ACT Health

Table of Contents

Purpose

This plan supports the integration of enterprise risk management at the ACT Health Directorate (Directorate) and is aimed at embedding Risk Management into all critical business areas of the organisation.

It contains the roles of those accountable and details those activities that will ensure its effective integration.

This plan articulates opportunities and objectives, accountability requirements; resources and training; communication and reporting requirements.

This plan should be read in conjunction with the [Enterprise Risk Management (ERM) Framework](#).

Objective of this Plan

The objective of this plan is to ensure that:

- the Directorate's approach to risk management is fit-for-purpose, aligned with the whole of Government guidance (ACT Government Risk Management Policy and Guide) through the Australian Capital Territory Insurance Authority (ACTIA) and is continuously reviewed and improved;
- systematic risk management processes are effectively and consistently embedded into business processes at the Directorate;
- effective communication and consultation about risk occurs throughout the organisation;
- staff have the appropriate tools, training and resources in order to manage risk consistently and effectively within their span of control; and
- the risk culture at the Directorate continues to mature.

Accountability

The ultimate responsibility for enterprise risk management in the Directorate rests with the Director-General. *The Financial Management Act 1996 (FMA Act)* states that the Director-General must manage the Directorate in a way that:

(a) promotes the achievement of the purpose of the Directorate;

(b) promotes the financial sustainability of the Directorate; and

(c) is not inconsistent with the policies of the government.

In achieving these goals, and in terms of risk:

'Territory entities must establish and maintain effective risk governance that includes an appropriate internal management structure and oversight arrangements for managing risk'[1]. Accordingly, the Directorate's aim is to have:

(a) an appropriate system of risk oversight and management for the organisation;

(b) an appropriate system of internal control for the organisation; and

---

[1] ACT Government Risk Management Policy 2019 and Implementation Guide

(c) appropriate guidance for officials of the organisation to effectively meet their related Legislation and Policies obligations in terms of risk management.

Roles and Responsibilities

The **Director-General** is responsible for ensuring the effective management of risk across the Directorate with the support of the Deputy Directors-General's and the Group General Managers.

The **Deputy Directors-General's** are responsible for promoting the application of risk management principles and ensuring that risk management is embedded into all critical business activities, processes and systems. They are also responsible for ensuring that staff within their respective Groups and associated Divisions have the appropriate tools, training and resources in order to manage risk consistently and effectively, to achieve division objectives.

The **Directorate Leadership Committee** is responsible for:

- governing the implementation of the ERM Framework and Plan and assessment criteria;
- determining the Directorate's risk appetite and tolerance;
- assessing, monitoring and reviewing identified, emerging and key strategic risks;
- periodic review of the Strategic Risk Register;
- overseeing the implementation of risk treatment strategies;
- reviewing whether a sound and effective approach has been followed in developing risk management plans for major projects or undertakings;
- periodically reviewing with the aim of improving the ERM Framework and associated plan and procedures; and
- reporting on the organisation's risk profile as appropriate in the annual report and as required by governing authorities (e.g. The Ministers Office; ACT Legislative Assembly; and, the Auditor General).

The **Audit and Risk Management Committee's** responsibilities regarding risk management are detailed in its charter2. It is responsible for ensuring:

- *ensuring that the Directorate has a sound enterprise risk management framework and associated processes for effective identification and management of business and financial risks, including those associated with individual projects and program implementation activities, business continuity management planning arrangements, legal and compliance risks; and*
- *the process for developing and implementing Directorate's fraud control and corruption prevention plan is sound and that the Directorate has appropriate processes and systems in place to detect, capture and effectively respond to fraud and corruption risks including reporting from the Senior Executive Responsible for Business Integrity Risk (SERBIR).*

---

2 ACT Health Directorate Audit and Risk Committee Charter (July 2019)

The **Divisional Executive Group Managers** and related **Executive Branch Managers** are responsible for:

- managing risk within their span of control;
- assisting with the identification of global or broadly-based risks that could impact on the Directorate as a whole, including risk treatment strategies in Group, Divisional, Branch and Team/Project Plans;
- reporting on risk matters to the Directorate Leadership Committee;
- raising awareness and organising risk management training within their Groups;
- integrating risk management into Group processes and plans;
- ensuring identified risks are adequately addressed;
- ensuring relevant Risk Registers are reviewed and kept current;
- promoting the application of risk management by contractors; and
- being familiar with and competent in the application of the Directorate Enterprise Risk Management Framework and Policy.

The **Director, Enterprise Risk Management** Corporate and Governance Branch and relevant staff within the section are responsible for:

- leading the implementation of this plan;
- developing and embedding a comprehensive enterprise risk management capability throughout the Directorate;
- maintaining the organisation's Strategic Risk Register and reporting on treatments, risk and changes to the risk profiles to the Directorate Leadership Committee and the Audit and Risk Management Committee;
- reviewing and improving the Enterprise Risk Management Framework to ensure that it continues to meet the needs of the Directorate;
- identifying Business Group risks that are classified as Extreme and requiring treatment, or common risks across divisions/groups that should link into the Strategic Risk Register and associated reporting obligations;
- reviewing developments in the field of risk management as well as changes to statutory, legislative and/or regulatory requirements at a strategic level;
- raising the awareness of risk management at the Directorate;
- coordinating risk management training for staff;
- ensuring that risk management tools and intranet accessibility is maintained and current;
- providing advice and disseminating risk management information; and
- providing regular reports to the Directorate Leadership Committee and the Audit and Risk Management Committee.

Managers and Supervisors are responsible for:

- managing risk within their span of control;
- supporting staff in assessing risk and identifying risk owners while ensuring that staff adopt and utilise the Directorate's Enterprise Risk Management Framework;
- ensuring that risk registers for which they are responsible are maintained, reviewed and updated where appropriate and that relevant changes that may affect the Strategic Risk Register are communicated to the Director, Enterprise Risk management, Governance and Risk Branch; and

- assisting with the identification (when required) of broadly-based risks that could impact on the Directorate as a whole.

Staff are responsible for:

- managing risk within their span of control;
- considering the Directorate's Enterprise Risk Management Framework prior to conducting risk assessments;
- using the Directorate's Enterprise Risk Management Guide when undertaking risk assessments (including the risk register and treatment plan template and other tools provided on the risk management intranet page) to assist in managing risk;
- recognising, communicating and responding to emerging or changing risks;
- communicating and informing colleagues, managers and supervisors of changes to current risks, or new and emerging risks; and
- contributing to the process of developing risk assessments for their section or business group.

Reporting and Communication mechanisms

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 teach of the governance forum meetings.

Risk reporting and associated Risk Registers

The requirements and areas for maintaining the reporting of risks and associated risk registers are:

Report	Audience	Responsibility	Report/Review Frequencies
Strategic Risk Register	**Directorate Leadership Committee**	Director Enterprise Risk Management, Governance and Risk Branch	Quarterly – or as risks are advised

Report	Audience	Responsibility	Report/Review Frequencies
Group Risk Register	DG & DDG's/Equivalents	The relevant areas for direct responsibility for development and maintenance of the registers; with ongoing support from the Governance and Risk Branch (i.e. the Director of Enterprise Risk Management).	Quarterly – or as risks are advised
Divisional Risk Register	Executive Group Manager – Divisional Head	The relevant areas for direct responsibility for development and maintenance of the registers; with ongoing support from the Governance and Risk Branch (i.e. the Director of Enterprise Risk Management).	Quarterly – or as risks are advised
Team/Project	Team/Project Leader	The relevant areas for direct responsibility for development and maintenance of the registers; with ongoing support from the Governance and Risk Branch (i.e. the Director of Enterprise Risk Management).	Aligned to Project reporting timeframes (e.g. Prince 2 – at Project Gates)
Audit and Risk Committee	Audit and Risk Committee	Director Enterprise Risk Management, Governance and Risk Branch	Quarterly
Emerging Risks	Relevant Executive Members	Risk Owner/assessment officer	As they occur
Critical/Extreme Risks	Minister through DG/DDG's/ Executive Contact	Nominated Executive in Discussion with Director Enterprise Risk Management, Governance and Risk Branch	As and when Risks are confirmed by the Executive

Resources and Training

Resources

The DIRECTORATE Enterprise Risk Management Framework consists of:

- An acknowledgement of primary documents such as:
    - *the Public Sector Management ACT 1994;*
    - *the Financial Management Act 1996;*

- o *the Insurance Authority Act 2005; and*
- o *the Work Health and Safety Act 2011*
- A policy statement that articulates the DIRECTORATE's approach to risk; its tolerance and appetite for risk;
- The ERM Plan defines -
  - o *the roles, accountabilities and responsibilities of our people;*
  - o *the resources available in support of enterprise risk management in the Directorate; and*
  - o *the various reporting and communication mechanisms for staff undertaking risk management in the organisation.*
- The ERM Guide- a step by step process using the ACT Government Risk Management Policy and Guide incorporating the ACTIA Risk Matrix, addressing how, why and when risks are managed and escalated;
- Tools (an addendum of the Guide) - these include links to the ACT Government Policy and Guidelines through ACTIA, AS ISO 31000:2018 Risk Management Guidelines, as well as in house risk treatment plan templates (i.e. a generic risk register for use in the Directorate);
- Links to 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 support, including external resources for staff when undertaking risk management activities for the organisation; and
- Our ACTHD Risk Management intranet page, which can be accessed from the Governance menu on the HealthHub home page. The page also has linkages to an online training module and training opportunities provided by ACTIA.

Training

- Work is continuing on the development of a comprehensive training package for staff, a significant amount of support material will be our ACTHD Risk Management intranet page, which can be accessed from the Governance menu on the HealthHub home page;
- 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; and
- Individual Training and/or guidance is available now for all level staff in the organisation on request – contact the Director of Enterprise Risk Management on EXT. 49702 for details.