help illustrate how to use a qualitative scale to analyse risks. Agencies should substitute or adapt them when applying the process in their organisation.

As the business owner (or their nominated delegate) is the owner of the risk they are responsible for rating the identified risks. However, the subject matter experts should provide information to help them with the assessment.

Impact Assessment

Assess the impact of the risk eventuating with **no** controls in place. This will inform the gross risk rating and enable the effectiveness of any current controls that reduce the impact of a risk event that occurs to be assessed.

Although there may be multiple impact statements documented for a risk, only one impact rating can be assigned to the risk. As a result, the highest rated impact statement should be used to determine the impact rating of a risk.

Likelihood Assessment

Assess the likelihood of the risk eventuating with **no** controls in place. This will inform the gross risk rating and enable the effectiveness of any current controls that reduce the likelihood of a risk event occurring to be assessed.

Where historic information is available about the frequency of an incident's occurrence it should be used to help determine the likelihood of the risk eventuating. However, it must be noted that the absence of such information 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 that it has occurred.

Risk Rating

The risk rating is evaluated using a risk matrix. Appendix B – Example Risk Scales and Matrix also presents a risk matrix that can be used to map the likelihood with the impact rating, the overall risk rating being the point where the two ratings intersect. For example:

- A risk with likelihood of *Almost Never*, and impact rating of *Moderate* would result in an overall risk rating of 6;
- A risk with a likelihood rating of *Possible*, and an impact rating of Severe would result in an overall risk rating of 22; and
- A risk with a likelihood rating of *Almost Certain*, and an impact rating of *Minor* would result in an overall risk rating of 16.

The risk rating without any controls in place have been assessed is called the gross risk. Typically risks that are assessed as being 1 to 3 on the rating scale without any controls in place are considered acceptable to the business and may not require the implementation of any controls to manage them. However, because risk is rarely static they should be added to the agency's risk register so that they can be monitored and re-assessed on a regular basis to ensure that the likelihood and/or impact do not change.

Controls Identification and Assessment

Regardless of whether the risk assessment is being performed for an information system that is in production or as part of the development lifecycle process for a new information system there will already be controls in place to reduce the likelihood and/or impact of some of the risks that have been identified.

A control can reduce the risk by reducing the likelihood of an event, the impact or both. Assessing the effect that the control has on the overall risk leads to determining the residual risk rating. Figure 2 below can be used to identify the affect each type of control has on the likelihood or impact of a risk. Typically deterrent and preventive controls reduce the likelihood of a risk eventuating whereas detective and corrective controls reduce the impact should it eventuate.

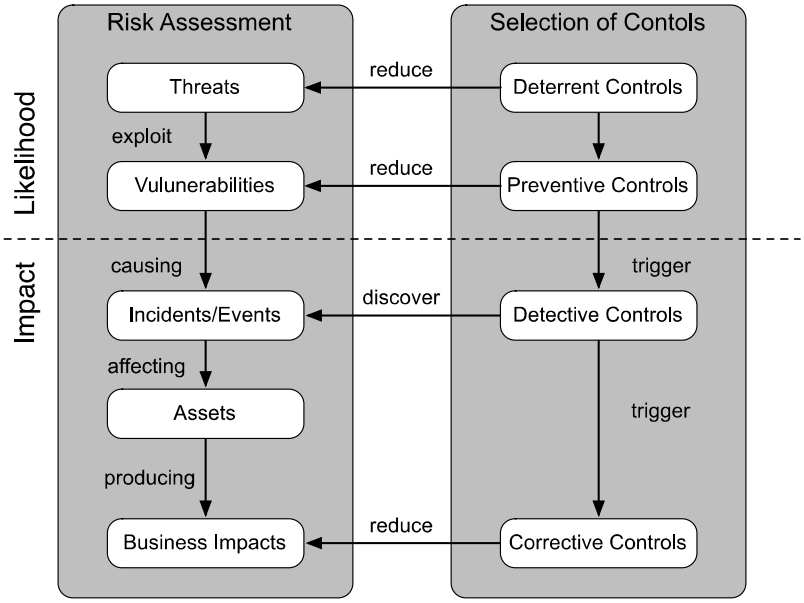


Figure 2 – Types of Controls[2]

The following provides a brief description and some example for each type of control highlighted in the Figure 2:

- **Deterrent Controls** – are intended to discourage a potential attacker. For example, establishing an information security policy, a warning message on the logon screen, a Kensington lock or security cameras.

- **Preventive Controls** – are intended to minimise the likelihood of an incident occurring. For example, a user account management process, restricting server room access to authorised personnel, configuring appropriate rules on a firewall or implementing an access control list on a file share.

- **Detective Controls** – are intended to identify when an incident has occurred. For example, review of server or firewall security logs or Intrusion Detection System (IDS) alerts.

[2] **Source:** adapted from Sherwood, J., Clark, A. and Lynas, D. (2005). Enterprise Security Architecture: A Business-Driven Approach

- **Corrective Controls** – are intended to fix information system components after an incident has occurred. For example, data backups, SQL transaction log shipping or business continuity and disaster recovery plans.

The Australian Defence Signals Directorate (DSD) has published the Top 35 Mitigation Strategies[3] that includes an assessment of the effectiveness of 35 controls. This document can be used to perform a high-level assessment of a control's effectiveness in the absence of other information.

It is recommended that a multidisciplinary workshop be used to identify and assess the controls that are currently in place to reduce the likelihood and/or impact of the risks eventuating. The business owner and subject matter experts who can identify and describe the current controls that are in place to manage the identified risks must be involved in assessing their efficacy. Where information is available that provides evidence about the effectiveness of the current controls it should be considered during the controls assessment phase.

During the risk assessment a control may be identified as being ineffective, not sufficient or simply not relevant to the risk it is supposed to be mitigating. If this is the case, an analysis should be performed to determine whether it should be removed and replaced by another more suitable control or whether it should remain in place and be supplemented with additional controls.

The residual risk rating is derived by assessing the effect that the current controls have on the gross risk and using the risk matrix presented in Appendix B – Example Risk Scales and Matrix to map the likelihood and impact ratings, with the residual risk rating being the new point where the two ratings intersect. For example:

- A risk scenario with likelihood rating of *Possible but Unlikely*, and impact rating of *Severe* would result in an overall risk rating of 19. A control currently in place is highly effective at reducing the impact of the risk. The impact rating is revised to *Moderate* with the control in place, therefore the residual risk rating is 9;

- A risk scenario with a likelihood rating of *Possible*, and an impact rating of *Severe* would result in an overall risk rating of 22. A control currently in place is effective at reducing the impact of the risk. The impact rating is revised to *Significant* with the control in place, therefore the residual risk rating is 18; and

- A risk scenario with a likelihood rating of *Almost Certain*, and an impact rating of Minor would result in an overall risk rating of 16. A control currently in place is very effective at reducing the likelihood of the risk. The likelihood rating is revised to *Possible* with the control in place; therefore the residual risk rating is 8.

Risk Evaluation

Once the risk analysis has been completed the residual risks can be evaluated against the agency's risk tolerance levels. Risk evaluation seeks to assist the business owner in making decisions on which risks requirements treatment, and the priority for implementing a risk response.

[3] http://www.dsd.gov.au/publications/Top_35_Mitigations.pdf

Residual risks that are assessed as being between 1 and 3 on the ratings scale are generally considered to present an acceptable level of risk to the business and do not require any further evaluation. However, because risk is rarely static they should be added to the agency's risk register so that they can be monitored and assessed on a regular basis to ensure that the likelihood and/or impact do not change.

All residual risks that are evaluated as being between 4 and 25 on the rating scale need to be evaluated and prioritised. Typically the higher the risk rating is, the higher its priority. However, there may be two or more risks with the same risk rating. If it is not clear which risks have a higher priority the information protection priorities defined by the business owner when establishing the business context for the system should be used to determine the priority for the implementation of additional controls.

Risk Treatment

Although the implementation of additional mitigating controls is typically beyond the scope of the risk assessment process, the identification and selection of them is not. The business owner can choose to avoid, treat, transfer or accept the risk. The provides an overview of each:

- **Avoid** – stop the activity that would give rise to the risk, thus eliminating the risk. Risk avoidance is not commonly selected as it typically results in not being able to exploit the associated opportunity;

- **Treat** – implement controls to reduce the likelihood and/or impact of the risk eventuating. Risk treatment is the most commonly selected risk treatment;

- **Transfer** – transfer or share all or part of the impact of the risk eventuating with a third party. The most common risk transfer techniques are insurance and outsourcing;

- **Accept** – the business owner may choose to accept a risk. Risks are usually accepted when they are assessed as being within the business's defined risk tolerance level. However, they may also be accepted when it is not practical to avoid, treat or transfer the risk.

Usually there will be a number of controls that can be implemented either individually or in combination with each other to reduce the likelihood and/or impact of a risk eventuating. The risk assessment should clearly identify the priority for implementing the proposed controls.

As highlighted in the ***Controls Identification and Assessment*** section there are different types of controls that can be implemented to reduce the identified risks to an acceptable level. It is important to ensure that any recommended control will reduce the residual risk. For example, if a risk has a residual risk rating of 15 (i.e., a likelihood of *Almost Never* and a impact of *Severe*) recommending a control that reduces the likelihood of the risk eventuating will not reduce the residual risk. However, recommending a control (or a combination of controls) to reduce the impact of the risk eventuating will.

Agencies are required to select controls to meet the requirements defined within the New Zealand Information Security Manual (NZISM)[4]. The NZISM presents the mandatory and

[4] The NZISM is available from the Government Communications Security Bureau's (GCSB) website at http://www.gcsb.govt.nz/

discretionary controls that should be implemented based on the classification of the official information stored, processed or transmitted by the information system and should be used in conjunction with a risk management framework. As a result, it is recommended that agencies align their risk treatments with the controls defined in the NZISM.

Examples of recommended controls to reduce residual risks to an acceptable level are:

- Implement an appropriate access control lists on shares, folders and files to ensure only authorised personnel can access information stored within the folders.
- Review the patch management process to ensure that it includes all operating systems, applications and firmware. Ensure monthly maintenance windows are defined and agreed with the business to ensure that patches are implemented regularly and in a timely manner.
- Implement additional servers and load balancing hardware to ensure that the service scales to meet the businesses requirements and that it meets the availability requirements in the event of a server failure.
- Implement an operational procedure to test the restoration of data from the backup media to ensure that critical data can be restored.

As a control may apply to multiple risks it is recommended that the controls be defined in a controls catalogue and cross-referenced against the relevant risks.

The output of the process is a risk assessment report. The business owner must acknowledge that the report accurately documents the outcome of the risk assessment by signing off on the report.

If the risk assessment was for a current production information system then the report should be used to develop a risk management plan. The risk management plan may be based on the agency's risk register or a formal programme of work. If the risks need to be managed as a formal programme of work the plan should follow the agency's project management methodology and must be approved at the appropriate governance level within the organisation.

However, if the risk assessment was for a new system then the report should be used to ensure that the controls required to manage the risks are incorporated into the solutions architecture and design documents and/or Request For Proposal (RFP) document.

3 Monitoring and Review

Very few risks remain static. A risk that is currently within the business owner's risk appetite may not remain so. Therefore ongoing review of risks is essential to ensure that the selected treatment remains effective.

The factors that affect the likelihood and impact of a risk eventuating may change, as could the factors that affect the suitability or cost of the treatment options. Therefore it is necessary to review risks on a regular basis. The monitoring and review of the risk seeks to ensure that likelihood has not increased and to ascertain if the cost of the control to reduce the impact has decreased to a level that makes its implementation affordable.

The monitoring and review of risks enables the agency to learn lessons from the risk management process by reviewing events, treatment plans and their outcomes. The results of monitoring and review activities should be fed back into the risk management process.

4 Communication and Consultation

Communication and consultation are an important consideration at each step of the risk assessment process. There must be a two-way dialogue between the stakeholders with the focus on consultation rather than a one-way information flow. Effective communication between stakeholders is essential to ensure that risks are understood and decisions about risk response selection are appropriate.

The perception of a risk can vary significantly. Stakeholders are likely to make judgements on the acceptability of the risk based on their own experience of it, therefore it is important to ensure that their perceptions of the risk, as well as their perceptions of the benefits, are identified and documented and the underlying reasons for their position are clearly understood and addressed.

Information about a risk may be distributed to a large number of different stakeholders within the agency. To be effective, all information relating to the management of risks should be:

- **Clear and Concise** – ensure that the information can be understood by all recipients and does not overwhelm them with extraneous detail;
- **Useful** – any communication related to risk must be relevant. Technical information that is too detailed or sent non-technical recipients will likely impede, rather than enable, a clear view of risk;
- **Timely** – timely communications enable decisions and actions to be taken at the appropriate time in the risk management process;
- **Targeted** – information must be communicated at the right level of aggregation and adapted for the audience to enable informed decisions to be made. However, the aggregation of the information must not hide the root cause of a risk;
- **Controlled** – information related to risks should be made available on a need-to-know basis. Only parties with a genuine need should have access to risk reports, risk management plans and the risk register.

Appendix A – Threat Catalogue

Threat Sources

Table 1 presents the typical threat agents that can adversely affect the information security of an agency's information assets. They are categorised into threat groups to enable agencies to consider whether they need to define a risk statement for each individual threat agent, a group of threat agents or a combination of the two. For example, it may be sufficient for an agency to consider the threats from employees and external attackers rather than each type of individual or external organisations threat agents but they may need to consider each type of technical, accidental and natural event.

Table 1 – Threat Sources[5]

Threat Group	Threat Agent
Individuals	Employees/Contractors
	Customers/Clients
	Service Provider Employees/Contractors
	Hackers
	Hacktivists/Activists
	Criminals
	Terrorists
External Organisations	Service Providers
	Hacktivist or Activist Groups
	Foreign Governments
	State Sponsored Action Groups
	Organised Crime Syndicates
	Terrorist Groups
Technical Events	Malicious Code (e.g., viruses, worms etc.)
	Defective Code
	Equipment Failure
	Failure of air-conditioning
	Loss of power supply
Accidental Events	Fire
	Water damage
	Major Accident
	Destruction of equipment or media
Natural Events	Weather (e.g., electrical storm)
	Earthquake
	Volcanic Eruption
	Flood

[5] **Source:** adapted from Sherwood, J., Clark, A. and Lynas, D. (2005). Enterprise Security Architecture: A Business-Driven Approach

Table 2 presents some of the potential reasons for an individual or external organisation threat agents to try to exploit a vulnerability in an information system or service. It may also be important to also consider the intent of the threat agent, as their actions may be accidental, deliberate or malicious. For example, an employee may accidentally, deliberately or maliciously violate a process or procedure (e.g., they forget to perform a step, they choose not perform a step as they believe that it is unnecessary or they choose not to perform a step knowing that it will have adverse impact on the organisation).

Table 2 – Threat Agent Motivation[6]

Threat Domain	Motivation
Individuals	Minimise their effort to complete a process or procedure
	Financial gain
	Revenge
	Gaining knowledge or information
	Exerting power
	Gaining peer recognition and respect
	Satisfying curiosity
	Furthering political or social aims
	Terrorising certain target groups or individuals
	Enhancing personal status with other individuals or a group
External Organisations	Gaining a competitive advantage
	Gaining an economic advantage
	Gaining a military advantage
	Gaining a political advantage
	Furthering political or social aims
	Financial gain
	Terrorising certain target groups

A threat agent's motivation may be accelerated or moderated by other factors such as their capability (e.g., equipment, expertise, experience etc.) and whether there is an opportunity (e.g., the employee has full access to source code or the information system is exposed to the Internet etc.) for them to exploit vulnerabilities in the agency's information system or service. Therefore agencies should also consider the factors that may influence a threat agent's intention to attempt to exploit a vulnerability.

Note: The tables presented in this document should not be considered a complete list of all possible threats. Agencies must consider if they need to define additional threat agents based on their specific business context.

[6] **Source:** adapted from Sherwood, J., Clark, A. and Lynas, D. (2005). Enterprise Security Architecture: A Business-Driven Approach

Appendix B – Example Risk Scales and Matrix

Introduction

This appendix presents sample risk rating scales and a matrix that can be used to assess a risk, give it a rating and escalate or report it to the individual or group that needs to be aware of the risk and is accountable for deciding how it should be managed.

Developing and Tailoring Scales

Risks must be evaluated within the agency's business context. Agencies should substitute the risk rating scales and matrix presented in this document with their own. Where an agency has not previously defined its own scales and matrix it should tailor the examples provided to reflect their unique risk appetite and governance structures.

It is important that senior management are involved in the development of and sign-off on the risk rating scales to ensure that they accurately reflect their risk appetite and tolerance levels and consider the agency's operating context.

When developing or tailoring an impact scale senior management must carefully consider the different types of consequences that could compromise the agency's operations and prevent it from achieving its strategic objectives. This should take into account reputation, financial, legal, health and safety, service delivery and any other area that is specific to the agency's context.

Once the categories have been identified senior management must define the impacts at each point on the scale. A useful strategy when defining the points on an impact scale is to capture the maximum credible consequence and the lowest consequence of concern first (i.e., define what is meant by 5 – Severe and 1 - Minimal first). The definitions must be clear, concise and not open to interpretation by risk workshop participants to enable risks to be rated in a consistent manner across different risk assessments.

Similarly, the likelihood scale should be as unambiguous as possible and must reflect the agency's standard lifecycle for an information system or service (i.e., if the agency typically refreshes its information systems after 5 years of operation the scale should consider likelihood over that period). The scale needs to take into account that the lowest probability must be acceptable for the highest defined consequence, otherwise all activities with an impact rated at 5 – Severe would be beyond the agency's risk appetite even if they have a likelihood rating of 1 – Almost Never.

Note: It is strongly recommended that agencies do not use qualitative scales without any definitions (e.g., high, medium or low), as they do not provide adequate information for the reader of a risk report to understand how and why a risk was given a specific rating.

In addition to developing or customising the impact and likelihood scales, agencies must identify and document who must be informed and has authority to accept risk based on its magnitude. For example, a 5x5 matrix typically bands risks into four ratings levels. The risk escalation and reporting requirements should take into account the agency's governance structure to ensure that risk treatment and acceptance decisions are made at the appropriate level within the organisation.

Risk Rating Scales and Matrix

Impact (Consequences) Assessment

This section presents two different qualitative scales that can be used to assess the impact of a risk. Table 3 presents a basic scale that describes the potential impacts using quite subjective terms, whereas Table 4 presents a more complex scale that separates the impacts into the different impact categories and uses clearly defined descriptions.

There are advantages and disadvantages to each approach. For example, it is easier to create a simple impact scale. However, simple scales are typically more difficult to use when assessing and rating risks, as workshop participants are more likely to interpret the definitions based on their own experience. Conversely, it requires more effort to define a detailed scale. However, workshop participants are more likely to consistently assess the impact of the identified risks when using a detailed scale, as the descriptions are not so easy to misinterpret.

All impacts need to be seen in a business context, and be informed by the business. The effect of a risk event materialising should 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 3 – Simple Impact Scale

Rating	Description	Meaning
5	Severe	• Could severely compromise the strategic objectives of the agency. • Could severely compromise whole programme or sub-project outcomes or benefits. • Severe ongoing impact on service delivery across multiple agencies. • Severe political or reputational damage to Minister, or NZ Government or multiple agencies. • Chance of serious breach of laws or litigation against the NZ Government or multiple agencies. • Impact cannot be managed without significant extra resources (financial or human) and re-prioritisation.
4	Significant	• Could significantly compromise the strategic objectives of the agency. • Could significantly compromise whole programme or sub-project outcomes or benefits. • Significant ongoing impact on service delivery across one or more agency. • Significant political or reputational damage to the NZ Government or one or more agency. • Chance of breach of laws or litigation against the NZ Government or one or more agency. • Impact cannot be managed without extra resources (financial or human) and re-prioritisation.
3	Moderate	• Could compromise a strategic objective of the agency. • Could compromise whole programme or sub project outcomes. • Limited impact on work delivery across the NZ Government or border protection agencies. • Limited political or reputation damage to the NZ Government or one or more agency. • Impact can be managed with some re-planning and modest extra resources (financial or human). • Minister(s) may need to be briefed. • Chance of litigation against one or more government agency.
2	Minor	• Minor impact on work delivery across the agency. • Minor impact on a strategic objective of the agency. • Impact can be managed within current resources, with some re-planning. • Communication with key stakeholders may be needed.
1	Minimal	• No real effect on the outcomes and/or objectives of the agency. • No real effect on the strategic objectives of the agency. • Any impact on the agency's capacity and/or capability can be absorbed. • No impact to any stakeholder.

Table 4 – Detailed 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 agency's 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

This section presents a qualitative scale that can be used to assess the likelihood of a risk eventuating. As shown in Table 5 it is important to define what each rating level means. This ensures that risks can be assessed in a consistent manner by providing workshop participants with a standardised framework for assigning a likelihood rating. 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.

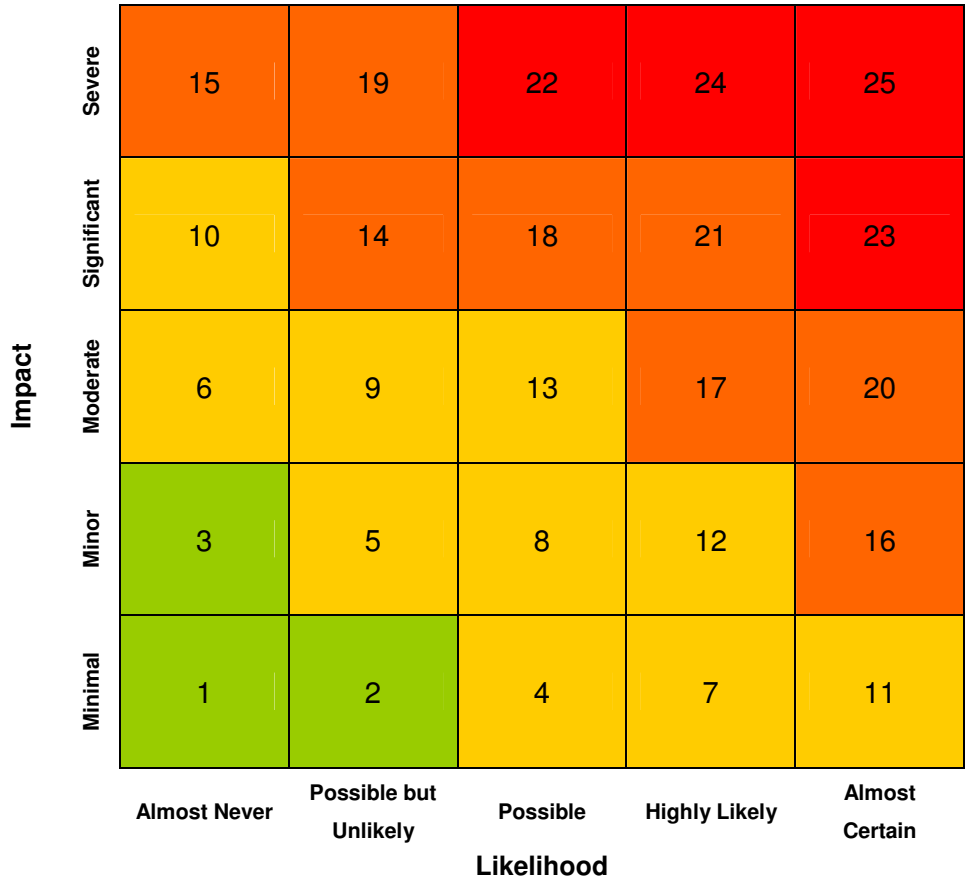
Table 5 – Likelihood Scale

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

Table 6 – Risk Matrix



Risk Escalation

Table 7 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 7 – 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