ICT Risk Management Guidance

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.

Context

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

"ICT risk refers to the business risk associated with the use, ownership, operation, involvement, influence and adoption of ICT within the department[1]."

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.

Benefits of risk management

Effective ICT risk management helps 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 Queensland Government Chief Information Office

Government Chief Digital Officer System Assurance Team

New Zealand Government

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.

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.
- The **second line of defence** is the governance and oversight arrangements that exist for ongoing monitoring of ICT risks.
- The **third line of defence** is the independent assurance you get from Internal Audit and third party assurance providers, including External Audit, that ICT risks are effectively managed.

Below is an example of how the three lines of defence model can be applied to ICT security risk.

First line of defence	**Application and Systems Support Manager** • There is a documented procedure for patch management • Review of weekly patch management status report by Support Manager
Second line of defence	**Security and Risk Manager** • Level of patching and associated risk exposures reported on a monthly basis to Security and Risk team • Quarterly security risk report to ICT Leadership team
Third line of defence	**Third party assurance provider** • Annual security review of vulnerable systems

Role of Executive Leadership team

The Executive Leadership team (ELT) has primary responsibility for risk governance and overseeing the top risks (i.e. those rated Critical or High) faced by the government organisation. This includes ensuring that risk management is embedded into the organisation's governance, decision-making, and reporting structures to promote a robust risk management culture.

Establishing the context

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.

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?

Risk assessment

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

Risk assessment questions

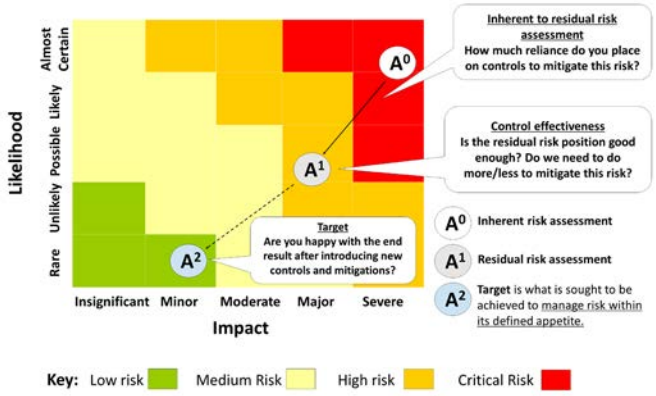
- What are the specific inherent ICT risks to your business outcomes?
- What might cause these risks to occur (e.g. what are the internal and external causes of the risk)?
- What's the likelihood these risks will occur?
- What are the consequences (business impact) of these risks if they were to occur?
- 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 assessment activities

- **Risk identification:** Identify the ICT risks that threaten the achievement of your business objectives or that create an opportunity to exceed them.
- **Risk analysis:** Assess the likelihood and impact of the risk occurring; identify and assess the effectiveness of existing controls that are in place to mitigate the risk; and assess the residual risk rating based on the effectiveness of mitigating controls.
- **Risk evaluation:** Evaluate whether the residual risk rating is acceptable or unacceptable based on an assessment of the target risk rating.

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



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, for example, insurance or 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.

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.

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 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 risk (e.g. new legislation)?

Communication and consultation

Good risk conversations help to elicit information and manage stakeholder expectations for managing risk.

Tips for effective communication and consultation

- Focus risk conversations on business objectives and values.
- Make sure the right people are involved in the discussion.
- Provide stakeholders with relevant information prior to discussion.
- Ensure good risk conversations happen regularly.

Contact us

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

Additional guidance and templates can be found on the GCDO's website: bit.ly/2ZQCCbo

For the AoG Enterprise Risk Maturity Assessment Framework, visit: bit.ly/2J9NURC