New Zealand Government

# Assuring Digital Government Outcomes

## ICT Risk Management Guidance

Version 1.0 July 2019

*Better information, better conversations, better decisions*

# Document History

| Version | Issue date | Description of changes |
|---|---|---|
| Version 1.0 | July 2019 | Initial version (published) |

"a positive declaration intended to give confidence"

**Confidence**

Informative

Certainty

*"the goal of improving information or the context of information so that decision makers can make more informed, and presumably better, decisions"*

**Independence**

**"the comfort that can be derived from credible information"**

**"an independent and objective oversight of the likely future performance of major investments for those responsible for sanctioning, financing or insuring such undertaking"**

*Assurance* is the process of providing confidence to stakeholders that *an investment* will achieve their objectives, and realise their benefits.

AN OBJECTIVE EXAMINATION AND INDEPENDENT ASSESSMENT OF AN INVESTMENT INCLUDING RISKS, CONTROLS, PROCESSES, AND GOVERNANCE.

Credibility

# Table of Contents

# 1 Introduction

## 1.1 Purpose

This guidance supports government organisations to implement a risk management process that enables critical information and communication technology (ICT) risks to be effectively identified, managed and governed.

## 1.2 Context

This guidance is an extension of the All-of-Government (AoG) ICT Operations Assurance Framework[1] which outlines the principles of good assurance.

We recognise that many government organisations will have existing enterprise risk management frameworks in place. This guidance is not intended to replace these frameworks; it's to provide practical help and advice to supplement these frameworks. In the first instance, you should adopt your enterprise risk management framework.

This guidance is based on the ISO 31000: 2018 *Risk Management - Guidelines*[2].

As a guiding principle:

***"ICT risk refers to the business risk associated with the use, ownership, operation, involvement, influence and adoption of ICT within the department[3]."***

The term 'ICT risk' is used here to mean both traditional ICT risk as well as new and emerging risk resulting from adopting digital technologies.

## 1.3 Benefits of risk management

Government organisations are increasingly dependent on technology to deliver public services. At the same time, the traditional ICT function in government organisations is changing to support new ways of working, including a shift towards continuous delivery through Agile/DevOps approaches.

Now more than ever, managing ICT risk requires a well-coordinated, integrated approach that prioritises understanding the business impacts of ICT risk. Integrated ICT risk management means that government organisations are in a better position to achieve their strategic business outcomes as well as create opportunities to exceed them.

---

[1] https://www.digital.govt.nz/standards-and-guidance/governance/system-assurance/all-of-government-ICT-operations-assurance-framework/

[2] https://www.iso.org/standard/65694.html

[3] Queensland Government Chief Information Office

Effective risk management helps government organisations to:

- Clarify objectives for how ICT supports business outcomes
- Ensure critical ICT risks to service delivery are identified and effectively managed, avoiding operational surprises
- Make risk-informed investment decisions based on a shared view of ICT risks and their potential business impacts
- Prioritise the allocation of resources to areas of greatest risk
- Be more responsive to new and emerging ICT risks.

## 1.4 Risk management principles

The purpose of risk management is the creation and protection of value. ISO 31000 sets out eight principles of effective and efficient risk management:

1. Framework and processes should be customised and proportionate
2. Appropriate and timely involvement of stakeholders is necessary
3. Structured and comprehensive approach is required
4. Risk management is an integral part of all organisational activities
5. Risk management anticipates, detects, acknowledges and responds to changes
6. Risk management explicitly considers any limitations of available information
7. Human and cultural factors influence all aspects of risk management
8. Risk management is continually improved through learning and experience.

Government organisations should adopt and adapt these principles to design, implement and operate a risk management process that is tailored to their organisation.

# 2 Risk governance, roles and responsibilities

Effective risk management depends on appropriate governance and oversight. Risk oversight covers both the risk management process as well as individual accountabilities for managing risk outcomes.

## 2.1 Three lines of defence model

It is essential you establish roles and responsibilities for effective risk management across the organisation. The 'three lines of defence' model is a framework that is often used to clearly define risk management roles and responsibilities:

- This **first line of defence** is the day-to-day operational management processes and controls you have for identifying and managing ICT risks. This includes business management and line managers who are responsible for the design and implementation of business processes and controls.
- The **second line of defence** is the governance and oversight arrangements that exist for ongoing monitoring of ICT risks. This includes oversight functions that provide advice and guidance on how to ensure the correct organisational settings are in place for the business to manage risk e.g. Finance, Human Resources, Procurement, Security and Risk, Privacy, etc.
- The **third line of defence** is the independent assurance you obtain from Internal Audit and third party assurance providers, including External Audit, that ICT risks are effectively managed.

Figure 1 below shows an example of how the three lines of defence model can be applied to ICT security risk.


*Figure 1: ICT risk example of three lines of defence model*

## 2.2 Role of Executive Leadership team

The Executive Leadership team (ELT) has primary responsibility for risk governance and overseeing the top risks faced by the organisation. This includes ensuring the risk management principles are embedded into the organisation's risk management framework, governance, decision-making, and reporting structures to promote a robust risk management culture.

ELT may delegate monitoring of specific risks to other management or governance bodies within the organisation e.g. financial reporting, regulatory, ICT, health and safety, reputational risks, etc. Ultimately, however, ELT remain accountable for effective risk management across the organisation.

## 2.3 Risk escalation

A key component of risk management and governance is knowing when to escalate risks to ensure they are managed at the right level within the organisation. A formal risk escalation process should identify who has the authority to accept the risk, based on the residual risk rating. Different types of risk (e.g. strategic risk versus operational risk) may have different escalation paths.



# 3 Establishing the context

## 3.1 Operating environment

Establishing the context for the risk assessment will help you to define the purpose and scope, who needs to be involved and the risk rating criteria to be used. For example, the subject of the risk assessment may be the organisation as whole, a business unit, a programme or project, or a process.

At the organisational level, the risk context is typically informed by the overall strategic plan. The strategic plan defines the relationship between the organisation and its operating environment, identifying strengths, weaknesses, opportunities and threats.

At the business unit level, the risk context is set by the detailed objectives and business plans of the business unit in question. These are established as part of the planning process and demonstrate how the business unit will support the achievement of strategic outcomes.

At the programme or project level, the risk context is determined by the specific investment objectives and the expected outcomes.

At the process level, the risk context is likely to be less formalised, but it is important to ensure objectives are clearly understood and that risk rating criteria are appropriate to make the risk assessment meaningful.

In all cases, it is important to start with a clear understanding of the operating environment, both internal and external, which may reasonably impact on the organisation. The operating environment should be regularly reviewed to ensure that it remains current.

Below are some questions which may be helpful in establishing the risk context:

***Risk context questions***

- What are the overall strategic and business outcomes of the activity or change?
- What is the significance of the activity or change to the organisation's business outcomes?
- Who is the customer of the activity or change and what do they want or need?
- What other government organisations or external stakeholders might be involved?
- What regulations and legislation do you need to consider?
- Will the Minister be interested?
- What other external uncertainty might exist?
- What is the internal environment for the activity of change e.g. operating model, policies and frameworks, values and culture, etc?
- What other parts of the organisation might be impacted by the activity or change?

### 3.1.1 Inter-agency risks

Increasingly, government organisations must work together to deliver integrated citizen-centric services. This means that risk governance must extend beyond traditional organisational boundaries with explicit accountabilities for managing 'system' level risks in support of inter-agency, sector and AoG outcomes.

Where this is the case, the parties should agree a lead agency who is responsible for making sure there is a common understanding of the risks involved and how they will be managed. This includes ensuring there is a joint risk register and that it is clear who owns which risk. This may require other government organisations to adopt the risk assessment process of the lead agency in order to provide compatible risk ratings and risk reporting.

## 3.2 Risk appetite

When establishing the context, you should also consider your organisation's risk appetite. Risk appetite is the amount of risk that an organisation is willing to accept in the pursuit of its business objectives and outcomes. It represents the organisation's attitude to particular risks and takes into consideration the expectations of key stakeholders, such as Ministers, customers, third party providers, staff and the public.

Risk appetite can be expressed as a series of boundaries or statements that have been appropriately authorised by ELT. It is often reflected in the target risk rating for individual risks or categories of risk. This does not mean that the target risk rating must always be Low.

An organisation may seek to encourage innovation, using digital technologies and new ways of working to support the delivery of new channels or services. As a result, the target risk rating for a new channel or service may be higher than for core products and services, where the organisation has a lower risk appetite.

To identify acceptable levels of risk, it is important to hold discussions at the executive level in order to clearly communicate, assess and provide direction on what are acceptable levels of residual risk. Risk appetite may change over time as new information and outcomes become available, and as stakeholder expectations evolve.

### 3.2.1 Risk tolerance

You should also consider risk tolerance when establishing the context of the risk assessment. Risk tolerance can be defined as the acceptable variance from the organisation's risk appetite. Government organisations should determine acceptable tolerance limits and whether they are negotiable.

For example, an organisation may define a target that no critical system should have a service disruption of more than one working day. This could then be monitored and escalated based on a risk tolerance of no more than two working days for a service disruption.

You may need to set up an appropriate process for when a risk falls marginally outside the desired risk tolerance. In this scenario, clearly define why the risk should be accepted or managed e.g. the cost of further mitigation.

# 4 Risk assessment

The goal of the risk assessment process is to apply a consistent methodology for assessing the ICT risks faced by the organisation. It provides the foundation for effective risk management and ensures significant ICT risks and their potential business impacts are identified and assessed in a timely manner.

The primary questions addressed by the risk assessment process are:

***Risk assessment questions***

- What are the specific inherent ICT risks to your business outcomes?
- What might cause these risks to occur (e.g. what are the internal and external causes of the risk)?
- What's the likelihood these risks will occur?
- What are the consequences (business impact) of these risks if they were to occur?
- What mitigating processes and/or controls are currently in place to manage risks?
- How confident are you that risk and control interventions are operating effectively?
- Are you comfortable with the level of residual risk after taking these risk and control interventions into account?
- What additional actions (if any) should be taken to further manage this risk?

The risk assessment process covers three key activities:

- Risk identification
- Risk analysis
- Risk evaluation

These are described in more detail below.

## 4.1 Risk identification

Once you have established the context for the risk assessment, the next step is to identify the ICT risks that threaten the achievement of your business objectives or that create an opportunity to exceed them. There are numerous risk identification techniques you can use:

- One-to-one interviews
- Group discussions/facilitated workshops
- Questionnaires/surveys
- Strengths, weaknesses, opportunities, threats (SWOT) analysis
- Dependency modelling
- External environment/horizon scanning

- Scenario analysis
- Process mapping.

The techniques you use will vary depending on the nature of the risk assessment being performed. For example, at the business unit level you may use a combination of one-to-one interviews and then group discussion to gain consensus. The important thing is to find ways to consider all possible sources of ICT risk. Refer to Appendix A for an example of an ICT risk universe.

### 4.1.1 Types of risk

In identifying and then subsequently managing risks, it can be helpful to consider different types of risk. There is no one standard classification system for different types of risk. As a minimum, we recommend identifying strategic risks versus operational risks. This is because strategic risks and operational risks will likely be owned and managed at different levels within the organisation, and different escalation paths may be used.

### 4.1.2 How to state risks

There are three elements for stating risks:

1. **Event:** A risk event is defined as something that could prevent the achievement of an objective, milestone or target or something that could create an opportunity to exceed any of these things.
2. **Causes:** The event may occur as a result of a number of causes that may be internal or external. Identifying the causes of a risk event will help you to better understand the risk and the interrelationships between different risks. This will help you put the right prevention strategies in place.

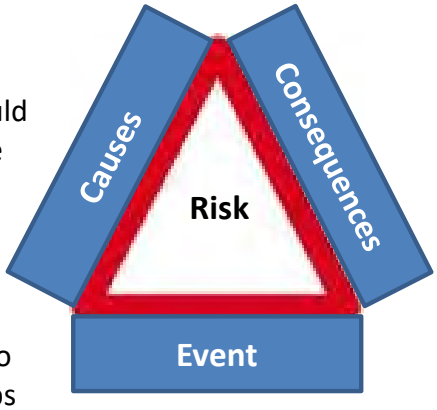



*Figure 2: Elements of risk*

3. **Consequences:** The consequences describe the outcomes of the risk event, if it were to occur. These may include service interruption, safety, financial, reputational and/or regulatory impacts. Understanding the consequences of risks allows you to ensure you have the appropriate strategies in place for risk mitigation and/or recovery.

By acting on any one of these three elements, you can affect the risk rating.

### 4.1.3 Who owns a risk?

There should be a single point of ownership for each risk. A risk owner should have the authority to influence the risk outcome and be held accountable for doing so. In many instances risk ownership is clear. However, conflicts and confusion over accountability can arise where risks cross functional boundaries, which can often be the case for ICT risks.

In selecting the most appropriate risk owner, it is important to consider the source of the risk and the risk-bearing function i.e. the business unit that will be most impacted by the risk should it occur. We recommend the risk owner is someone in the risk-bearing function, as they will be incentivised to manage the risk effectively. However, the most important consideration is for the risk owner to have the authority to hold other business units accountable for managing their contribution to the risk outcome.

For example, a business unit is dependent upon the availability of an ICT system that is critical for their work. The source of the risk is the failure of the system, which is influenced by the ICT function. However, it is the business unit that is dependent on the system that bears the risk because it will the one that's most impacted should the system fail. In this case, risk ownership lies with the business unit as it is the business unit that defines the availability, continuity and recovery objectives for the system and holds the ICT function responsible for meeting these.

## 4.2 Risk Analysis

Risk analysis involves three steps:

1. Assess the likelihood and impact of the risk occurring in the absence of mitigating controls. This is referred to as the inherent risk rating and should be based on normal circumstances i.e. the most probable case as opposed to the worst-case scenario. Refer to Appendix B for an example of risk likelihood and impact rating criteria.

2. Identify and assess the effectiveness of existing controls that are in place to mitigate the risk. Assessing control effectiveness accurately is important for making an accurate assessment of residual risk. Refer to Appendix C for an example of control effectiveness ratings.

   To assess the effectiveness of a control, the control needs to be evaluated on multiple levels, as illustrated by Figure 3 below.

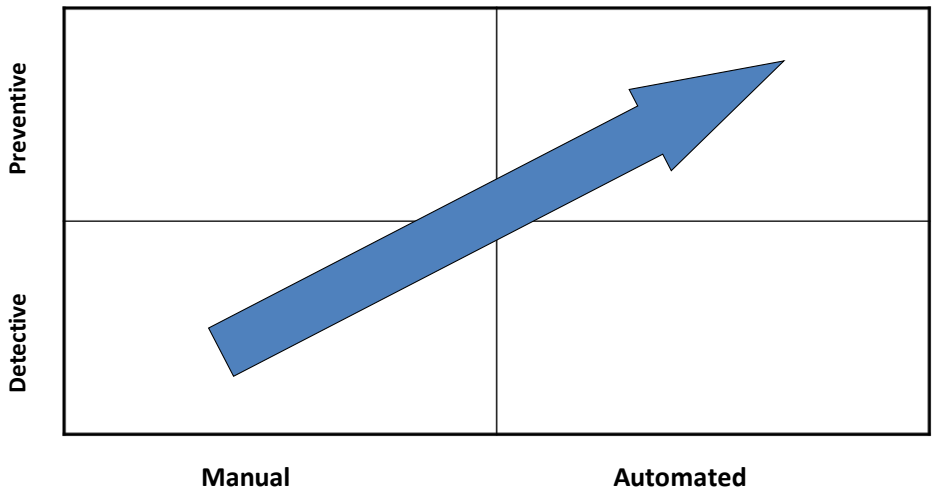



*Figure 3: Types of controls*

- Preventative controls stop the risk from occurring. These tend to be mostly automated actions performed by a system.
- Detective controls usually identify risks after they have occurred. These tend to be manual (although some manual controls may rely on information generated by systems, but the control itself is still performed manually).

You should consider the following factors when rating control effectiveness:

***Assessing control effectiveness***

- How well is the control designed to mitigate the risk?
- Is the control consistently applied?
- Can the control be overridden?
- Is there evidence of the control being applied?
- Is the effectiveness of the control monitored?
- How well is the control understood?

3. Assess the residual risk rating based on the effectiveness of mitigating controls. As a rule, controls reduce the likelihood of the risk occurring. Some controls, however reduce the impact of the risk once it has occurred e.g. a business continuity plan may reduce the impact of a natural disaster but not the likelihood of it occurring.

Although the first step of risk analysis will generally represent an artificial environment, when you consider it in conjunction with the second and third steps, it gives you a framework you can use to assess the existence and effectiveness of the controls that are believed to be in place. It can also lead to a re-assessment of whether the cost of these controls is still justified.

This three-step risk analysis approach will help make sure all key risks are recorded and that judgments about the appropriate management of those risks are substantiated.

## 4.3 Risk evaluation

The final step in the risk assessment process is to evaluate whether the residual risk rating is acceptable or unacceptable. This is based on an assessment of the target risk rating.

The relationship between inherent, residual and target risk is shown in the heat map in Figure 4 below.

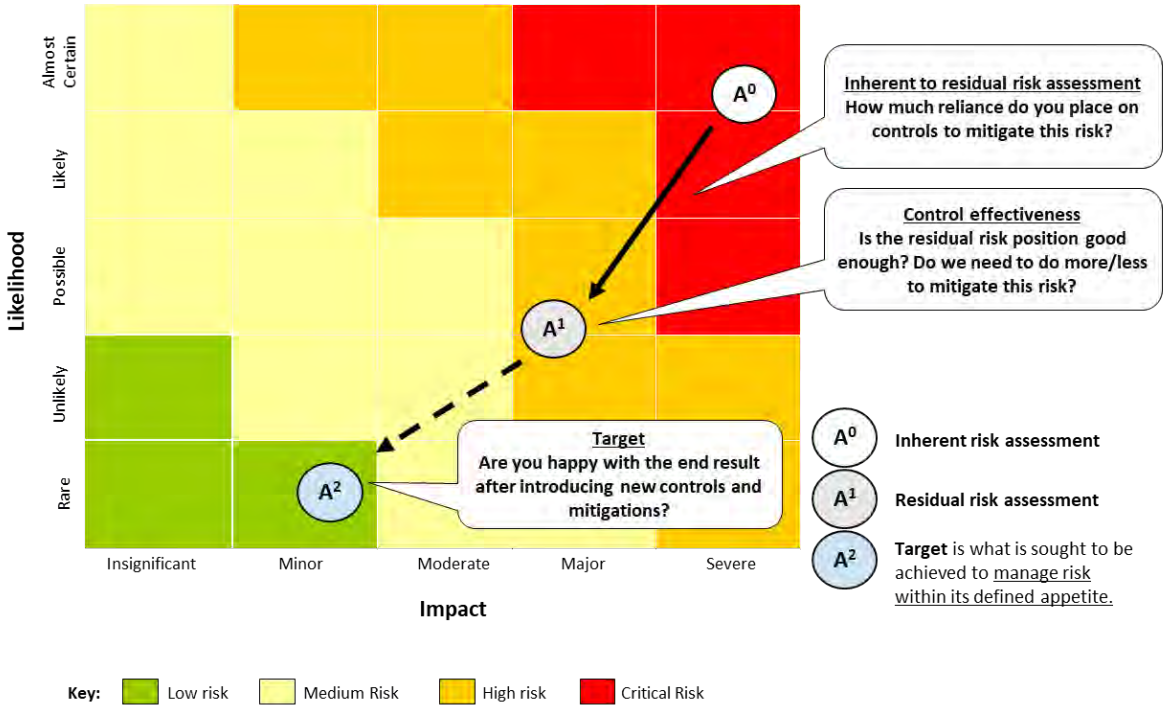



*Figure 4: Relationship between inherent, residual and target risk*

A risk is considered 'acceptable' if the residual risk rating is equal to or less than the target risk rating. No further action is required beyond maintaining existing controls.

This does not mean the target risk rating must always be Low for the risk to be accepted. The evaluation of the target risk rating considers the:

- Organisation's overall appetite for the risk
- Degree of control the organisation has over the risk
- Cost, benefits and opportunities presented by the risk.

For example, a Medium residual risk related to a new digital channel or service may be deemed acceptable because the opportunities presented outweigh the threats to such a degree that the risk is justified.

# 5 Risk Treatment

There are four ways to deal with a risk:

***4 T's of risk management***

- **Tolerate** (or retain): Deciding that a risk is acceptable. A risk is considered acceptable if it equals the target risk rating and no further action is required.
- **Treat** (or reduce): Putting in place controls that bring the risk down to an acceptable level. This is the most common form of risk treatment.
- **Transfer**: Passing the risk on to someone else e.g. by using insurance or by outsourcing a service where there is no in-house expertise.
- **Terminate** (or avoid): Simply not undertaking the activity that is causing the risk, in which case you will need to change your plans to avoid the risk altogether.

## 5.1 Risk improvement plan

Risk owners should develop a risk improvement plan whenever the residual risk rating is greater than the target risk rating. The risk improvement plan documents:

- The management actions to be taken to reduce the risk to an acceptable level
- The people responsible for implementing the actions
- Due dates for completion.

The risk owner is ultimately responsible for the risk improvement plan but may delegate responsibility for implementing actions to others who have appropriate authorisation to do this.

## 5.2 Root cause analysis

When developing a risk improvement plan, it is important to consider the root causes of the gap between the residual and target risk ratings and make sure management actions appropriately address these. You should review:

- The causes of the risks that have been identified as part of the risk assessment process
- The impact of the risks on other areas of responsibility
- Third parties and their ability to control and mitigate the risk.

## 5.3 Cost-benefit analysis

Suggested management actions should be subject to a cost-benefit analysis in the same way as other new initiatives. This is to ensure that actions are cost effective and will achieve the desired risk reduction in the risk rating.

# 6 Monitoring and reporting

Monitoring and reporting are essential steps in the risk management process. However, they should not be viewed as something separate or stand-alone. Instead, integrate risk monitoring and reporting into the regular rhythm of business performance measurement, reporting and governance.

## 6.1 Monitor risks

To ensure risk information remains current and dynamic, consider the following questions:

***Risk monitoring questions***

- Have there been any changes in the underlying causes of the risk?
- Has there been an increase/decrease in the number of incidents of the risk occurring?
- Have assurance reviews been completed for the risk or for the supporting controls? If so, what issues were identified and how do they impact the control effectiveness rating in the risk register?
- Have systems, controls and processes been stable or subject to recent change?
- Have there been any changes to the level of resources or budgets?
- Have there been any changes in the external environment that may create new risks (e.g. new legislation)?

## 6.2 Establish metrics

Establish metrics to monitor key risks. In many instances, these will be existing Key Performance Indicators (KPIs), but they should also include leading indicators of risk. This will help to integrate risk information into business performance and support the flow of risk information up through the organisation to provide early warning of a changing risk profile.

# 7 Communication and consultation

The goal of communication and consultation is to support good risk conversations that are based on relevant, accurate and timely information. Good risk conversations help to elicit information and manage stakeholder expectations for managing risk. This includes:

- Helping to develop a common understanding of diverse views
- Promoting timely action
- Ensuring effective risk management contributes to the achievement of strategic and business outcomes.

As such, communication and consultation should take place during each step of the risk management process. This should identify who should be involved in the assessment of risk, including those who will be involved in the treatment, monitoring and review of risk. It is very rare that only one person will hold all the information needed to identify and manage risks to an activity or change. So, it is important to identify the range of stakeholders, both internal and external, who will help develop a complete picture of the risks.

It is important to ensure that all staff understand, in a way appropriate to their role, their responsibilities for managing risk. If you don't achieve this, the organisation's risk culture may not be aligned to achieving successful business outcomes.

***Tips for effective communication and consultation***

- Ensure stakeholders understand their risk management responsibilities and what is expected of them.
- Focus risk conversations on business objectives and values.
- Make sure the right people are involved in the discussion.
- Encourage stakeholders to take ownership of their risks, including developing risk improvement plans and regularly monitoring risks.
- Give stakeholders the relevant information they need prior to the discussion.
- Ensure good risk conversations happen regularly.

# 8 Engaging with us

## 8.1 Lifting risk management and assurance capability

The System Assurance team works collaboratively with government organisations to lift risk management and assurance capability. Further information on the role of the System Assurance team can be found on the GCDO's website: https://www.digital.govt.nz/standards-and-guidance/governance/system-assurance/role-of-the-system-assurance-team/

For the AoG Enterprise Risk Maturity Assessment Framework visit: https://www.digital.govt.nz/standards-and-guidance/governance/system-assurance/enterprise-risk-maturity/

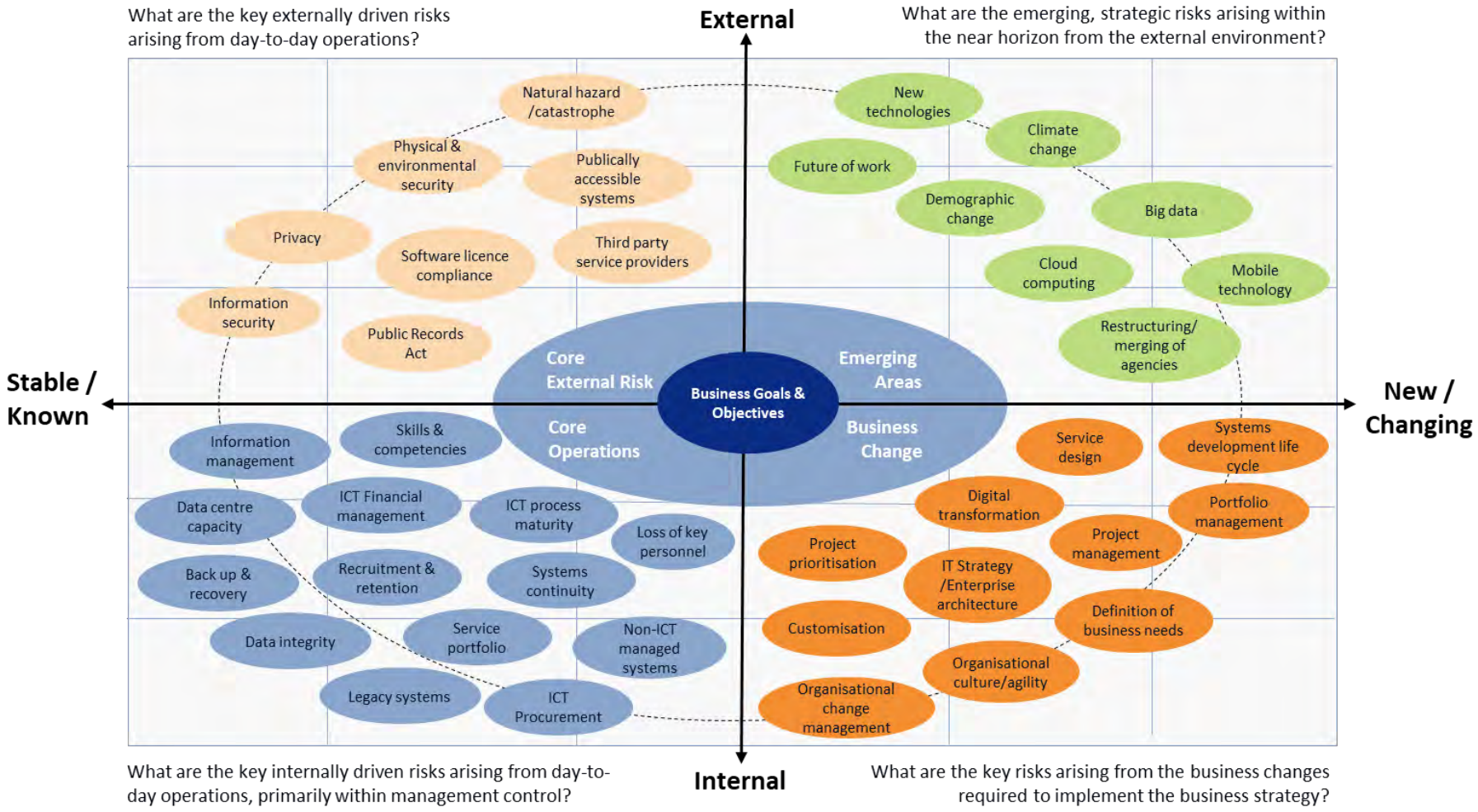
## 8.2 Guidance and templates

Further guidance and templates, including risk register and heat map templates, can be found on the GCDO's website: https://www.digital.govt.nz/standards-and-guidance/governance/system-assurance/all-of-government-ict-operations-assurance-framework/guidance-and-templates/

## 8.3 How to contact us

The System Assurance team can be contacted for ICT risk management and assurance queries, advice and guidance at systemassurance@dia.govt.nz

# Appendix A – Example of an ICT risk universe



# Appendix B – Example of likelihood and impact rating criteria

| Rating | Description | Probability | Criteria |
|---|---|---|---|
| 1 | Rare | < 5% chance of occurring | May occur in specific or exceptional circumstances/no known history or has happened rarely |
| 2 | Unlikely | 5-35% chance of occurring | Not expected but could occur at some time/has happened rarely |
| 3 | Possible | 36-65% chance of occurring | Might occur at some time/has happened occasionally |
| 4 | Likely | 66-85% chance of occurring | Has happened/probably will occur in most circumstances |
| 5 | Almost certain | > 85% chance of occurring | Regularly happens/expected to occur in most circumstances |

| Rating | Description | Criteria |
|---|---|---|
| 1 | Insignificant | • No visible impact on reputation of the organisation<br>• Financial impact manageable within existing budget<br>• Negligible impact on business objectives and strategic outcomes<br>• Isolated interruption to service delivery which can be resolved quickly via standard operating procedures<br>• Negligible impact on security, privacy, health and safety and/or staff wellbeing |
| 2 | Minor | • Limited reputational damage to the organisation; minor media criticism of the organisation<br>• Financial impact can be managed within existing budget with some minor re-planning<br>• Minor impact on business objectives and strategic outcomes<br>• Limited short term interruption to service delivery which can be resolved via standard operating procedures<br>• Minor breach of security, privacy, health and safety and/or staff wellbeing |
| 3 | Moderate | • Some political and/or reputational damage to the organisation; sustained media interest with criticism of levelled at parts of the organisation<br>• Financial impact can be managed within existing budget but requires re-prioritisation<br>• Some compromise on business objectives and strategic outcomes |



| Rating | Description | Criteria |
|---|---|---|
| | | • Disruption to service delivery with moderate impact on customers and/or key stakeholders<br>• Moderate breach of security, privacy, health and safety and/or staff wellbeing |
| 4 | Major | • Significant political and/or reputational damage with loss of confidence and trust in the organisation by Minister and/or public<br>• Significant re-planning and prioritisation of key activities; additional funding required to maintain core infrastructure<br>• Significant compromise on business objectives and strategic outcomes<br>• Major wide-spread disruption to service delivery impacting customers and/or key stakeholders<br>• Significant breach of security, privacy, health and safety and/or staff wellbeing |
| 5 | Severe | • Severe political and/or reputational damage with loss of confidence and trust in the organisation by Prime Minister and/or public<br>• Severe impact on financial sustainability of the organisation without significant cash injection<br>• Severe compromise on business objectives and strategic outcomes requiring broad realignment of the organisation's activities<br>• Mission critical disruption to service delivery impacting customers and/or key stakeholders over a prolonged period<br>• Serious and sustained high profile breach of security, privacy, health and safety and/or staff wellbeing |



# Appendix C – Example of control effectiveness ratings

| Rating | Description | Impact on Risk Rating |
|---|---|---|
| Effective | Risk exposure is effectively controlled and managed | Where controls are deemed to be effective, the residual risk rating is usually expected to be lower than the inherent risk rating. However, for some risks, where it is only possible to reduce the likelihood of the risk and not the impact, the residual risk rating may remain High despite having effective controls in place. |
| Partially Effective | Some of the risk exposure is controlled; however, there are some deficiencies in control measures | Depending on the nature of the deficiencies identified, partially effective controls may still reduce the inherent risk rating. However, care should be taken to carefully assess the nature of the deficiencies to ensure an accurate assessment of their impact on the residual likelihood and impact ratings. |
| Ineffective | Control measures are ineffective | Typically, an ineffective rating would not be expected to reduce the residual risk rating. If this is the case, you should re-review your assessment of the residual likelihood and impact ratings to ensure these are accurate. |



# Glossary of terms and abbreviations

| Term | Definition |
|---|---|
| **AoG Enterprise Risk Maturity Assessment Framework** | A framework that allows government organisations to objectively measure their current level of risk management capability and identify improvement opportunities that will enable them to reach a higher level of maturity. |
| **Assurance** | Assurance is an independent and objective assessment that provides credible information to support decision making. Assurance provides confidence to governance bodies and management. |
| **Control** | A control is any measure or action that modifies risk. This may include any policy, procedure, practice, process, technology, technique, or method. Risk treatments become controls, once they are implemented. |
| **Control effectiveness** | Control effectiveness is a measure of the strength of a control that is implemented to mitigate the risk. For example, a weak control may be ineffective if there are significant factors outside of an organisation's control. |
| **Enterprise risk management** | Enterprise risk management is a top-down, enterprise-wide approach to managing all the risks that an organisation is exposed to versus a traditional silo-based approach. |
| **Function** | A function is a business unit or business group that performs a specific role within an organisation, such as finance, ICT or human resources |
| **Governance body** | A governance body is a group of people with the authority to challenge and exercise oversight over the organisation's risk profile as whole or in a key risk area. It may be a separate board, committee or a sub-committee. |
| **Heat map** | A heat map is a visual representation of risk profile. Also known as a risk map, it is a data visualization tool, for communicating specific risks an organisation faces. It also helps to identify and prioritize the risks to be managed based on the organisational risk context and criteria. |
| **ICT risk** | The business risk associated with the use, ownership, operation, involvement, influence and adoption of information and communications technology (ICT). |
| **Impact** | An impact is the outcome of a risk event and severity of the consequence should the risk actually occur. It has an effect on the achievement of business objectives and outcomes. A single event can generate a range of consequences which can have both positive and negative effects. |
| **Inherent Risk** | Inherent risk refers to the level of risk without taking into account the effectiveness of existing controls. |
| **Level of risk** | The level of risk (or magnitude) estimated by considering and combining likelihood and impact ratings. |
| **Likelihood** | Likelihood is the probability or chance that risk will occur. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively (using mathematics). |
| **Residual risk** | Residual risk refers to the level of risk remaining after taking into account the effectiveness of existing controls. |

| Term | Definition |
|---|---|
| **Risk** | Risk is the "effect of uncertainty on objectives" and can include both positive or negative impacts. |
| **Risk appetite** | Risk appetite is a high-level (usually narrative) expression of the amount and type of risk that an organisation is willing to take in the pursuit of its business objectives and outcomes. |
| **Risk-bearing function** | The risk-bearing function is the business unit that will be most impacted by the risk, should it occur. |
| **Risk improvement plan** | A risk improvement plan documents the management actions to be taken to reduce the risk to an acceptable level, those responsible for implementation and due dates for completion. |
| **Risk management capability** | Risk management capability defines the culture, practices, experience and application of risk management within an organisation. |
| **Risk management framework** | A risk management framework describes the organisational arrangements that are put in place to systematically identify, analyse, evaluate, treat, monitor and review risk. |
| **Risk improvement plan** | A risk improvement plan documents the management actions to be taken to reduce the risk to an acceptable level, those responsible for implementation and due dates for completion. |
| **Risk management process** | A risk management process systematically applies management policies, procedures, and practices to a set of activities intended to establish the context, communicate and consult with stakeholders, and identify, analyse, evaluate, treat, monitor, record, report, and review risk. |
| **Risk mitigation** | Risk mitigation refers to the actions taken to further mitigate the level of risk to an acceptable level. Sometimes referred to as risk treatment. |
| **Risk owner** | A risk owner is a person or entity that has been given the authority to manage a particular risk and is accountable for doing so. |
| **Risk profile** | A risk profile is a written description of a set of risks. A risk profile can include the risks that the entire organisation must manage or only those that a particular business unit or part of the organisation must address. |
| **Risk source** | A risk source has the intrinsic potential to give rise to a risk. It is where a risk originates from and could generate a risk that must be managed. |
| **Risk tolerance** | Risk tolerance is the specific maximum amount of risk (exposure) that an organisation is willing to take / accept regarding each risk to which it is exposed. |
| **Risk universe** | The risk universe contains all potential and existing risks that could affect an organisation. |
| **Target risk** | A target risk is the risk rating after actions from a risk improvement plan have been implemented. |