

# Risk Management Policy

---

## 1. Purpose

The purpose of this policy is to establish the Royal Australasian College of Medical Administrators (**College**)'s approach to risk<sup>1</sup> and outline a methodology for the systematic identification, assessment and management of risks.

## 2. Scope

This Policy applies to all College Staff, Board Directors and people in Board-established committees.

## 3. Policy Statement

### 3.1 Intent

3.1.1 The College is committed to embed risk management in decision-making, strategic and operational planning and resource allocation.

3.1.2 Effective risk management creates organisational value by supporting:

- a) proactive identification and management of opportunities and threats
- b) informed and timely decision-making and planning, underpinned by clear risk-taking boundaries (risk appetite statement)
- c) appropriate allocation of resources
- d) achievement of optimal outcomes and minimisation of the likelihood of unacceptable outcomes
- e) compliance with relevant legal, regulatory and contractual requirements
- f) robust corporate governance including good risk reporting.

### 3.2 Risk Appetite

3.2.1 The Risk Appetite Statement articulates the amount and type of risk the College is prepared to pursue, retain or take to achieve its objectives<sup>2</sup>.

3.2.2 Acknowledging that the College operates in an environment that is rapidly evolving, the Risk Appetite Statement supports conscious risk-taking needed to drive innovation and achieve the College's strategic ambitions, while also operating in line with our values, maintaining reputation, relevance and ongoing sustainability.

---

<sup>1</sup> A risk in this Policy is defined as an uncertain event that, if it materialises, will affect (positively or negatively) the achievement of objectives (definition from *ISO 31000:2018 – Risk management – Guidelines*).

<sup>2</sup> Definition of risk appetite from *ISO 31000:2018 – Risk management - Guidelines*. This is understood to be risk after application of controls (residual risk).

- 3.2.3 The Board acknowledges that some risks cannot be avoided or fully controlled as they are inherent to initiatives and operations that are essential to the College given its objectives and strategy.

### **3.3 Approach**

- 3.3.1 The College adopts an approach aligned with the *ISO 31000:2018 Risk Management* standard. While the risk management process is outlined as a series of steps presented in a sequence, it is not actually linear and should rather be considered as a cycle with multiple iterations.

#### **Risk assessment**

- 3.3.2 Risk identification is the process of finding, recognising and describing risks that could affect the achievement of objectives. This also includes identification of primary causes (i.e. plausible) and material impacts.
- 3.3.3 Consideration is then given to controls or mitigating circumstances that reduce the likelihood of the event occurring, or its severity if it does. Only controls that are already in place and that are assessed to be effective at mitigating the risk (even if there is room for improvement) will be included. Effectiveness may be determined through formal evaluation or testing (e.g. internal audit), but in most cases will be based on judgement and experience.
- 3.3.4 Each identified risk is assessed in terms of its likelihood (probability of the risk event occurring) and consequences (impact of the risk event happening), to determine the risk rating after application of controls (residual risk), using the risk matrix in Appendix 1. If there are multiple independent causes or multiple consequences, the highest likelihood of the most probable cause and the highest impact of the most probable consequence are used to determine the rating.
- 3.3.5 The risk rating and the risk appetite are jointly considered to determine how to respond to the risk.
- a) Where a risk is within the risk appetite – any action to further mitigate the risk will fall within usual business activities (without prioritisation of resource allocation).
  - b) Where a risk is outside the risk appetite –
    - i. If the risk is unlikely to seriously affect the achievement of strategic or operational objectives – the College will determine if additional treatment is practicable and possible, considering costs and benefits.
    - ii. If the risk is likely to threaten a business function and potentially seriously affect the achievement of objectives – the College will take reasonable action to reduce exposure to within agreed appetite.
    - iii. If the risk threatens and/or stops a strategic or operational objective – the College will take all reasonable steps to reduce exposure to within the agreed appetite. This includes considering modifying or abandoning the activity.
  - c) The Chief Executive may recommend that the Board accepts a risk that is outside of the risk appetite where:
    - i. actions have already been taken but their impact on the risk rating is as yet unclear.
    - ii. they consider that there is no additional commercially and practically sensible way to further mitigate the risk, and the activity cannot be changed or abandoned.
- 3.3.6 Communication and consultation should occur throughout the risk assessment process to leverage expertise and insight, including about precedence (inside and outside the College), as well as incidents or complaints, to better understand the risk.

## Risk treatment

- 3.3.7 Risk treatment is the action taken to address and manage the residual risk. Actions may include:
- a) avoiding the risk, if possible, e.g. by not starting or discontinuing an activity.
  - b) transferring the risk, if a third party is better placed to manage this risk at a cost that is reasonable to the College.
  - c) managing the risk by doing things differently or doing more to mitigate the risk.
- 3.3.8 Each action will be owned by a nominated individual, who will be responsible for its implementation. Actions will be recorded and progress against completion tracked regularly.
- 3.3.9 A risk treatment only becomes a control once it is assessed to be effective in mitigating the risk.

## Review, reporting and escalation

- 3.3.10 Risks (description, assessment, controls, rating and treatment) will be documented in risk registers.
- 3.3.11 Risks should be reviewed at least quarterly so risk registers reflect our latest understanding of risks, assessment of effectiveness of controls, and the impact of implementation of risk treatments on the risk rating. This should also act as a prompt to consider any new/emerging risks.
- 3.3.12 Risk reporting will focus on priority risks, which are:
- a) risks rated high or very high after application of controls
  - b) risks that rely significantly on controls operating as intended
  - c) new risks identified since the last report
  - d) risks rated outside of the risk appetite.
- 3.3.13 Risks will be reported to the relevant Board-established committee on at least a yearly basis or more frequently if deemed necessary (e.g. material change), and to the Finance and Audit Committee and to the Board on a quarterly basis.
- a) The Chair of that entity or the Chief Executive may decide to escalate the risk to the Board where risks are rated very high or are significantly outside of the risk appetite.

## 3.4 Roles and responsibilities

Body/Person	Responsibilities
Board	<ul style="list-style-type: none"> <li>▪ Approve the Risk Management Policy</li> <li>▪ Oversee the enterprise risk register and adequacy of controls</li> <li>▪ Promote a proactive risk culture</li> </ul>
Finance and Audit Committee	<ul style="list-style-type: none"> <li>▪ Review the Risk Management Policy</li> <li>▪ Monitor the enterprise risk register and adequacy of controls, provide advice to the Chief Executive on risk assessments and mitigation strategies</li> <li>▪ Review issues that may impact the College's ability to achieve its strategic objectives</li> <li>▪ Oversee the College's insurance</li> </ul>

Committees	<ul style="list-style-type: none"> <li>Monitor the risks applicable to their scope and adequacy of controls</li> </ul>
Chief Executive	<ul style="list-style-type: none"> <li>Implement the Risk Management Policy</li> <li>Review the enterprise risk register (including mitigation strategies in place) regularly and report to the Finance and Audit Committee</li> <li>Resource risk management activities and risk capability in the organisation appropriately</li> <li>Embed a risk culture in the College, where risk management is valued, supported and ingrained in the way people think and act</li> <li>Promote a culture of transparency that encourages and supports staff to speak up about their concerns</li> </ul>
Senior Leadership Team	<ul style="list-style-type: none"> <li>Oversee risk management in their department and report to the relevant Committee</li> <li>Escalate risks to the Chief Executive as required</li> </ul>
All leaders	<ul style="list-style-type: none"> <li>Promote positive risk practices in area of responsibility to drive a risk-aware culture and integrate risk into decision-making</li> <li>Keep abreast of risk in area of responsibility – identify and assess risks and monitor controls and oversee implementation of mitigating actions.</li> </ul>

#### 4. Related documents

- Risk Appetite Statement
- Finance and Audit Committee Terms of Reference

Document information			
Type:	Policy - Governance	Approval Date:	August 2024
Custodian:	Chief Executive	Approved by:	Board
Version:	v2.0	Endorsed by:	Finance and Audit Committee
Next Review: 3 years from approval date or earlier if required			
Uncontrolled when printed			
Revision history			
Version	Date	Description	
v2.0	August 2024	New sections on risk appetite approach, review of roles and responsibilities, new formatting	
v1.1	September 2018	New Policy	

## Appendix 1 Risk Rating

### Risk rating

	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Severe
Almost certain	Low	Moderate	High	Very high	Very high
Likely	Low	Moderate	High	High	Very high
Possible	Low	Moderate	Moderate	High	High
Unlikely	Low	Low	Moderate	Moderate	High
Rare	Low	Low	Low	Moderate	Moderate

### Likelihood

Consider the likelihood of the event as described in the risk description occurring. You may think of it in terms of probability of occurrence over the next 12 months, or frequency of occurrence over a time period. Where there are many different likelihood, judgement is required to determine which applies.

Likelihood	Probability of event occurring in next 12 months	Alternative characterisation
Almost certain	Greater than 80%	OR Likely to happen once or more in a year
Likely	50% - 80%	OR Likely to happen once every 1-3 years
Possible	20% - 50%	OR Likely to happen once every 3-5 years
Unlikely	5% - 20%	OR Likely to happen once every 5-10 years
Rare	Under 5%	OR Likely to happen once every 10 years

### Consequence

The table below outlines examples of interpretation of the consequences of a risk event happening. Where there are many different consequences, judgement is required to determine which applies.

	Insignificant	Minor	Moderate	Major	Severe
Strategic	Negligible impact on objectives	Limited impact on objectives that can easily be remedied	Some objectives are affected	Some important objectives may not be met	Most or many major objectives may not be met
Compliance and legal	Minor compliance gaps against internal policies	Compliance gaps / incidents with potential to draw regulator attention or litigation	Potential regulatory breach that may result in less than 12 months scrutiny; or moderate level remediation Potential for litigation	Potential regulatory breach that may result in fines; enforceable undertaking; multi-year scrutiny; or material level remediation.	Regulatory breach that may result in significant remediation and/or suspension or loss of accreditation
Reputation	Grievance or complaint manageable as part of normal processes	Short term adverse publicity with some tangible impact	Significant reputation issue requiring considerable management effort to address	Long-term reputation issue taking in excess of 12 months to recover from. Adverse media coverage	Enduring loss of confidence with permanent impact on the College's future Sustained adverse media coverage
Financial	Financial impact <\$100k or under 10% of project <sup>3</sup> value	Financial impact \$100k - \$500k or between 10-30% of project value	Financial impact \$500k - \$1 million or between 30-50% of project value	Financial impact \$1m - \$3millions or between 50-70% of project value	Financial impact >\$3millions or greater than 70% of project value
Operational	Limited impact on services, resolve within 1 week	Short term impact on services, resolve within 4 weeks, minimal management time required	Services affected requiring effort for recovery with an impact of between 1-3 months	Services affected requiring substantial effort for recovery with an impact of between 3–6 months	Services affected requiring significant effort for recovery with an impact greater than 6 months
Health and safety	Near miss	Minor injury that requires first aid or illness with no long term physical or emotional effects.	Injury or illness requiring medical intervention or treatment with no long term physical or emotional effects	Serious injury or illness requiring hospitalisation. Ongoing physical or emotional impairment	Permanent impairment with significant functional restriction Loss of life

---

<sup>3</sup> Only strategic projects with a value exceeding \$250k are in scope