ACT Government | ACT Health

Table of Contents

Overview

The ACT Health's Directorates **Enterprise Risk Management (ERM) Framework** guides and links the overall structure for enterprise risk, our policy and its effect on the culture of the organisation. Our **ERM Plan** outlines accountabilities and resources, our **ERM Guide** has a step by step process for risk management and its application at a practical level.

Our ERM Framework

Our goal with the ERM framework is to ensure that it clearly supports our people when considering risk and when undertaking risk management. Simply, we seek to ensure that risk management is both considered and integrated into all critical decision-making processes associated with the ACT Health Directorate.

Our framework, at its foundation aligns with the current Australian Standard – AS ISO 31000:2018 Risk Management Guidelines1 (the Standard) and mirrors its application through and in accordance with the *ACT Government Risk Management Policy* and its attributes, namely:

- *Attribute 1* - Cultivating a positive risk culture;
- *Attribute 2* - Establishing a risk management framework and policy;
- *Attribute 3* - Establishing a robust risk assessment process - a risk management plan;
- *Attribute 4* - Defining responsibility and accountability;
- *Attribute 5* - Aligning our risk management with our strategic objectives; and
- *Attribute 6* - Embedding risk management into all operations and processes.

This framework recognises that within the ACT Government, current legislation requires all ACT staff to manage risk, and to ensure that they comply with legislation including, but not limited to:

- *the Public Sector Management ACT 1994;*
- *the Financial Management Act 1996;*
- *the Insurance Authority Act 2005; and*
- *the Work Health and Safety Act 2011.*

Key Elements of the ERM Framework

- The Directorate aligns its risks to the Strategic Plan and through it the organisation's objectives;
- Policy Statement – this policy articulates the Directorates approach to risk;
- The ERM Plan defines -
    - the roles, accountabilities and responsibilities of our people;
    - the resources available in support of enterprise risk management in the Health Directorate; and
    - the various reporting and communication mechanisms for staff undertaking risk management in the organisation.
- The ERM Guide- a step by step process using the *ACTIA Risk Management Implementation Guide and the ACTIA Risk Matrix*, addressing how, why and when risks are managed and escalated;

1 AS ISO 31000:2018 Risk Management Guidelines

- Tools (an addendum of the Guide) - these include links to the ACT Government Risk Management Policy and Guidelines, AS ISO 31000:2018 Risk Management Guidelines1, as well as in house risk registers;
- Training (an addendum of the Guide), this area identifies opportunities for further refinement through an online training module (under development) and links to both internal help and external resources for staff when undertaking risk management activities for the organisation; and
- An intranet presence housing all items associated with the framework.

Enterprise Risk Management

Enterprise risk is the integration of risk into and across critical business processes, it impacts on the culture of the organisation, it considers aspects such as the assessment of risk in terms of its effects across the organisation, and it effectively seeks to manage, monitor and report on risk in a quality review cycle seeking to improve on both its use and integration across the organisation.

Diagram 1: A visual representation of how risk is considered across the enterprise

Risk Management – the concept

Risk is defined as the 'effect of uncertainty on objectives'1; and risk management as 'coordinated activities to direct and control an organisation with regard to risk'1.

In the Directorate, we look at risk and its management from two perspectives; one that considers events that may have a negative impact on our business (i.e. threats), and one that considers embracing some level of risk as an opportunity.

In undertaking risk management, staff are directed to consider issues or events that may impact on expected results – positive or negative. Our risks are assessed in terms of the consequences of an event, and the likelihood of that event happening; and we do this in accordance with the Australian Standard, AS ISO 31000 Risk Management Guidelines1, and specifically utilise the ACTIA Risk Matrix for this activity.

Policy Statement

The ACT Health Directorate is committed to achieving best practice in the management of risk that may impact on the organisation meeting its objectives.

Our risk management practices align to the Australian standard of risk management AS ISO 31000:2018 Risk Management Guidelines1; and the policy and guide to risk management provided by ACTIA – *ACT Government Risk Management Policy/Implementation Guide 2019* for managing and reporting on risk.

Dependent on the type of risk its severity and controls attributed, we follow defined processes for assessment, ownership, on-going management and reporting obligations, as outlined in the **ERM Plan and Guide.**

Risk Policy Environment

The Directorate, as the steward of health and health services in the Australian Capital Territory (the Territory) and its regions faces a broad range of risks that reflect its unique responsibilities.

Typically, these risks can affect our:

- reputation and our ability to manage and effectively deliver high quality health services;
- ability to behave strategically and deliver value to the people of Canberra and its regions both now and in the future;
- financial stability, and longevity; and
- ability to ensure the well-being of people, including our workers and stakeholders.

Considering Our Risk Appetite and Tolerance1

The difference between appetite and tolerance of risk

Simply, **risk appetite** is the amount of risk, on a broad level, that the Directorate's Executive are willing to accept in the pursuit of the organisation's objectives. Tolerance relates to specific levels of variation that the organisation is willing to accept around specific objectives. For example, a project may be a high-risk venture that is considered tolerable for a specific objective – greater reward.

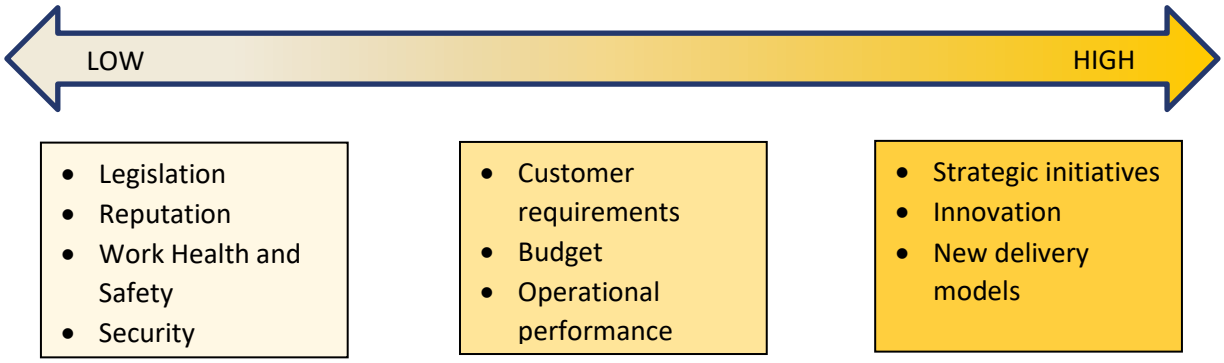

Diagram 2: A graphical representation of our risk appetite and tolerance for Risk

Appetite and tolerance defined

Risk appetite is defined as 'the amount of risk an entity is willing to accept or retain to achieve its objectives. It is a statement or series of statements that describes the entity's attitude toward risk taking.'2

The Directorate's risk appetite involves effectively managing uncertainty, not avoiding or eliminating risk. A higher risk appetite in some sectors allows us to consider opportunities that involve the acceptance of some risk. Our goal is to consider risk and then manage, mitigate or embrace risk and monitor and report on risk. Accordingly, the Directorate is prepared to pursue, retain or accept risk that has been well considered, thoroughly assessed and is managed and monitored appropriately. The Directorate has generally a low appetite for any risk that will affect our management and through it our stewardship of health services delivery for the Territory and region.

Risk tolerance is defined as 'the maximum level of risk an entity can accept within the risk appetite without hindering the achievement of its strategic objectives or operating plan.'2.

Dependant on the objective, the Directorate will tolerate higher risk levels for specific circumstances. By way of example, this may take the form of innovative concepts around service delivery models. Consideration and acceptance of any high-risk ventures would typically be at the Directorate Leadership Committee level.

2 ACTIA – ACT Government Risk Management Policy/Implementation Guide 2019

Risk Management Process - (Defined in detail in the **ERM Guide**)

We consider the value of our objectives (as identified in our planning documentation - strategic, divisional, branch and project/team) and the risk to them, and then we assess and consider if the process or its reporting would benefit from documenting the exercise using the risk assessment template. By way of example, a complex project may require a detailed risk analysis to be undertaken, complete with documentation, while for a simple activity this may not be appropriate with the cost involved (time and effort) and may not justify the benefit.

When we assess risk, we consider the current measures that are in place ('controls') and their effectiveness. Using the ACTIA matrix, risks are given a rating (low to extreme). Further measures ('treatments') can then be considered to ensure that the risk is further mitigated, actively managed, transferred or eliminated. When we document this evaluation process, we generally use templates (risk registers); This ensures consistency of approach, risk ownership, ongoing monitoring and reporting across the organisation.

Specific risk tolerances can and would typically be determined by the appropriate risk owner to manage risk to a level that is reasonably practical. The ERM Guide expands on the concept below and gives practical examples in support. The diagram below maps out this process of evaluation, assessment, documentation and review.

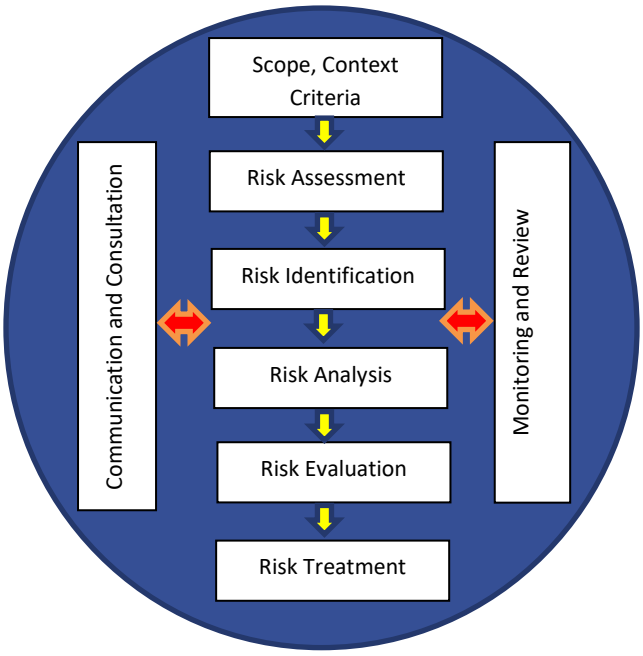

Diagram 3: ***The Risk Assessment Process, AS ISO 31000:2018 Risk Management Guidelines***1

Risk – Governing in terms of the Enterprise

In the Directorate we integrate our risks into our business that enables linkages from lower risks to be brought to the attention of management and into the strategic risk profiles; This enterprise approach enables clear monitoring and reporting lines to be established. The below diagram provides a visual representation of this process and the individuals that take responsibility for both the ownership and reporting of risk in the organisation.

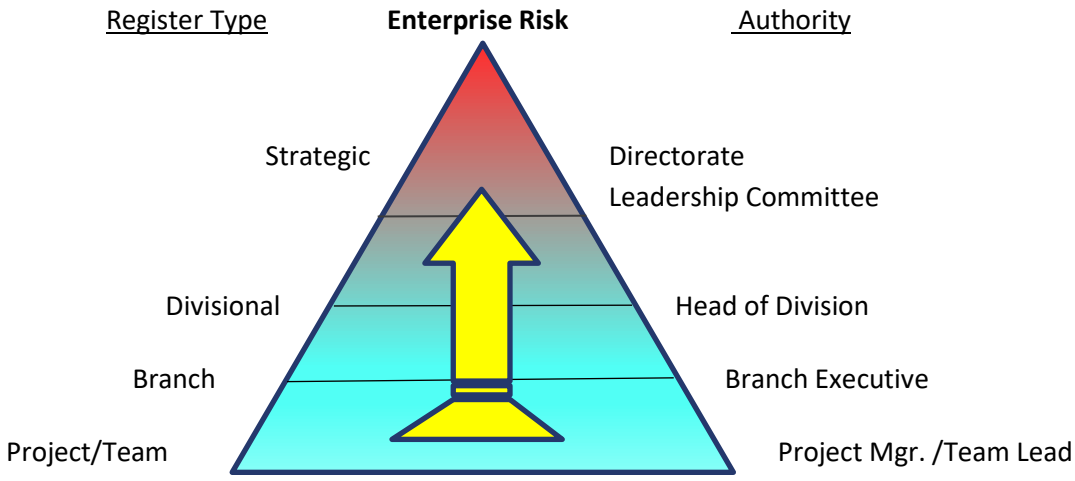

Diagram 3: ***Risk linkages from the lowest to the strategic***

Governance Forum

A governance forum that meets quarterly, with a representative from each Division (nominated by the Executive at the EO level – Senior Officer C) has been established. Topics coved by this forum include Risk Management, Delegations; Audits (internal and External); FOI – issues of note. Members of this forum represent the conduit for information exchange to the divisions and the leadership, the group discusses any proposed changes to Governance related initiatives, with the goal of continual improvement and embedding governance into the business streams, e.g. Risk Management. The forum members also advise their Division of any training and resources that become available through the Governance and Risk Branch of the organisation. The secretariat for this forum is the Governance and Risk Branch – specifically the Director of Enterprise Risk management.

Escalation of Risk – Risk that may impact on a higher-level register

Any risks that may need to be escalated upwardly i.e. Project to Branch, to Division, to Group, to Strategic should be advised to the Director Enterprise Risk Management, Governance and Risk Branch, ACT Health Directorate. Risks will then be considered for inclusion at the next level. In addition, emerging risks and general discussion on risk treatments and controls are standing items for discussion at each of the governance forum meetings.

Documenting Risk

When the Directorate considers risk, and its effects on meeting our objective at any level, we effectively map the risk, assign ownership, and define its rating (e.g. Low, Medium, High or Extreme risk), along with controls treatments etc.

Post the mapping exercise we then consider the risks priority for attention Low (1-3 months), Medium (within 3 months), High (within 7-14 days) or Extreme (within 24 hours). In addition, we consider our identified controls and their effectiveness as inadequate, room for improvement or adequate.

All the information in the above is documented in our standardised risk register – they all look the same whether be it the strategic risk register, or the down to the project/team risk register. They, by necessity have varying reporting obligations. The detail associated with the assessment, mapping, associated controls, risk ownership, monitoring and reporting obligations etc. are articulated in the Directorate's **ERM Guide**.

Related Documents

- **The ERM Plan**: ***defines***
  - the roles, accountabilities and responsibilities of our people;
  - the resources available in support of enterprise risk management in the ACT Health Directorate; and
  - the various reporting and communication mechanisms for staff undertaking risk management in the organisation.
- **The ERM Guide: provides**
  - an overview of risk management and its implementation in the ACT Health Directorate;
  - a step by step process for conducting a risk assessment; and
  - practical examples for completing a risk assessment utilising the ACTIA Rix Matrix and guidance for completion of your risk register.

Training

- Training – an overview of risk management is provided through the induction program for new starters in the Directorate (in progress) – all and any staff are welcome to attend to refresh their appreciation of risk management;
- Individual training and/or guidance is available now for all staff in the organisation on request – contact the Director of Enterprise Risk Management on EXT. 49702 for details; and
- Our ACTHD Risk Management intranet page, which can be accessed from the Governance menu on the HealthHub home page. The page has linkages to an online training module provided by ACTIA.

Some useful Hyper-links to Risk Management material (on line version)

- Australian Standard, AS ISO 31000:2018- Risk Management Guidelines;
- ACTIA – the Authority for Risk Management in the ACT Government; and
- The Institute of Internal Auditors Australia – a link to gaining formal qualifications as a Certified Practicing Risk Manager (CPRM); an internationally recognised certification.

Practical Help

- **We are here to help – please call Ext. 49702 to talk to the Director Enterprise Risk Management.**

Legal based documents

Legislation:

- *the Public Sector Management ACT 1994;*
- *the Financial Management Act 1996;*
- *the Insurance Authority Act 2005; and*
- *the Work Health and Safety Act 2011.*

Policies, Guides and Standards used in Risk Management in the Directorate

- *Australian Capital Territory Insurance Authority (ACTIA) provided ACT Government Risk Management Policy and Implementation Guide; and*
- *Australian Standard, AS ISO 31000:2018- Risk Management Guidelines.*

ACT Health acknowledges the Traditional Custodians of the land, the Ngunnawal people. ACT Health respects their continuing culture and connections to the land and the unique contributions they make to the life of this area. ACT Health also acknowledges and welcomes Aboriginal and Torres Strait Islander peoples who are part of the community we serve.

www.health.act.gov.au | Phone: 132281 | Publication No XXXXX