South Gippsland Shire Council

Risk Management Framework

Contents

1 Purpose 3
2 Introduction 3
3 Risk Management Philosophy 3
3.1 Risk Management Objectives 3
3.2 Risk Management Principles 4
3.3 Risk Management Foundations 5
3.3.1 Risk Attitude, Appetite and Tolerance 5
3.3.2 Risk Strategy 6
3.3.3 Policies and programs 7
3.4 Training 7
3.5 Leadership and Commitment 7
4 Risk Reporting 8
5 Roles and Responsibilities 8
6 Risk Management Approach: The Three Lines Model 12
7 Appendix 1 Definitions 14
8 Supplementary supporting documents: 15

Version Control

File Name:	South Gippsland Shire Council Risk Management Framework
Version Number:	1.0
File Path:	TBD
Owner:	Manager - Governance
Endorsed by:	Executive Leadership Team, Audit & Risk Committee
Approved by:	Council
Date Created:	February 2021
Last Updated:	16/02/2021 14:28

1 Purpose

The purpose of this document is to provide a detailed Risk Management Framework setting out South Gippsland Shire Council's (Council) processes, procedures and tools for understanding, documenting, managing and continuously improving Risk Management throughout its operations. The Risk Management Framework supports Council's Risk Management Policy.

The Risk Management Framework has been developed to ensure a consistent approach to risk across the Council and provides a structure for compliance with *AS/NZS ISO 31000: 2018 - Risk management - principles and guidelines'* ('ISO 31000').

Although there are no specific legislative requirements requiring local government agencies to implement a risk management framework, under the Local Government Performance Reporting Framework, our organisation is responsible for identifying our strategic risks.

2 Introduction

Council faces internal and external factors and influences that make it uncertain whether and when it will achieve or exceed its objectives under the current Council plan (2020-2024). The Risk Management Framework aims to ensure that Risk Management is embedded within all of Council's processes.

'Risk' is the effect this uncertainty has on an organisation's objectives. All activities of Council involve risk. We manage risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy our risk appetite.

While all Councils manage risk to some degree, to be effective at managing risk, Council must develop, implement and continuously improve its Framework, with the intention of integrating risk management into our overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Following guidance from The International Risk Management Standard AS/NZS ISO 31000:2018, the relationship between the principles for managing risk, the framework in which it occurs and the process by which risk management is done is described in more detail in the following sections of this document.

3 Risk Management Philosophy

3.1 Risk Management Objectives

Council understands and recognises that rigorous risk and opportunity management is essential for council stability and for sustaining our long-term performance.

The following objectives drive Council's approach to risk management:

- Increase the likelihood of achieving objectives
- Support more effective decision making
- Achieve a truly integrated risk management approach
- Improve stakeholder confidence and trust

- Encourage a high standard of accountability at all levels
- Safeguard Council's assets – human, property, reputation and knowledge
- Improve organisational resilience and minimise losses
- Enable Council's staff, Executive Leadership Team, Audit & Risk Committee and Council to fulfil its governance and compliance requirements.

Council has implemented a risk management framework to improve its ability to meet the above objectives and which incorporates the ISO 31000's 8 key principles of effective risk management,

3.2 Risk Management Principles

The risk management framework seeks to ensure that there is no distinction between usual business practices and risk management practices, and emphasises the integrated nature of risk management within the Council.

Council's philosophy for effective risk management is underpinned by ISO 31000's 8 key principles:

Principle	Description
Integrated	Risk management is an integral part of Council's organisational activities.
Structured and Comprehensive	We will take a structured and comprehensive approach to risk management that contributes to consistent and comparable results
Customised	Our risk management framework and processes are customised and proportionate to our resources, risks and objectives
Inclusive	Stakeholders will be involved appropriately and in a timely manner to enable their knowledge, views and perceptions to be considered. This will improve awareness and inform risk management.
Dynamic	Risks can emerge, change or disappear as our circumstances change. Our risk management will anticipate, detect, acknowledge and respond to those changes and events in an appropriate and timely manner.
Best Available Information	The inputs to our risk management will be based on historical and current information, as well as future expectations
Human and Cultural Factors	Human behaviour and culture significantly influence all aspects of risk management.
Continual Improvement	Risk management is continually improved through our learning and experiences

Underpinning the 8 key principles are the 6 distinct components that form an effective integrated risk management framework. These 6 components are:

- Leadership and commitment
- Integration
- Design
- Implementation
- Evaluation
- Improvement

3.3 Risk Management Foundations

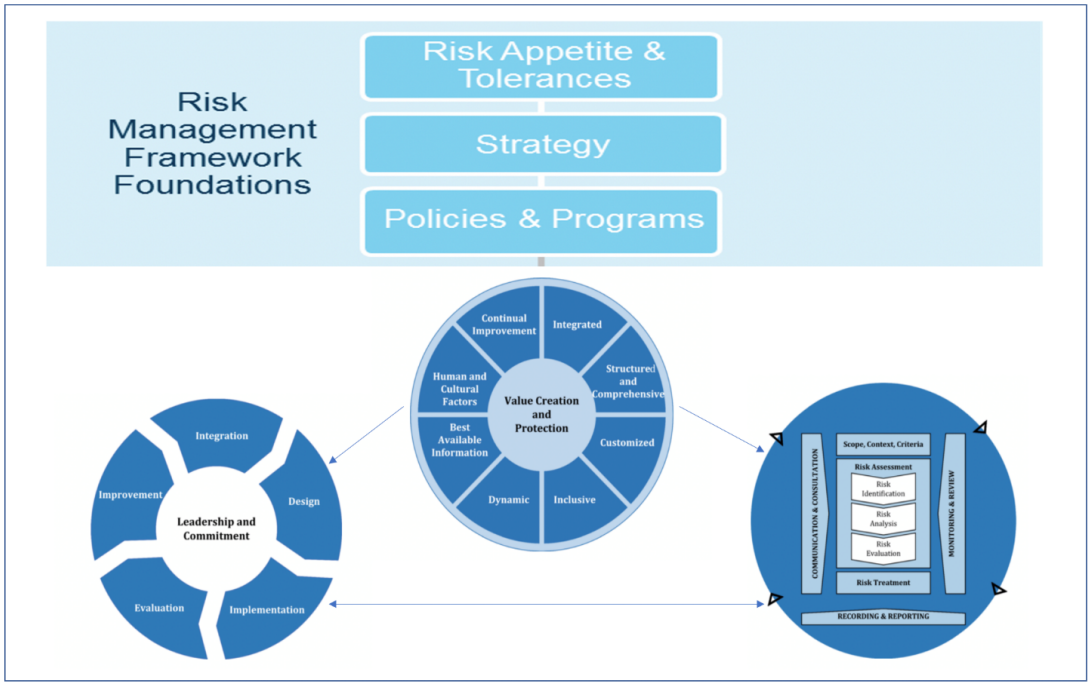


Figure 1: Council's Risk Management Framework

The foundations of the Risk Management Framework has 3 core elements:

3.3.1 Risk Attitude, Appetite and Tolerance

Risk Appetite is the level of risk that Council is prepared to accept in delivering its key strategic objectives. The key strategic objectives for Council are outlined in the 2020-2024 Council Plan. Council faces multiple internal and external factors and influences that make it uncertain whether, when and to what extent it will achieve or exceed its objectives.

Council recognises that all activities involve risk because outcomes of operations are not always certain. As a consequence, Council's risk attitude is broken down into two categories:

1. Risks that Council will **not** accept
2. Risks that Council will actively manage, tolerate and accept.

General Statement of Risk Appetite ***(TO BE CONFIRMED BY COUNCIL)***

"Council is willing to take on a certain level of risk to pursue opportunities that benefit the community but not at the expense of its responsibilities to ethical leadership, regulatory compliance, health and safety, financial sustainability or environmental responsibility.

We recognise that our appetite for risk varies according to the activity undertaken, that acceptance of risk is subject always to ensuring that potential benefits and risks are fully understood before developments are authorised, and that sensible measures to mitigate risk are established.

Council faces a broad range or risks in relation to its operations. These risks include specific risks resulting from our purpose 'To serve in the best interests of the whole Shire, delivering quality services and advocating for community needs' along with the associated strategies and objectives to support this purpose. Risks associated with our operations are managed through detailed processes and procedures that emphasise the importance of integrity, quality and accountability.

Council is committed to making resources available to facilitate effective risk management and to control risks to acceptable levels."

Risk Tolerance

Each risk identified by Council will be individually assessed by the risk owner to determine whether the risk is within Council's tolerance and will be actioned accordingly. Risk tolerance assessments will be included in the Risk Register.

3.3.2 Risk Strategy

The risk management strategy begins with aligning to the Council's overall business strategy and objectives, as outlined in the 2020-2024 Council Plan.

As part of Council's risk strategy, we categorise risk into Strategic Risks and Operational Risks as follows:

1. **Strategic Risks** are those risks which are generally entity wide, may impact on the ability of Council to achieve its objectives set out in the Council Plan and / or the delivery of critical services. Council can manage these strategic risks by:

    a) **Defining business strategy and objectives.** Council plan should integrate risk at the planning stage.
    b) **Establishing key performance indicators (KPIs) to measure results.** KPIs measure historical performance. Council should define KPIs that are aligned to the business strategy and objectives
    c) **Identifying risks that can drive variability in performance.** These are the unknowns, such as COVID and future customer demand, that can impact results.
    d) **Establishing key risk indicators (KRIs) and tolerance levels for critical risks.** KRIs are early warnings for risk exposure levels that may exceed tolerance levels and are intended to anticipate potential roadblocks. Tolerance levels serve as triggers for action. KRIs can be forward-looking leading indicators (such as monitoring CPI forecasts) or backward-looking lagging indicators (such as monitoring Lost Time Injuries)
    e) **Providing integrated reporting and monitoring.** Council must monitor results and KRIs continuously in order to mitigate risks and manage unexpected opportunities as they arise.

    Examples of strategic risk are reputational risk and Council wide compliance risk.

2. **Operational Risks** are those risks which may impact on the achievement of directorate, business unit or service unit to support the strategic Council plan objectives.

    Operational risks are primarily the responsibility of each Department, and the monitoring and reporting responsibilities reside with the Management, the Executive Leadership and

the Audit & Risk Committee. The approach to manage operational risks are further defined in **Section 6 Risk management approach – Three Lines Model.**

Examples of Operational risks are financial and procurement risk.

3.3.3 Policies and programs

Council have embedded risk policies and audit risk programs that provide governance to manage Council's risk. Refer to:

- Risk Management Policy (C35)
- Risk Management Framework (this document)
- Risk Management Processes (refer attachments), including:
  - Risk identification
  - Risk assessment
  - Risk evaluation
  - Risk treatment
  - Risk monitoring and reviewing
- Audit & Risk Committee Charter
- Internal Audit program

3.4 Training

Training in Risk Management will be provided to all staff involved in risk management. Training will be tailored to the recipient's level of involvement and responsibility.

Questions on the Risk Management Policy, Risk Management Framework or Risk Management in general, should be directed to the Risk team or Governance Manager.

3.5 Leadership and Commitment

In achieving an overall effective risk management, Council recognises the importance of leadership. As such, Council, the Council's Executive Leadership Team and the Audit & Risk Committee have responsibility for driving and supporting risk management across the Council. Council has appointed a Manager - Governance who is responsible for maintaining and continuously improving the Risk Management Framework. While risks are owned and managed by staff at all levels of the organisation, the existence of a risk champion in each business unit will help ensure a consistent approach.

Enterprise-wide risk management seeks to apply risk management principles across an entire organisation, and it does this so that all material exposures can be identified, analysed, evaluated and treated. In recognition of this, Council, the Council's Executive Leadership Team and the Audit & Risk Committee have formally endorsed an approach to risk management which includes consideration of financial, safety, reputation and environmental consequences.

Council acknowledges that some events may be largely unpredictable and exceed the capacity of even the most robust management methods and structure. Council's Risk Management Framework includes a Business Continuity Management Plan which seeks to increase the Council's resilience to exceptional events and in turn contribute to more stable corporate performance.

It is the policy of Council to periodically review the effectiveness of the Risk Management Framework through self-assessment and independent assurance. Findings from reviews are communicated in formal reports to the Council's Executive Leadership Team, Audit & Risk Committee and Council, and appropriate action is taken to support the existence of a strong and robust risk and control environment.

The combined strength of Council's culture of integrity, risk management and assurance activities (our three lines model) provide Council with an effective risk management framework.

4 Risk Reporting

Council

An annual briefing is provided to Council on the key strategic risks impacting Council. The briefing provides Council with an overview of how Council monitors its key Strategic and Operational Risks, inform Council of the status of the Strategic Risk Register and discuss newly identified risks.

In addition, the Council receives quarterly minutes from the Audit & Risk Committee along with a biannual report from the Audit & Risk Committee that describes the activities of the Audit & Risk Committee including findings and recommendations.

Executive Leadership Team

At a minimum, risk reporting is provided by the Manager Governance to the Audit & Risk Committee for each meeting (quarterly) and will include:

- Strategic and Operational Risk Registers
- Treatment Plans
- Open action items from audits
- Updates on internal audit programs
- Newly identified risks and other changes to risk registers
- Updates to Risk Management Policies, Frameworks and Procedures
- Updates on training

Audit & Risk Committee

At a minimum, risk reporting is provided by the Manager Governance to the Audit & Risk Committee for each meeting (quarterly) and will include details of Council's Risk Profile (i.e. Heat Maps, Top 10 Risks based on current risk ratings including highlights of changes to the Top 10), treatment plans for significant strategic risks

5 Roles and Responsibilities

At Council, we aim to build a strong risk management and control culture; one where risks are understood. We promote risk awareness, ownership and proactive management of key risks while promoting prudent risk taking.

Adherence to the Council's Risk Management Policy, Risk Management Framework and general Risk Management practices is the responsibility of **all Council's employees**, either through specific responsibilities documented within the Risk Management Policy or through general adoption of Risk

Management strategies by every employee. **All employees** are expected to support the development of a positive risk culture within Council.

The table below sets out key responsibilities for the management of risk across all levels of Council:

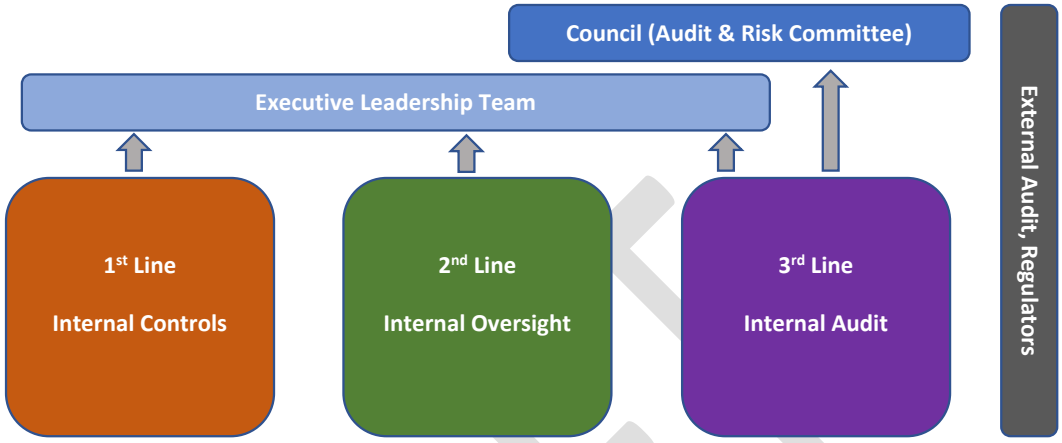
Role	Responsibilities
Council	• Set strategic direction and policy in relation to Risk Management, including determining risk appetite; • Foster and promote a strong Risk Management Culture; • Approve and periodically review the Risk Management Framework and Risk Management Policy; • Consider risk as an important element of Council's strategic planning and decision making processes; • Provide sufficient oversight to ensure risk management is managed efficiently and effectively; and • Receive reports from the Audit & Risk Committee to ensure that strategic risks are being adequately managed.
Audit and Risk Committee (A&RC)	• The Audit & Risk Committee has oversight responsibilities for risk management with no executive authority. The Committee undertakes its role in accordance with the Audit & Risk Committee Charter and acts in this capacity by monitoring, reviewing, endorsing and advising on: ◦ Council's Risk Management Framework and Risk Management Policy; ◦ Council's risk management processes and procedures ◦ Council's risk profile and the changes occurring in the profile; ◦ Council's treatment plans for significant risks ◦ Council's Strategic Risk Register(s) ◦ Internal auditor's annual plan in relation to risk
Chief Executive Officer	• Is responsible for the management of risk across Council; • Foster and promote a strong Risk Management culture; • Ensure overall accountability, authority and resources for managing risks, including incorporation of Risk Management KPIs into performance measures for Directors, Managers and staff; • Ensure the establishment, implementation and maintenance of the Risk Management Framework; and • Ensure appropriate reporting of risk to the Executive Leadership Team, Audit & Risk Committee and Council.
Executive Leadership Team	• Oversee the implementation, operation and annual review of the Risk Management Framework and Risk Management Policy in accordance with AS/NZ ISO 31000: 2018; • Review Strategic (quarterly) and Operational (annual) risk registers ("Risk Registers"); • Facilitate the identification and monitoring of key Strategic Risks and confirming the appropriateness of risk treatments and controls; • Ensure that appropriate staff are identified and appointed who are accountable for updating the Executive Leadership

Role	Responsibilities
	Team on key strategic and operational risks; • Ensure that Risk Owners and managers establish a risk aware culture which reflects the intent of Council's Risk Management Framework and Risk Management Policy • Ensure that Councillors and staff are adequately trained in risk management; • Monitor Council's compliance with recommendations made by Councils internal and external auditors; • Ensure that Risk Management is incorporated into the development and implementation of Council's corporate and business planning process; and • Provide periodic status reports to the Audit & Risk Committee and Council.
OHS Committee	• Identify, monitors and reports on OHS risks; and • Provide OHS minutes and reports to the Executive Leadership Team on a quarterly basis
Directors	• Monitor and report on the status of all Strategic and Operational Risks within their directorate; • Implement Risk Management practices within their directorate to ensure that risks are appropriately identified, managed and reviewed; • Ensure that appropriate Risk Owners are appointed and oversee handover arrangements as / when Risk Owners leave and / or transfer to other parts of theorganisation; • Facilitate the embedding of a risk aware culture within their directorates; • Initiate the incorporation of Risk Management KPIs into the performance measures for managers and staff; and • Implement and review progress of treatment plansfor improved mitigation within their area of operation.
Managers	• Ensure that Strategic and Operational Risks are identified, managed, reviewed and updated regularly within their areas of responsibility; • Facilitate the embedding of a risk aware culture within their teams; • Assist Directors to appoint appropriate Risk Owners and manage handover arrangements when risk owners leave and / or transfer to other parts of the organisation; and • Implement and review progress of treatment plans for improved mitigation within their area of operation.
Risk Team	• Oversee the development, facilitation and implementation of the Risk Management Framework and Risk Management Policy. • Support the activities of Council and the Audit & Risk Committee with regard to risk; • Ensure that the Strategic and Operational Risk Registers are properly maintained across Council;

Role	Responsibilities
	• Provide reports on key Strategic and Operational Risks to assist with managing risks; and • Provides advice and assistance to the Executive Leadership Team, managers and staff in relation to the Risk Management Framework to ensure consistent adoption and approach.
All staff	• Ensure that Risk Management practices are applied in their day-to-day activities; • Maintain an awareness of current and potential risks that relate to their area of responsibility; • Ensure that Risk Management reporting is appropriately undertaken and advise managers of any issues they believe require attention; and • Ensure compliance with Council's Risk Management Policy.
Contractors	• Ensure that contractual and legal obligations are met in accordance with Council's Risk Management Framework, Risk Management Policy, OHS Policy and Safety Management System; • Ensure that required Risk Management documentation is completed and provided to Council's nominated contract / project manager; • Ensure that identified risks are adequately assessed and reported to Council's nominated contract / project manager; and • Ensure compliance with all lawful directions issued by Council's nominated contract / project manager.
Internal Audit	• Ensures the internal audit plan takes into consideration identified high and extreme rated Strategic and Operational risks and associated response activities, including internal controls; • Evaluates the effectiveness and application of the Risk Management Framework; and • Reports to the Audit & Risk Committee.

6 Risk Management Approach: The Three Lines Model

Council has adopted a Three Lines Model for the management of risk. Under the oversight and direction of Council, the Executive Leadership Team and the Audit & Risk Committee, three separate lines are necessary for effective management of risk.



The responsibilities of each line are outlined below:

Council, Audit & Risk Committee, Executive Leadership Team

Council and the Executive Leadership Team are the primary stakeholder served by the Three Lines Model and are the best parties to ensure that the three lines are reflected in Council's risk management and control processes. The Executive Leadership Team and Council have responsibility and accountability for setting Council's objectives, strategies and governance structures to best manage the risks in accomplishing these objectives. The Audit & Risk Committee provides a supporting role to Council in discharging its oversight responsibilities in relation to Risk Management.

1st Line – Internal Controls

The responsibility of each Department, with process owners whose activities create and/or manage the risks that can facilitate or prevent objectives from being achieved. Operational management are responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis.

There should be adequate management and supervisor controls in place to ensure compliance and to highlight control breakdowns, inadequate processes and unexpected events. Departments are responsible for implementing corrective actions to address process and control deficiencies.

2nd Line – Internal Oversight

The second tier supports management by bringing expertise, process excellence, and management monitoring alongside the first line to help ensure that risk is effectively managed. The second line is

essentially a management and/or oversight function that sets direction and defines policy, identifies known and emerging issues, identifies shifts in risk appetites, guidance/training and internal reporting. This includes risk management and compliance functions such as:

- Governance
- Financial Control
- Occupational Health and Safety
- Quality
- Environmental Health

3rd Line – Internal Audit

Internal audit is the third line offering independent challenge to the levels of assurance provided by Internal Control and Internal Oversight functions. Internal auditors provide the Executive Leadership Team, Audit & Risk Committee and Council with comprehensive assurance based on the highest level of independence and objectivity within the organisation. Internal audit can provide assurance on the effectiveness of governance, risk management and internal controls. Internal audit receive access to Council's risk registers to inform their Internal Audit Plan and Internal Audit Scopes. Specific risks addressed are included within Internal Audit Scopes.

External Auditors and Regulators

External auditors and regulators reside outside of Council's structure but play an important role in Council's overall governance and control structure and can provide additional assurance to the Executive Leadership Team, Audit & Risk Committee and Council. Given the specific scope and objectives of their roles, however, can result in information gathered being generally less extensive than Council's internal lines.

7 Appendix 1 Definitions

Risk definitions in accordance with ISO 3100:2018

Term	Definition
Consequence	The outcome of the risk on the Organisation objectives.
Control	Any measure (i.e. process, policy, procedure) put in place by the Organisation to modify/reduce risk.
Current Risk	The level of risk as it presently stands, considering current status of completion of risk treatments.
Inherent Risk	The level of risk determined at the initial assessment, before taking into account the Organisation controls/activities to manage the risk.
Likelihood	The chance that the Organisation will be exposed to each risk.
Objectives	The overarching outcomes that the Organisation is seeking to achieve.
Residual Risk	The level of risk that remains after full implementation of the agreed and documented controls and Risk Treatment Plans.
Risk	The effect of uncertainty on achieving objectives. The effect may be positive or negative. The level of risk takes into account the likelihood of an event occurring and the associated consequence if that risk does occur.
Risk Appetite	The amount and type of risk that the Organisation is prepared to accept in pursuing its objectives.
Risk Management Attitude	The Organisation's approach to assess and pursue, retain, take or turn away from risk.
Risk Management	The combination of systems, processes and culture used to direct the Company in identifying, assessing, evaluating and treating risks. Risk Management allows the Organisation to find an appropriate balance of realising opportunities and minimising losses in the pursuit of its objectives.
Risk Management Framework	(This document). A detailed framework setting out the Organisation processes, procedures and tools for understanding, documenting, managing and continually improving Risk Management throughout its operations.
Risk Management Policy	The statement of overall intentions and directions of the Organisation in relation to Risk Management.
Risk Owner	The person assigned with accountability and authority to manage a specific risk.
Risk Register	A comprehensive list of risks for the Organisation, including a description of the risk and the associated rating(s) of the risk.
Risk Treatment Plan	A process to modify/manage the risk beyond current risk levels and can involve: • Avoiding the risk (deciding not to start or continue with the activity) • Reducing the likelihood of the risk • Transferring the risk (i.e. insurance) • Sharing the risk (i.e. distribute the risk amongst other participants) • Reduce the consequence of the risk • Reduce the likelihood and consequence of the risk

8 Supplementary supporting documents:

- Risk Management Policy (C35)
- Risk Management Procedures
- Strategic and Operational Risk Registers