

Portfolio:	Finance and Support System	Ref. No.	POL-6105
Department:	All Departments		
Title:	Risk Management Framework		

1. SCOPE AND PURPOSE

1.1. Purpose

Royal Australasian College of Surgeons (RACS) maintains a Risk Management Framework (RMF) which describes the systems, structures, policies, processes and people in place that identify, assess, manage, mitigate and monitor internal and external sources of risk that could have a material impact on RACS's business operations or the interests of its relevant stakeholders

This Framework is founded on principles which are currently industry's best practice; in particular, it draws influence from the Australian and New Zealand ISO Standard on Risk Management (AS/NZ ISO 31000:2018).

The RMF recognises that proactive management of risk ensures RACS will make informed decisions and make necessary adjustments throughout the business cycle to meet its business planning and strategic direction. It also acts to ensure that the stakeholders' best interests are at the centre of all decision making and protects RACS from adverse financial, strategic and operational outcomes to the best extent possible.

1.2. Scope

The RMF covers RACS which includes all the internal facing business groups and the surgical societies.

1.3. Application

This RMF is applicable to all Councillors, Executive General Managers and staff members of the Royal Australasian College of Surgeons.

1.4. Values and behaviour

This RMF is designed in alignment with RACS's attitude towards risk taking, risk management and the level of risk awareness in decision making while considering RACS's culture.

The underlying foundation of the RMF's implementation is that:

- All employees are expected to act ethically and in accordance with the law and RACS's corporate policies;
- The Executive General Managers will demonstrate ownership and accountability in regard to managing risks which sit within their respective business units; and
- Council will set the 'tone from the top' in regard to acceptable practices and behaviour.

2. RISK MANAGEMENT

Risk Management is defined as the coordinated activities to direct and control RACS' exposure to risk.

Risk is "the effect of uncertainty on objectives"¹. There are three key concepts to consider in determining the severity of a risk and the potential risk management required:

- The potential event and the context within which it occurs
- Probability of that event occurring (likelihood)
- The plausible worst-case impact of the outcome, should the event occur (impact)

The action taken to manage this uncertainty and identify opportunities is risk management. RACS's approach to business planning is to incorporate risk management in each strategic priority and ensure alignment of its strategic plan to Council's risk appetite.

¹ ISO 31000:2018

Approved By:	CEO	Original Issue:	November 2015
Document Owner:	EGM Finance and Support Systems	Version:	3
		Approval Date:	June 2023
Page 1 of 10		Review Date:	August 2026

Portfolio:	Finance and Support System	Ref. No.	POL-6105
Department:	All Departments		
Title:	Risk Management Framework		

3. RISK MANAGEMENT PROCESS

RACS' system to manage risks is a continuous and dynamic process, through which risks are identified, assessed, responded to and reported.

A summary of the Risk Management process and the key steps are set out below:



3.1 Risk Identification

The Risk Identification process involves generating a list of material risks that may impact RACS' ability to achieve its goals and objectives, and therefore require management's attention and monitoring.

In Risk Identification, the first step is to consider risks (internal and external) within the environment in which RACS operates. This results in a list of risks for RACS which can then be assessed (see section 3.2 Risk Assessment below).

Additionally, to aid management in the process of aggregating and analysing risks, each identified risk is assigned a category to allow for the grouping and evaluation of risks that are alike in nature. Risk management must be placed into a strategic, operational, emerging, financial and project-based context.

Strategic risks are the most consequential risks that may hinder RACS' ability to execute its strategies and achieve its business objectives. These include risk factors such as:

- Key thrusts or changes within RACS's principal stakeholder strategies involving the fellow members across 13 surgical societies
- Maintaining high standards of professionalism in surgical training
- Maintaining relevant accreditations across Australia and New Zealand
- Opportunities and threats associated with the internal, national/state, and global economic, social, political, cultural, environmental, regulatory, and competitive

Approved By:	CEO	Original Issue:	November 2015
Document Owner:	EGM Finance and Support Systems	Version:	3
		Approval Date:	June 2023
		Review Date:	August 2026

Portfolio:	Finance and Support System	Ref. No.	POL-6105
Department:	All Departments		
Title:	Risk Management Framework		

- environments
- **Operational** risks are the risks of losses to RACS which result from inadequate or failed internal processes, people and systems, or external events. These risks give consideration to RACS':
- Rapport and capacity to influence the fellow members of RACS across the 13 surgical societies.
- Organisational structure and culture;
- Control over business processes and execution;
- System failure including loss of data integrity or breach of data
- Business resilience and business continuity processes and
- Day to day issues associated with people, financial information and legal.

Project risks are any uncertain events that, if occurred, could have a detrimental effect on the achievement of project objectives or business outcomes. Project risks are categorised as either execution or delivered risks.

Projects are considered to be any temporary large-scale operation that will result in a permanent change in day-to-day activities.

This may include initiatives such as, but not limited to:

- New system implementations and upgrade of current systems;
- Digital Transformation projects;
- Process redesign;
- Organisational restructuring projects;
- Information Security projects to enhance cyber and data security

3.2 Risk Assessment and Analysis

The Risk Assessment process involves the estimation of the impact and likelihood of the risk on both an inherent and residual basis. The combination of impact and likelihood is used to derive the risk rating. The assessment is completed by the risk owner/s, reviewed by the Executive General Managers and the risk ratings are recommended for approval by the Finance Audit and Risk Management Committee (FARM) and endorsed by Council. Inherent risk assumes the failure of key controls associated with the risk and enables a decision to be made on how to manage the risk (see section 3.3 Risk Response and Strategy below). The residual risk assessment takes into consideration the effectiveness of controls.

The risk assessment facilitates management oversight and provides a framework to assist management in decision making in relation to risk management strategy and courses of action.

RACS has developed a matrix for determining the overall level of a risk and how it should be reported and managed. The matrix can be applied to both the inherent risk level and residual risk level although management actions are based on net (residual risk).

3.3 Risk Response and Strategy

The risk treatment process involves the identification of a range of options for accepting, mitigating, transferring or avoiding the risk, assessing these options and developing controls and/or risk treatment plans for the identified risk events.

Often more than one response may be necessary to address an identified risk. In those cases, treatment will involve a combination of the above controls to reduce or mitigate specific risks.

The assessment of risk is undertaken in the Risk Register which contains all relevant risk related information that includes the underlying causes of risk and its impacts, existing and desired controls that could reduce or eliminate the risk, and risk & control owners. The rating of the risk in accordance with the Risk Level Matrix will guide the response and strategy on how the risk is addressed, managed, and reported.

Approved By:	CEO	Original Issue:	November 2015
Document Owner:	EGM Finance and Support Systems	Version:	3
		Approval Date:	June 2023
Page 3 of 10		Review Date:	August 2026

Portfolio:	Finance and Support System	Ref. No.	POL-6105
Department:	All Departments		
Title:	Risk Management Framework		

3.4 Risk Monitoring and Reporting

The risk management process is iterative and should be the subject of a structured monitoring and review process.

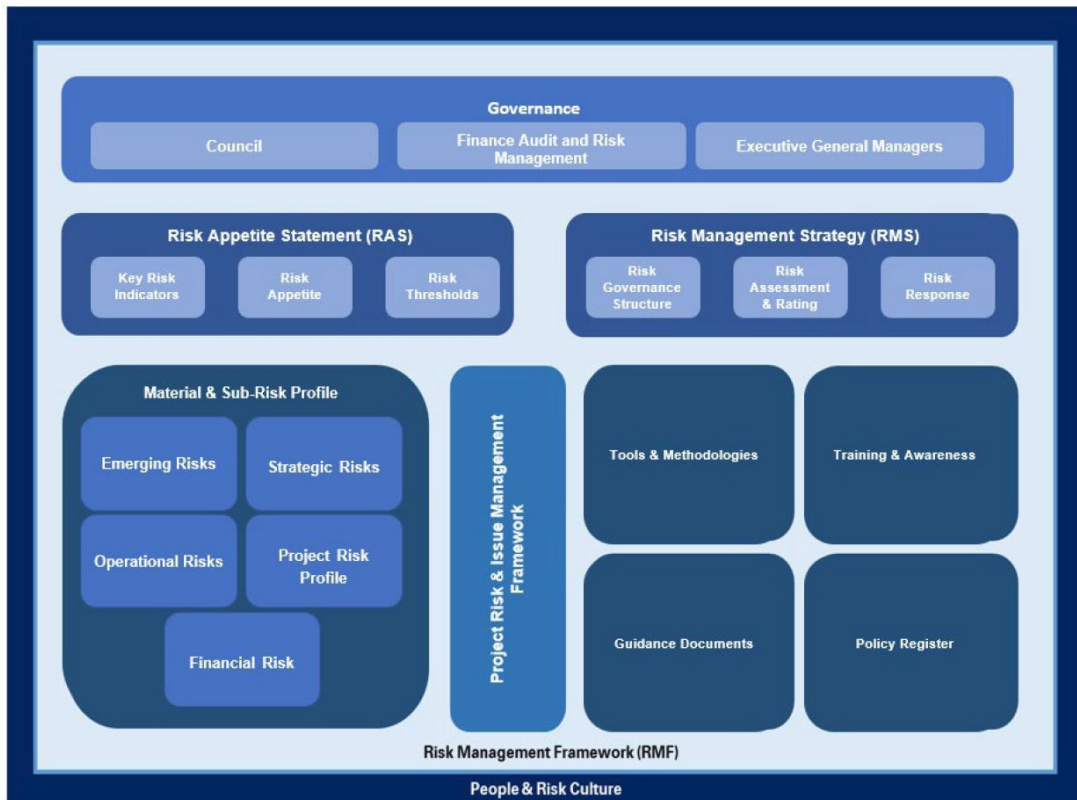
The EGM Finance and Support Services, with monthly input from risk owner/s, provides quarterly risk reporting to the Executive Leadership Group (comprising of the Executive General Managers) and Council. Risk reporting to the Finance Audit & Risk Management Committee (FARM) is done at the three FARM meetings held during the year. The key risk matters include but are not limited to:

- RACS’s material risks,
- risk measures from the Risk Appetite Statement,
- status of key controls and treatment actions,
- incidents and other material events.

4. RISK MANAGEMENT FRAMEWORK

The Risk Management Framework consists of a number of parts illustrated below. These mechanisms operate together to support awareness, action and management of the risk environment, and provide reasonable assurance that material risks are being prudently and soundly managed, having regard to the size, business mix and complexity of that risk.

These components are described below:



4.1 Risk Management Strategy

The Risk Management Strategy (RMS) outlines how management addresses each material risk for RACS with reference to the relevant policies, standards and procedures.

Approved By:	CEO	Original Issue:	November 2015
Document Owner:	EGM Finance and Support Systems	Version:	3
		Approval Date:	June 2023
		Review Date:	August 2026

Portfolio:	Finance and Support System	Ref. No.	POL-6105
Department:	All Departments		
Title:	Risk Management Framework		

Furthermore, for each identified risk, management is required to elect the appropriate acceptance response from the below options:

- **Accept:** Acknowledgement of risk existence
- **Avoid:** Business operations are to be tailored in order to bypass risk eventuation
- **Mitigate:** Acknowledgement of risk existence and an appropriate risk response plan to be developed and implemented
- **Transfer:** Risk is to be managed externally to the business (e.g. outsource to a third-party provider)

4.2 Risk Appetite Statement

The Risk Appetite Statement (RAS) serves as the overarching guide on RACS' tolerance to risk in its day-to-day operations and in the pursuit of its strategic and operational objectives.

RACS defines risk appetite as "the level of risk that RACS is willing and prepared to take in the pursuit of its strategic objectives". RACS's risk appetite is defined in the Risk Appetite Statement (RAS).

The RAS enables a balanced approach to risk taking by expressing the appetite to avoid or pursue risks based on perceived business outcomes, as well as guiding principles to inform risk decisions, for each material risk. Where decisions are taken to accept risk, the rationale will be consistent with the RAS.

The RAS will be initially defined at a qualitative level with a view to gradually build quantitative metrics such as Key Risk Indicators (KRIs). This will enable management to ensure that the material risks are measured and monitored and stay within appetite.

4.3 Project Risk and Issue Management Framework

RACS does not currently maintain a Project Risk and Issue Management Framework but the Executive General Leadership team is committed to develop and implement one at an appropriate time. Currently, project risks are managed in line with the processes outlined within the RMF. Risks are evaluated on an individual project basis and managed in accordance with the procedures outlined within the RMF and its associated documents and policies.

4.4 Governance

RACS's Risk Governance lies with the Council, Executive Leadership team and the Finance Audit and Risk Management Committee, strengthened by the 'Three Lines of Defence' risk management structure. Specific roles and responsibilities are outlined in section 5 below.

4.5 Material and Sub-Risk Profile

RACS's material risks are risks at the enterprise level that impact RACS as a whole. They are set by Council and owned by the management.

The Material Risk Profile includes:

- Emerging risks
- Strategic risks
- Operational risks
- Project risks
- Financial risks

4.6 Tools and Methodologies

In implementing the RMF and its associated policies and documents, RACS utilises the following digital resources:

- SharePoint: a repository for RACS's risk management documents, including the Risk Summary, Risk Registers and Corporate Strategy Update documents.

Approved By:	CEO	Original Issue:	November 2015
Document Owner:	EGM Finance and Support Systems	Version:	3
		Approval Date:	June 2023
Page 5 of 10		Review Date:	August 2026

Portfolio:	Finance and Support System	Ref. No.	POL-6105
Department:	All Departments		
Title:	Risk Management Framework		

- Thrive: training system for RACS' online training modules
- Risk Registers: The RMF and RAS are supported by a Risk Register Report which is maintained and updated manually. The Risk Register captures RACS's strategic and operational risks, controls, action plans, and risk and control owners.
- Controls Assurance Methodology: Risk and Controls guidance documents

4.7 Risk Culture

RACS's risk culture should align with the Council's and Executive Leadership Team's attitude toward risk taking, risk management and the level of risk awareness in decision making.

Key elements of RACS's risk culture	
Tone from the top	Strong 'tone from the top' across the Council and the Executive Leadership Team. Managers are required to role model appropriate risk management behaviour and take risks within the risk appetite set by the Council.
Ownership and accountability	Accountability for managing risks sits with those whose roles are most likely to incur the risk. Risk is consciously considered in decision making and taken within well-defined boundaries, is actively managed, and is considered from the whole RACS perspective in achieving business outcomes.
Clear expectations	The Executive General Managers are expected to be aware of the key controls and compliance obligations within their business and the impact on the whole organisation.
Speaking up, listening, and taking action	The Executive General Managers are committed to empowering people to 'speak up', learn from mistakes, listen to feedback and take action.
Challenge and collaboration	Effective management of risk is seen as a business enabler. The model adopted ensures that risks are owned by business units but that the Second Line of Defence (see Section 5 below) is consulted and provides input into key decisions impacting RACS's risk profile.

4.8 Training & Awareness

Training and awareness are a core part of the framework and an ongoing focus area to ensure the RMF is embedded and staff are aware of its importance and are managing risks within day-to-day operations. The following are planned training (desired state). Some examples of training include:

- Risk and compliance education program available to all staff and delivered via workshops, monthly town hall meetings, and online modules;
- Regulatory changes, updates and alerts are shared periodically;
- Employees receive training on risk management, both generic and tailored to their areas. This training can take the form of face-to-face and online training.

The effectiveness of the risk operating structure depends upon the capability and training of people responsible for managing risks.

Approved By:	CEO	Original Issue:	November 2015
Document Owner:	EGM Finance and Support Systems	Version:	3
		Approval Date:	June 2023
		Review Date:	August 2026

Portfolio:	Finance and Support System	Ref. No.	POL-6105
Department:	All Departments		
Title:	Risk Management Framework		

5. ROLES AND RESPONSIBILITIES

Notwithstanding RACS' "whole of organisation" approach to risk management, RACS's Risk Management Framework has specific elements which require a defined alignment of roles and responsibilities. The key responsibilities for each of the identified roles are as follows:

Role of Council

RACS Council has a fundamental role to play in the management of risk. This includes the following:

- Confirmation of the Risk Management Framework
- Ensuring that material risks are identified, managed, and controlled appropriately to achieve RACS's Strategic Objectives
- Recognise uncertainties, limitations, and assumptions attached to the measurement of each material risk
- Accountable to define the risk appetite of RACS
- Approve RACS's Risk Appetite Statement
- Form a view of RACS' risk culture and the extent to which this culture supports RACS's ability to operate within its risk appetite, identify any desirable changes to the risk culture and ensure that RACS takes steps to address those changes
- Ensuring that RACS' operational structure facilitates effective risk management
- Ensuring that policies and processes are developed for risk-taking that are consistent with the RMS and the established risk appetite
- Ensuring that sufficient resources are dedicated to risk management
- Appointing and resourcing the Finance Audit and Risk Management Committee
- Review the adequacy and effectiveness of the Risk Management Framework
- Review risk management policies, procedures and guidelines
- Review and approve the allocation of audit resources (if and when appropriate) in conjunction with the Risk Profile
- Receive periodic reports regarding identified risks/mitigation and their effectiveness from management
- Monitor changes to the Risk Profile and highlight material changes to the Finance Audit and Risk Management Committee.

Role of Executive General Managers (EGMs)

- The Executive General Managers are ultimately responsible for the effective implementation of risk management throughout RACS
- Support and encourage a risk aware culture within RACS
- Ensure the Risk Management Framework is in place and functioning adequately
- Review RACS's Risk Profile half yearly
- Ensure risk management is considered part of the Business Planning Process
- Be satisfied that all risks are appropriately identified, managed and controlled by each responsible risk owner, with management being held accountable for risks identified in their area of responsibility
- Ensure all risks assessed as "Critical" are escalated to the Finance Audit and Risk Management Committee
- Review and approve individual risk response plans

Role of EGM Finance and Support Services

- Develop, maintain and facilitate the implementation of the Risk Management Framework
- Ensure that Council and the Finance and Audit Management Committee is notified of all material

Approved By:	CEO	Original Issue:	November 2015
Document Owner:	EGM Finance and Support Systems	Version:	3
		Approval Date:	June 2023
		Review Date:	August 2026

Portfolio:	Finance and Support System	Ref. No.	POL-6105
Department:	All Departments		
Title:	Risk Management Framework		

risk matters

- Define and maintain roles and responsibilities for risk management
- Identify and assess RACS' risk profile through the facilitation of the annual organisation risk assessment and the half yearly review of the organisation risk assessment
- Ensure effectiveness of risk controls is assessed
- Provide appropriate risk reporting to FARM and Council periodically
- Maintain the accuracy and completeness of the Risk Registers

Role of Managers

- Ensure that the Risk Management Framework is implemented
- Identify and assess risks associated with line accountabilities
- Identify and Implement risk response plans
- Continuously monitor implementation and effectiveness of agreed risk responses
- Ensure staff are adequately trained to identify and assess risk

Role of Employees

- Identify and assess risks associated with personal tasks and activities
- Ensure personal compliance with risk management policies and procedures in the performance of duties/activities
- Ensure that any hazards identified are escalated to their Line Manager

Role of Identified Risk Owners

- Develop and implement appropriate risk response plans
- Actively monitor and manage risk in line with the RMF and its associated policies and procedures
- Provide bi-annually attestation on risk effectiveness

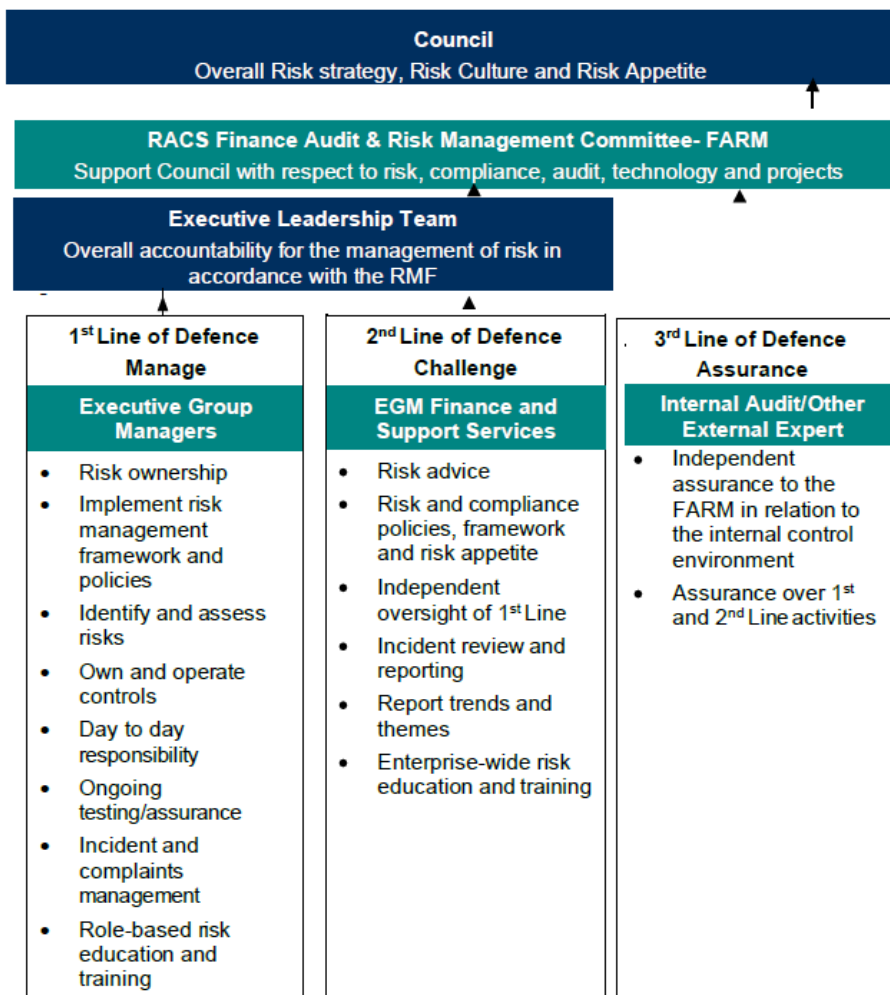
Role of Control Owners

- Ensure the design and operating effectiveness of controls are maintained.
- Provide bi-annual attestations in regards to control effectiveness.

Portfolio:	Finance and Support System	Ref. No.	POL-6105
Department:	All Departments		
Title:	Risk Management Framework		

Three Lines of Defence

RACS’s management seeks to implement a modified ‘Three Lines of Defence’ governance structure to define the roles and responsibilities under the RMF at all levels of the organisation and reinforce accountability



In the absence of a dedicated 2nd Line of defence, a modified ‘Three Lines of Defence’ governance model is used where the EGM Finance and Support Services will perform the role of 2nd Line, whilst still discharging their responsibility as 1st Line for Finance and Support Services. This governance structure provides an escalation channel for key risk management matters and enables risks to be managed in line with Council’s risk appetite. This framework is supported by effective periodic reporting and provides Council and the FARM with assurance over the effectiveness of the RMF.

6. NOTIFICATIONS REQUIREMENTS

RACS is required to notify the Finance Audit & Risk Management Committee when it:

- Becomes aware of a significant breach of, or material deviation from, the RMF; or
- Discovers that the RMF did not adequately address a material risk; or
- Discovers a material control deficiency within its operations, including where operations may have been outsourced by RACS to a third-party.

RACS must notify Council as soon as practicable when it becomes aware of any material changes to the size, business mix and complexity of RACS’s business operations.

Approved By:	CEO	Original Issue:	November 2015
Document Owner:	EGM Finance and Support Systems	Version:	3
		Approval Date:	June 2023
		Review Date:	August 2026

Portfolio:	Finance and Support System	Ref. No.	POL-6105
Department:	All Departments		
Title:	Risk Management Framework		

7. RMF MAINTENANCE

7.1. Record Keeping

Documentation to demonstrate the operation of the RMF will be retained in accordance with the Record Management Policy.

7.2. Availability of this RMF

This RMF is available to Directors and all employees of RACS and can be accessed via the RACS SharePoint.

7.3. Review

The RMF and its key components will be reviewed each year by the management as part of the annual strategic planning session, to ensure it remains relevant and effective in the management of risk. Reviews may occur more frequently if required, due to legislative changes or changes to the business operations of RACS.

A formal review of the RMF is undertaken annually by the Finance Audit and Risk Management Committee, and a comprehensive review is undertaken every three years by an operationally independent and appropriately qualified person.

7.4. Council Approval

The RMF must be approved by Council. Material amendments to this RMF are to be first approved by the Audit and Risk Committee prior to obtaining the formal approval of Council.

Non-material changes are permitted by the EGM Finance and Support Services with notification to the Finance Audit and Risk Management Committee for noting.