Risk Management Policy

Area of College	Governance
Document Writer	Risk and Compliance Manager
Document Owner	Chief Executive Officer
Approved by	RACP Board
Effective Date	25/06/2026
Next Review Date	30/11/2027
References/Legislation	AS/NZS ISO Standard 31000:2018 *Risk management - Principles and guidelines*
Associated RACP Documents	RACP Risk Management Framework RACP Enterprise Risk Management Framework Risk Appetite Statement
Applicability	Australia and Aotearoa New Zealand

Note: This is a controlled document within the RACP Policy Framework. The Framework covers all RACP policies, procedures, by-laws, terms of reference, guidelines, forms, etc. Any new documents or amendments of existing documents or changes to the approver, owner or area of college should be done in accordance with the RACP Policy Framework and Document Control (RACP Policy Framework) Procedure.

TABLE OF CONTENTS

1. INTRODUCTION 3
2. PURPOSE 3
3. SCOPE 3
4. RISK AWARE BEHAVIOURS 4
5. HOW IS RISK MANAGED AT THE COLLEGE 4
5.1. Risk Reporting and Governance 8
6. ROLES AND RESPONSIBILITIES 8
7. REVIEW OF POLICY 11
8. DEFINITIONS 11
9. HISTORY 12
1. APPENDIX 1: RISK MATRICES 13
1.1. Assessment Criteria − Likelihood (Strategic, Operational, and Project-level) ..13
1.2. Assessment Criteria – Consequence: Strategic and Operational Levels 14

1. INTRODUCTION

1) The Royal Australasian College of Physicians (The College) understands that risks could eventuate from internal and external factors impacting College's ability to achieve its strategic objectives. The College also understands that risk is inherent to all aspects of its operations and therefore the importance of risk management to be able to render services to the stakeholders it serves with minimal or no disruption. To achieve strategic objectives and uplift members satisfaction, effective risk management is central to the College.

2) Where risk is defined as an effect of uncertainty on objectives, risk management is a holistic process for coordinated activities to direct and control an organisation regarding risk[1]. It involves a systematic application of processes, policies and procedures by establishing the context, identifying, assessing, treating, escalating, monitoring, reviewing, recording and reporting risk.

3) This means that the College must review its constantly evolving risk landscape and have a current, relevant, and comprehensive understanding of its risks (including emerging risk) at a level that are acceptable to the College.

4) By managing its risks, the College can provide greater certainty and security to Fellows, Trainees, employees, regulators, and stakeholders resulting in better informed and effective decision making and an improved risk culture boosting confidence to achieve its goals.

5) The College's aim is to integrate all its critical processes with risk management so that before events occur or there is a change in circumstances that might enhance or prevent the College from achieving its purpose and objectives, the College can recognise and respond to the risks in a consistent and proactive way. Equally, if unintended events occur, the College will use systematic processes to learn the lessons from its successes, failures, and near misses.

2. PURPOSE

The Risk Management Policy (Policy) outlines the expectations that the College has in relation to risk management, and to ensure that the risks are being identified and managed in a way that are appropriate for the College's risk landscape and its objectives. The purpose of this Policy is to foster a positive culture where:

- accountability is visible across all levels
- risk is effectively managed by implementing a systematic approach and by integrating risk management into College's core functions
- operational excellence is driven by continuous learning and risk awareness
- sound risk-based decisions are made to maximise opportunities.

3. SCOPE

The Policy applies to all College Bodies, Fellows, Trainees, Management, consultants, contractors and its team members, and they **must** adhere to this policy, while engaged in

activities undertaken as part of their employment or volunteer work with the College. The Policy extends to all jurisdictions where such activity is undertaken.

This Policy shall be read in conjunction with College's Enterprise Risk Management Framework which outlines the overarching risk management guidance to manage risk and in accordance with *ISO 31000:2018 Risk Management Guidelines*.

4. RISK AWARE BEHAVIOURS

The College will be risk aware as evidenced by the following expected behaviours:

i. **Tone from the top** – the College recognises that risk is inherent in every activity of the College and proactively integrates risk awareness, assessment, and management behaviours into all College activities. Risk will be assessed against the Board's published risk appetite statements and management and mitigations approach developed as appropriate.

ii. **Positive risk culture** – the Board and the Senior Leadership Team (SLT) promote a culture that values openness, safety (physical & non-physical) and continuous learning.

iii. **Continuous disclosure** –

   a) the College community will communicate events (incidents, risks including emerging & opportunities) on time to their manager

   b) managers will listen to, and respond appropriately to, concerns or opportunities, and the College community will be encouraged to speak openly and honestly

   c) the SLT will monitor risk and will disclose risks identified as approaching or exceeding the RACP's risk appetite.

iv. **Prudent decision-making** – policies, delegations, processes, and procedures will reflect the degree of risk, empowering agility and innovation. Decisions will be prompt and prudent, based on relevant information.

v. **Single line accountability** – individuals will be held to account for the success of activities, projects, or functions, even when working in groups or teams. Team members will be appropriately empowered to deliver agreed outcomes within the College's risk appetite.

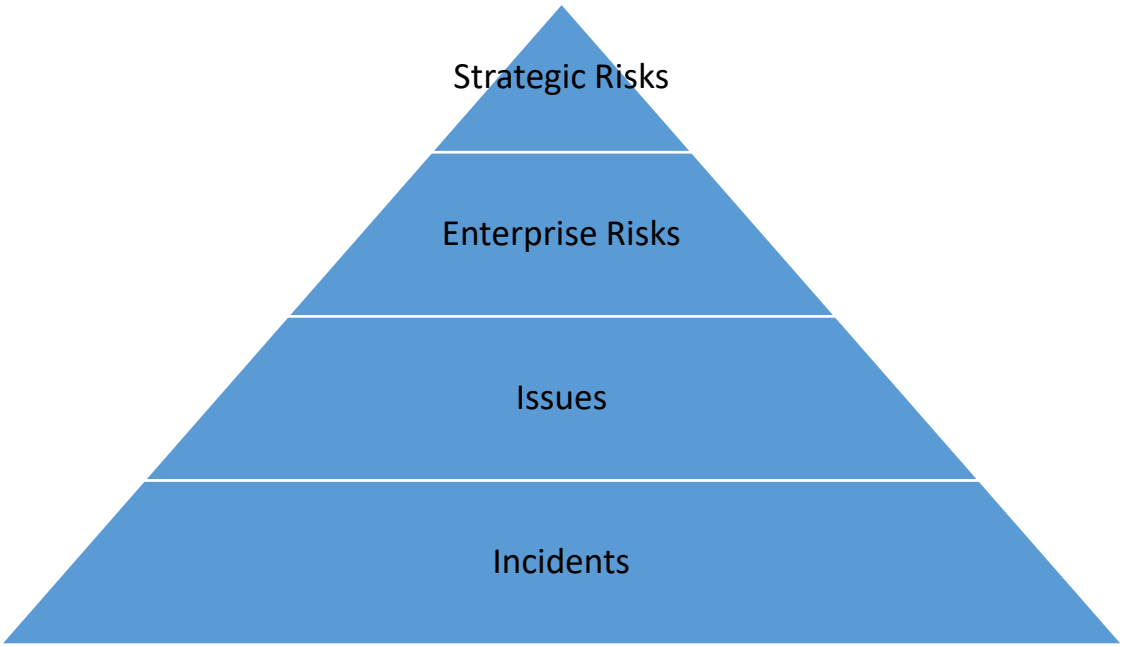
5. HOW IS RISK MANAGED AT THE COLLEGE

The College's risk management process is dynamic and is designed to evolve with College's strategic objectives and changes to its risk profile over time including internal and external risk factors.

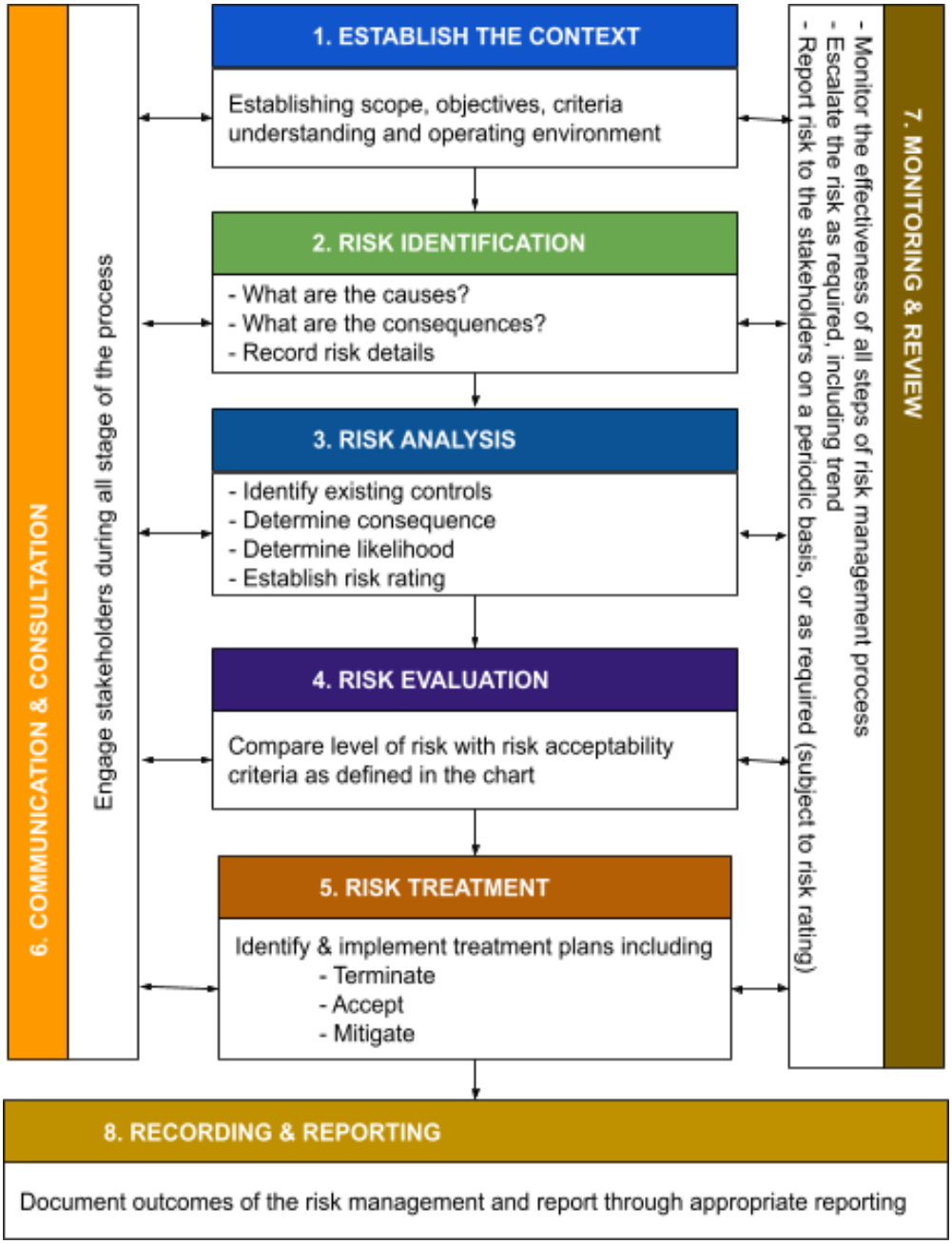
Regardless of the risk type i.e. whether strategic or operational or project, risk rating and location; the College has an accountability to manage it. The College undertakes a risk assessment when a threat or an opportunity is identified with the Risk & Compliance Manager, or the assessment is shared with the Risk & Compliance Manager. Post assessment. Where a residual risk rating exceeds the appetite, the risk is escalated to the relevant SLT member prior to proceeding on the task.

To implement the risk management process effectively, it is critical to understand the difference between an incident, issue, emerging risk and a risk; so that adequate resources are provided through timely decision making and thorough strategic planning for each event type and its management.

The College uses the below framework to manage the risk using the Bow-tie analysis method (outlined on Risk Management's SharePoint page).



Incident	Issue	Risk	Enterprise Risk	Strategic Risk
An event, situation or occurrence that might be, or could lead to, a disruption, loss, emergency or crisis such as an employee tripping on a recently mopped floor or an act of terrorism or a cyberattack.	Any actual event that has already occurred or is currently happening and is negatively impacting the College due to a systemic failure of a key control or key process established to mitigate the impact from incidents. The impact from an issue is significantly bigger than an incident as incidents keep occurring. E.g. injuries to staff due to tripping at the internal stairs.	An event that is considered to potentially have a significant impact on College's objectives with a potential of disruption to the core activities and/or its credibility such as ability to deliver high-quality member satisfaction due to dated systems and not acting on members' feedback.	Comprehensive management of all potential risks faced by the College in an integrated way (also known as core business risks) e.g. psychosocial risk impact staff and members or financial sustainability or adherence to compliance obligations	A risk that poses a threat to the College's ability to set and execute its overall strategy; and has a direct impact on College's ability to achieve its strategic outcomes such as financial sustainability or ability to attract talent or retain its existing talent



RACP Risk Management Process Map

The risk management response plan outlines how risk is managed at the College based on its risk rating, including its governance and reporting.

Risk Management Response Plan

Risk Management Process & Response Plan based on Risk Rating	
Extreme & High	**Medium & Low**
Step 1: Establish the context for the risk **Step 2: Identify** the objective and then associated risks hindering achievement of the identified objective. **Step 3: Analyse the risk** using the Bow-tie analysis method to determine its severity (likelihood & consequences) and rating (Refer to Appendix A). **Step 4: Treat** the risk by identifying current controls, where applicable, and propose treatment plans to prevent recurrence. **Extreme** - Immediate consideration whether the activity should be ceased. Escalate the risk to the SLT/FRMC/Board for consideration. Ongoing risk assessment & oversight. **High** - Periodic thorough review, reporting to SLT/FRMC & Board. Proposal of treatment plans to reduce exposure. **Step 5: Escalate and Report** to the relevant EGM for guidance, support and resources. This is to ensure risks are assessed, managed and escalated promptly through a collaborative approach. Relevant EGM must liaise with Manager Risk & Compliance to undertake a thorough risk assessment. Relevant EGM to oversee the risk and inform the CEO. CEO to inform the Board, where necessary **Step 6: Monitor** the effectiveness of all undertaken steps for continuous improvement. Review the Extreme rated risk monthly and High risk on a quarterly basis. **Step 7: Communicate** details of risk review with impacted stakeholders, including Manager Risk & Compliance. **Step 8: Record/Update** risks to JIRA. Summary of all High/Extreme risks to be reported by EGM – SS to the SLT/FRMC/Board on a periodic basis.	**Step 1: Establish** the context for the risk **Step 2: Identify** the objective and then associated risks hindering achievement of the identified objective. **Step 3: Analyse the risk** using the Bow-tie analysis method to determine its severity (likelihood & consequences) and rating (Refer to Appendix A). **Step 4: Treat** the risk by identifying current controls, where applicable, and propose treatment plans to prevent recurrence. **Medium** - Exposure is acceptable, provided thorough assessment on a periodic basis. **Low** - Exposure to risk is acceptable. Disseminate to operational risk, where approved by the SLT/relevant EGM and to be managed by the relevant Manager. **Step 5: Escalate and Report** to the Manager for guidance and support. No escalation required to the EGM/CEO. **Step 6: Monitor** the effectiveness of all undertaken steps for continuous improvement. Review the risk at least on a semi-annual basis and update the risk register. **Step 7: Communicate** details of risk review with impacted stakeholders, including Manager Risk & Compliance. **Step 8: Record** risks to the relevant systems (JIRA). Share details of risks (new & existing risk) with Manager Risk & Compliance for reporting, trend analysis and continuous improvements purposes. Manager Risk & Compliance to report to the ELT on the risks with common themes/root causes.

5.1. Risk Reporting and Governance

Once the risk is assessed, it should be reviewed as outlined in the table below. Depending on the risk rating, it must also be escalated through the appropriate channels to the relevant stakeholders by the Risk & Compliance Manager.

Risk Rating	Review & Reporting
Extreme	Monthly and escalated to SLT & Board where required.
High	Quarterly and escalated to SLT & Board where required.
Medium	Semi-annually and escalated to the SLT.
Low	Annually and managed by the relevant SLT member. Escalated to the SLT where relevant.

6. ROLES AND RESPONSIBILITIES

Role	Responsibilities
Board	1. Setting the 'tone at the top' by championing the College's risk management processes, review and approval of the Policy, Framework and the Risk Appetite Statement (RAS) and encouraging the right attitude to risk management amongst Fellows, trainees, and Team members 2. Regularly review and monitor the risk profile and risk limits against the approved thresholds 3. The Board, through the College Finance and Risk Management Committee, will make sure that the necessary resources are available to ensure that the College's risks are managed effectively 4. Establish an effective risk management and governance including strategic risk oversight of College's performance 5. Governance of the College and promotion of the College's interests by: a. ensuring that a sound system of risk management and internal control is implemented which, in all material respects, implements the policies adopted by the Board b. oversight and monitoring of the College's performance, the management of its most critical risks, and the effectiveness of its control processes c. determining the appropriate level of risk that the College is willing to accept d. reviewing recommendations from the Finance and Risk Management Committee and determining future actions e. approval of the College's list of strategic risks and risk treatment strategies (the strategic risk register).
Finance and Risk Management Committee (FRMC)	1. Oversight of and review the College's risk management activities and performance and its escalation to the Board 2. Monitoring the implementation of the risk management framework by a) receiving reports from management, external and internal auditors, legal counsel, regulators, and consultants as appropriate b) monitoring the strategic risk register c) reporting to the Board concerning the management of risks within the College d) at least annually providing to the Board an up-to-date register of the key risks facing the College

	e) assessing whether the College's risk management processes are continually adapting to reflect the changing environment f) act as a sounding board and key advisor to the Board for RAS g) escalate when the risk tolerance levels exceed the threshold.
Chief Executive Officer (CEO)	1. Implementing a sound system of risk management and internal control which, in all material respects, implements the policies approved by the Board. This includes translation and operationalisation of RAS into risk limits for each directorate for pragmatic decision-making 2. Ensuring that the risk management policy and framework are understood, adopted, complied with and effective at all levels of the College 3. Ensuring that a College-wide risk register, together with appropriate risk treatment plans, is reviewed and updated at least twice a year 4. Championing the College's risk management processes and encouraging the right attitude to risk management amongst Fellows, Trainees and Team members 5. Oversight strategic risks and ensure resources are provided to manage such risks 6. Brief the Board, FRMC Chair, as required, on risk with extreme and high residual risk ratings and other matters that pose significant impact on the College and achievement of its strategic objectives. This includes reporting of events exceeding the RAS to the Board Chair, where required 7. Ultimate responsibility and accountability for management of risk across the College 8. Provide support and guidance towards long-term preventive actions to manage risk 9. Foster a culture of continual improvement including effective and positive risk management 10. Making any reports and disclosures relating to risk required by law or regulation.
Senior Leadership Team (SLT)	1. Ensuring that: a. all material risks to the College are detected, understood, and responded to in accordance with its risk management policy and framework b. risk management activities and internal control systems operate effectively c. any inconsistencies, conflicts, and gaps in the College's risk management activities and internal control systems are identified and addressed. 2. Determining the relative priorities of strategies to manage risks and allocating resources between treatment strategies. 3. Assigning ownership of material risks. 4. Approving the risk analyses and risk treatment plans prepared by unit managers, project managers or process owners, including approval of additional resources where required 5. Periodic review and approve College's risk appetite statement (RAS) and tolerance levels for effective risk management. 6. Developing performance indicators to measure the effectiveness of the risk management activities and risk treatment plans for which they are accountable 7. Ensure their team members receive risk management training and support to implement the Policy & the Framework 8. Identifying and monitoring: a. the adequacy and effectiveness of the key controls on which the College is heavily reliant b. legal and regulatory obligations imposed on the College and appropriate compliance regimes c. systems, policies, processes, and procedures that promote effective risk management.

College Bodies, Heads of Programs, Projects and Functions	1. Identifying potential risks and advising the relevant member of Senior Management accordingly 2. Managing risk as it arises in their area(s) of responsibility as allowed by their By-Laws or Terms of Reference 3. Complying with all College policies, frameworks, and guidelines, including the: a. Risk Management Policy b. College Code of Conduct (where relevant) c. being aware of and accountable for the risks, controls, and treatment tasks allocated to them.
Risk Owner	1. Create and maintain formal records of key actions and decisions undertaken to manage the risk, including maintenance of records in the relevant systems with access to authorised personnel only 2. Complete an in-depth risk assessment to mitigate the risk, in conjunction with the Risk & Compliance Manager to ascertain the risk rating 3. Notify the relevant EGM when a new risk is identified, with its risk rating.
Risk & Compliance Manager	1. Supporting the CEO in ensuring that the: a. directives of the CEO and the Senior Leadership Group are implemented and followed b. Risk Management Framework is understood and coordinated across the College c. risk management processes are implemented and working effectively d. promote consistent application of risk management processes are implemented and working effectively e. work with the Board and SLT to develop an appropriate RAS for the College that meets the needs of the College and align with the College's strategic direction f. ensure RAS is approved by the Board and is periodically reported to the Board and the FRMC on the risk profile relative to the RAS. 2. Collation and recording risks identified and treatment strategies in the Risk Register 3. Providing the Board, College Bodies, and Team members with appropriate training on risk management principles and procedures where required 4. Monitoring of compliance with the risk management cycle; and reporting on new, emerging, and material risks to the Finance and Risk Management Committee 5. Supporting program and business managers in their risk management responsibilities by: a. advising on appropriate risk management procedures and measurement methodologies throughout the College b. assisting in the identification of stakeholders and parties affected by a potential risk c. reviewing risk analyses and risk treatment plans prepared by management, challenging the bases of assumptions, and advising on potential treatment strategies prior to submission for approval by the Risk Owner d. providing risk workshops where required. 6. Co-ordinating risk management training and a network of risk champions throughout the business 7. Advise SLT on risk matters, including breach of RAS thresholds, shared and insurable risks.
All staff	1. Understand the Policy and seek advice or support on how to implement risk management within their daily operations 2. Identify any incidents, issues, risks (including emerging risks), compliance matters and concerns and escalate to their line manager or relevant SLT member, as appropriate 3. Participate in risk management training relevant to their role 4. Contribute to a positive risk culture that encourages open and regular discussion of risks, with concerns about business practices raised and acted upon promptly.

Risk Champions	1. Nominated staff who lead their colleagues by modelling good risk behaviours 2. Lead risk activities, initiatives and assessments and encourage effective risk management in their area 3. Network with other risk champions to share good practice and build skills and capability.
Control Owner	1. Responsible for designing, maintaining and monitoring the control 2. Documenting its design and operating procedures and its periodic testing to ensure it is mitigating the risk as intended 3. Reporting any failure (design or operational effectiveness) to the relevant SLT 4. Work with other risk champions and R&C team to ensure proper governance.

7. REVIEW OF POLICY

1) This policy will be reviewed every two years or as required in the event of legislative changes or requirements. The policy may also be changed as a result of other amendments.

2) Team members and members of the College may provide feedback about this document by emailing RACPPolicy@racp.edu.au.

8. DEFINITIONS

Term	Means
"Board"	the Board of Directors of the College.
"College"	The Royal Australasian College of Physicians, ACN 000 039 047, an incorporated body limited by guarantee.
"College Body"	1) the council of each Division or Faculty of the College 2) the Committee of each Chapter formed within a Division or Faculty 3) each Board Committee 4) each Committee, sub-committee, working group, expert advisory group or other sub-group formed under the auspices of any of the above, whether limited in time or purpose or not.
Emerging Risk	A new or an unforeseen event that has not yet been considered but should be on the radar, but it isn't, and its potential for harm or loss is not fully known. However, there are signs/precursors of incidents happening occasionally such as increase in insurance costs due to psychosocial impact on staff and members.
"College Group" or "Group"	the Board and any College Body
"Fellow", "Trainee", and "Member"	have the same meaning as in the College Constitution
"Material Risk"	those risks, either strategic or operational, that the Senior Leadership recognises as having the potential to materially impact the College's performance
"Risk"	the effect of uncertainty on objectives. Risk is not just about negative outcomes but any deviation, positive or negative, from expected objectives, caused by uncertainty.

Term	Means
“Risk Management”	coordinated activities to direct and control an organization with regard to risk
"Senior Leadership Team”	The Chief Executive Officer, General Counsel, and Executive General Managers of the College
“Team members”	Employees of the College, contract workers, and volunteers engaged in the operations of the College.

9. HISTORY

Revision	Effective Date	Summary of Changes
1.0	March 2012	Initial approval.
2.0	February 2017	Updated references to College Risk Management Committee to reflect merger with Finance Committee
3.0	February 2020	1) Updated reference to ‘Department’ and ‘Owner’ to reflect a change in organisational structure 2) Updated reference to AS/NZS standard 31000 to reflect the adoption of the updated standard
4.0	April 2020	Amendment of section 2.4 and addition of Section 3 “Roles and Responsibilities
5.0	May 2020	Addition of “education” to the role of Risk and Compliance Manager
6.0	June 2022	1) Explicitly included Fellows, trainees, Management, and Team members in the scope 2) Inserted section 4 “Risk-aware Behaviours” 3) Strengthened wording of clause 5.4 to emphasise the role of the FRMC. 4) Minor terminology adjustments: “staff” and “employees” to “Team members”, “Senior Leadership Group” to “Senior Leadership Team.” 5) Minor grammatical and stylistic changes 6) Updated document to new template
7.0	Sept 2025	1) High-level review of the Policy and converting section 6 into a table including adding roles and responsibilities for team members and risk champions for its review by Grant Thornton (GT – IA).
8.0	Oct 2025	1) Updating RMP per feedback from the IA
8.1	May 2026	1) Updated roles and responsibilities per IA (#357)

1. APPENDIX 1: RISK MATRICES

Likelihood / Consequence	1 – Insignificant	2 – Minor	3 – Moderate	4 – Severe	5 – Catastrophic
5 – Almost Certain	5 – Medium	10 – High	15 – High	20 – Extreme	25 – Extreme
4 – Likely	4 – Medium	8 – Medium	12 – High	16 – High	20 – Extreme
3 – Possible	3 – Low	6 – Medium	9 – Medium	12 – High	15 – High
2 – Unlikely	2 – Low	4 – Medium	6 – Medium	8 – Medium	10 – High
1 - Rare	1 – Low	2 – Low	3 – Low	4 – Medium	5 – Medium

1.1. Assessment Criteria − Likelihood (Strategic, Operational, and Project-level)

RATING	POTENTIAL FOR RISK TO OCCUR
Almost certain	Likely to occur several times a year or more than once in the life of a project
Likely	Likely to occur once a year or at least once in the life of a project
Possible	Possibly occurs once every few years; a 50% chance of occurring during a project.
Unlikely	Might occur once in 5 years; a 20% chance of occurring during a project
Rare	Might occur once in 10 years; a 10% chance of occurring in a project

1.2. Assessment Criteria – Consequence: Strategic and Operational Levels

Source	Catastrophic	Severe	Moderate	Minor	Insignificant
Strategy	- failure to deliver strategic priorities for a prolonged period resulting in threat of on-going existence - failure to deliver a strategy which is unmanaged, unmitigated and unexpected requiring some services to be terminated e.g., nonalignment to strategy	- failure of delivery of a significant component of a strategy for consecutive months to years - significant delay in timely delivery of strategic objectives requiring some services to be terminated e.g., nonalignment to strategy or complete restructure to align to mission and strategy of the entity including reduction in staff - significant increase in cost/effort for stakeholders (6-12 months).	- delay or threat to timely delivery of key components of a strategic objective with a need to review or revise the strategy outcome - moderate increase (up to 6 months) in cost/effort for stakeholders from impairment of activities.	- minor degradation in quality of services provided by Agencies (Strategic) or minor threat of delivery or timing of a strategic objective that can be addressed by those responsible - marginal increase in cost/effort for stakeholders to assess and update the strategy.	- insignificant to no reduction in quality of service or delivery of strategic outcomes (including timeliness) - remediation by updating processes or minor adjustments to the strategy.
Reputation	- reputation, confidence, and trust irrevocably destroyed or damaged resulting in significant changes in member and stakeholder perception for RACP - international / National media coverage - formal and prolonged intervention by canonical or civil jurisdictions.	- loss of reputation, confidence, and trust severely damaged requiring considerable cost, extensive time and effort to rebuild - sustained negative national and state media coverage utilising staff resources - formal communication and intervention by canonical or civil jurisdictions.	- state-wide adverse media coverage resulting in reputational damage, loss of stakeholders' confidence and trust with some time, cost and effort required to recover reputation - shorter-term state and local adverse media coverage.	- member and stakeholder complaints - confidence and trust impacted but satisfactorily resolved - loss of reputation is localised - limited to local news coverage.	- minor loss of goodwill or stakeholders' trust - internal complaints about lack of adherence to procedures - no local news coverage.

Financial	- threatens organisational viability due to financial loss (one-off or ongoing loss >$10m) - more than 10% drop in receipt of membership fee. - membership exits increase by 10% or more from the same time last year - may raise concerns for insolvency or require external intervention by auditors/regulators	- may raise concerns for insolvency or require external intervention by auditors/regulators with one-off or ongoing loss between $5-10m - drop in 6% -10% membership or equivalent member exits or inability to recover membership fee dues.	- one off loss resulting in moderate overspend or loss of income of >$1m and <$5m - multiple strategic priorities delayed or cancelled resulting in Board reviewing recovery plan - drop in membership fee overdue by >1% but <6% from same time last year - membership exits increase by >1% but <6% from same time last year	- one off loss resulting in overspend or loss of income of >$500k but < $1m - localised or project-level budget issue; contained with management oversight. - drop in membership fee overdue by >0.5% but <1% from the same time last year - member exits increase by >0.5% but <1% from the same time last year	- one off loss resulting in overspend or loss of income less than $500k - ongoing annual financial impact of <$500k - increase in membership fee overdue rates by more than 0.5% from the same time last year - members exits increase by 0.5% from the same time last year.
---------- **Fraud & Corruption**	- systemic acts of fraud or corruption across parts of RACP for a sustained period to obtain actual or perceived gains - one off large fraud event involving multiple staff through collusion - significant issue with culture of the entity which fails to identify misuse of power, fraud and corruption - prolonged legal action taken on those involved in defrauding the entity	- repeated acts of fraud or corruption for a sustained period by one or more staff to obtain significant or actual prospective gains - one off large fraud event involving one or more staff through collusion - substantial remediation work on process review and controls required - legal action taken on those involved in defrauding the entity - reimbursement imposed for any financial lost to the entity - potential Mandatory reporting to external agencies	- repeated but insignificant incidents of fraud by one or more staff for a limited period of time through misuse of money, resources, confidential information or delegations with moderate impact and benefit (actual or perceived) from an activity - remediation achieved via EGM across multiple areas with mandatory training required - reimbursement imposed for any financial loss to the entity	- single, isolated and minor incident by a staff through misuse of money, resources, confidential information or delegations with no, limited or minor impact and benefit (actual or perceived) from an activity - remediation can be achieved through Manager/EGM intervention with training and counselling for all involved - reimbursement imposed for any financial loss to the entity.	- potential weaknesses in compliance with the Fraud and Corruption policy. Gaps managed through review of internal controls (such a policy review, undertake training etc).

Source	Catastrophic	Severe	Moderate	Minor	Insignificant
	- reimbursement imposed for any financial lost to the entity - substantial remediation work required to undertaken by the entire RACP - mandatory reporting and penalties imposed by regulatory authorities and potential prosecution against RACP.	- disciplinary action which may include dismissal of all relevant staff. Matter referred to ICAC / relevant	- disciplinary action which may include dismissal of relevant staff.		

Source	Catastrophic	Severe	Moderate	Minor	Insignificant
Operational (Crisis Management including BCP and Critical Infrastructure, Facilities & Asset Management, IT including Networks, Server etc) **-----** **Cybersecurity**	- failure to achieve objectives including total shut down due to multiple critical incidents at single or multiple sites resulting in unavailability in resources (down time of staff and applications) for an extended period (> 10 business days). - mandatory compliance orders & fines imposed by OAIC / regulators - significant interruptions to business operations entire College - loss of all member & employee data due to data breach	- failure to achieve some operational objectives due to major disruptions across single or multiple sites (> 5 business days & ⩽ 10 business days) resulting in inability to continue normal operations - prolonged significant impact on the operations and staff - critical operations interrupted - voluntary compliance orders or fines by regulators - significant Interruptions to business operations affecting 5 or more business units - significant loss of member or employee data due to data breach	- disruption at a single site or across multiple sites due to restriction of services reducing operational deliverables (> 2 business days & ⩽ 5 business days) - moderate impact on operations - all non-critical operations suspended. - several complaints in relation to data breaches - ongoing regulatory audits and monitoring - significant interruptions to business operations affecting 3 or more business units - impact on member or employee data where majority of data could be recovered i.e. prevented from leaving RACP system	- minor interruptions to service delivery and to operations at a single or multiple sites (> 6 hours & ⩽ 2 business days) resulting in minor operational degradation - limited impact to staff. - complaints of data loss from a few stakeholders being resolved by process improvement and staff training - interruptions to business operations affecting 1 or more business units - multiple phishing emails impacting member or employee data - update by cybersecurity policy	- limited localised interruptions to service delivery of operations (short & infrequent disruptions to services (< 6 hours) resulting in insignificant operational degradation - no impact to staff. - complaint from stakeholders for their personal data being used without consent expressing concerns expressed, being rectified by process improvement - no business interruption or loss of member or employee data
Compliance	- mandatory compliance orders - fines which threaten the liquidity of the College	- voluntary compliance orders or fines ≥$100k	- fines ≥$50k <100k - regulators formally investigate the activities of the College	- fines ≥$10k <$50k - regulators raise formal queries about the operations of the College	- fines >10k - regulators contact RACP to clarify information

Source	Catastrophic	Severe	Moderate	Minor	Insignificant
	- all or most stakeholder groups lose confidence in the College - systemic and substantial non-compliance with legislation, regulations or policies resulting in enforceable undertakings - significant penalties imposed by regulatory and legislative authorities - prosecution of Responsible Officers - sanctions imposed to operating conditions by external regulators, loss of licence to continue operating for medium to long term until remediation is completed.	- regulators or Governments lose confidence in the College - repeated non-compliance with legislation, regulations or policies resulting in an enforceable undertaking. - significant financial penalties imposed on business operations - single, isolated or a combination of systemic patterns of non-compliance with legislation, regulations which could result in enforceable undertakings due to negligence and review of Compliance Management Framework.	- regulators or Governments express concerns about the management or governance of the College - repeated instances of non-compliance with legislation and regulations which could result in one-off financial penalty or potential regulatory intervention or loss of confidence in internal processes if not corrected promptly or if no remediation processes is demonstrated - potential review of compliance management framework and procedures.	- more than one stakeholder group expresses formal concerns about the management or governance of the College - isolated incident of non-compliance with obligations and policies - legal/compliance issues require professional advice and have internal impact.	- one stakeholder group expresses limited concerns about the management or governance of the College - minor, one-off, low-level non-compliance with standards, procedures, and policies with limited impact on business operations - issues can be addressed with minor changes in internal standards, policies, and procedures.

Source	Catastrophic	Severe	Moderate	Minor	Insignificant
Wellbeing, Health, and Safety (Physical)	- single or multiple fatalities - physical injury or illness resulting in irreversible total permanent impairment or disability - significant and prolonged workers compensation claims by multiple staff - penalties or jail terms imposed under the WHS Act by SafeWork NSW or through criminal litigation.	- physical injury or illness resulting in partial disability or long-term impairment - significant but not prolonged workers compensation claims by multiple staff - SafeWork NSW receives complaints regarding H&S matters. Investigation undertaken by SafeWork NSW and issues an improvement or prohibition notice.	- physical injury or illness resulting in impairment with potential for shorter term hospitalisation (6-12 months) - notification/complaint made to relevant regulator (SafeWork NSW, Fair Work or UNHRC) regarding H&S matters. Investigation undertaken by regulator resulting in updates to processes, policies and procedures - SafeWork NSW receives a complaint regarding H&S and investigates the matter recommending significant updates to policies, procedures and processes.	- physical injury or illness requiring professional medical attention with no long-term impact (3 - 6 months) - H&S procedures may require review.	- physical injury or illness requiring treatment or that can be addressed up to first aid and does not require any further medical attention.

Source	Catastrophic	Severe	Moderate	Minor	Insignificant
WHS (non-physical)	- staff death by suicide, permanent impairment or disability resulting from a major incident or due to a breach of duty of care at College locations - significant capability gap identified/ongoing effect on staff deliverables across multiple teams resulting in widespread absenteeism, lack of confidence and trust from staff - failure to report incidents to the relevant regulator within the approved timeframe - significant and prolonged workers compensation claims due to stress related to staff's wellbeing management.	- significant or persistent mental health concerns resulting in serious risk of harm to self or others or notable distress to others - long term (6 - 12 months) loss of capability / ongoing effect on staff deliverables across multiple teams resulting in widespread absenteeism. Matter not managed by the relevant EGM and escalated to the SLT/Board - delay in reporting incidents to the relevant regulator resulting in review of procedures and staff dismissal - matters reported to external regulators and processes being reviewed and issues an improvement or prohibition notice.	- frequent disagreements about how work should be managed and interpersonal workplace conflict resulting in harmful workplace behaviour that is not managed properly through an agreed risk management plan. Matter escalated to P&C/SLT. Actual physical harm requiring hospitalisation, emergency services contactable rendering medical support - staff engage in an ongoing pattern of behavioural issues with vicarious trauma - medium term (3 - 6 months) loss of capability / ongoing disability or resulting in absenteeism - one-off matter reported to the external regulators and investigates the matter recommending moderate updates to processes, policies and procedures.	- psychological injury or illness requiring professional medical attention with no long-term impact - repetitive complaints due to lack of controls / following procedures requiring procedures review - short term (up to three months) loss of capability/temporary effect resulting in absenteeism across one or two teams - inadequate information, advice and help provided by the manager.	- conflicts at College location, but not escalating to actual violence/arguments - risk management plans not effectively supporting and escalating to behavioural issues - short term (a couple of weeks) loss of capability / temporary effect of staff deliverables and limited to one or two teams.