Risk Management Policy and Guidelines (QA-Pol-022)

Document Title	Risk Management Policy and Guidelines
Document Number	QA-Pol-022
Version	1.0
Department	Manager, Quality Assurance and Risk Management
Owner/Responsible for Implementation	Head of Professional Affairs
Approving Body	Senior Management Group, Executive Board
Effective date:	October 2020
Next Review date:	October 2022
Related Documents	QA-Pol-023 – Quality Assurance and Enhancement Policy ED-SOP-098 – Programming Monitoring and Review Procedure Gov-TOR-004 – Finance, Audit and Risk Committee TOR

1. Risk Management Policy

1.1 Introduction

The Royal College of Physicians of Ireland considers risk management to be fundamental to good management practice and a significant aspect of corporate governance.

The objective of Risk Management is to improve the College's ability to deliver on its strategic and operational objectives by providing a framework to manage threats and opportunities in a systematic and transparent manner.

Risk Management is an integral part of RCPI's strategic policy decisions and the initiation of major projects, therefore, the adoption of best practice in the identification, evaluation and control of risks is critical as it informs the decision-making process.

This approach to risk management is reflected in RCPI's business processes, including:

- Strategic & operational planning
- Financial planning
- Service planning
- Policy making and review
- Performance management
- Project management
- Partnership working

1.2 Risk Management Objectives

RCPI is committed to establishing and maintaining a systematic approach to the identification and management of risk. The College's risk management objectives are to:

- Prevent death, injury, damage and losses, and reduce the cost of risk and opportunities.
- Ensure compliance, as a minimum standard, with legal obligations
- Inform policy and operational decisions by identifying risks and their likely impact.
- Anticipate and respond to changing economic, social, environmental and legislative requirements.
- Agree an appropriate Risk Control Approach to each opportunity being considered.
- Raise staff awareness of the need for risk management.
- Ensure that all significant risks to the College nationally and internationally are identified, assessed and where necessary treated and reported to the Executive Board in a timely manner.

These objectives will be achieved by:

- Adopting best practice in the management of risk.
- Ensuring that risk management is consistently integrated in the activities of the organisation.
- Demonstrating the application of risk management principles in the activities of the College.
- Clearly defining the roles, responsibilities and reporting lines within the RCPI for Risk Management.
- Assigning accountability to all staff for the management of risks within their areas of control.
- Including risk management when considering decisions or facilitating decision-making.
- Reinforcing the importance of effective risk management as part of the everyday work of our staff.
- Maintaining a register of risks linked to the RCPI's business, strategic and operational objectives.
- Maintaining documented procedures for the control of risk and provision of training and supervision.
- Maintaining an appropriate system for recording health and safety incidents and identifying preventative measures against recurrence.
- Undertaking compliance audits and monitoring risk mitigations.
- Preparing contingency plans to ensure business continuity where there is a potential for an event to have a major impact upon the RCPI's ability to function.
- Encouraging an environment where we regularly ask:
    - What could go wrong?
    - How likely is it to happen?
    - What would the impact be of it happening?
    - What should be done to reduce the risk?
    - Who owns the risk?
    - Having evaluated and reduced specific risks can the decision now go ahead to implementation?
    - What else do we need to do about it?

1.3 Risk Reporting Structure

Risk Reporting				
Document	**Sent To…**	**Frequency**	**Purpose**	**Responsibility**
Risk Register	SMT	Monthly	Discuss management of red risks.	Manager, QA and Corporate Risk
	Executive Board	Quarterly	Consider management of red risks and request attendance of risk	
	FinARC	Each Meeting	Approval of register and consideration of management response & mitigating actions and provide assurance to	
	Academic Board (Academic/ Programme delivery risks only)	Each Meeting	Review, assessment and mitigation of risks to QQI validated programmes	Secretary of the Academic Board
Risk Management Policy / Risk Appetite	SMT Executive Board FinARC	Annually	Review and recommend Changes	Manager, QA and Corporate Risk
FinARC Report on Risk Management	Executive Board and Council	Annually in October	Assurance to Council that risk is being managed appropriately	FinARC Secretary

1.4 Risk Tolerance

RCPI - Risk Tolerance Table			Low			Medium			High		
	Code		1. Low	2. Low	3. Low	4. Med	5. Med	6. Med	7. High	8. High	9. High
Core Mission	A	Training Standards					X				
	B	Trainee Services					X				
	C	Trainer Services					X				
	D	Member Engagement							X		
	E	Course Development						X			
	F	Examinations	X								
	G	International Services							X		
Building Relationships & Ensuring Compliance	H	Medical Council Relationship			X						
	I	QQI Relationship			X						
	J	HSE Engagement			X						
	K	Training Site Relationships				X					
	L	Forum Relationships				X					
	M	Policy and Advocacy						X			
	N	Statutory Compliance	X								
	O	Litigation	X								
Business Development & Continuity	P	Financial Stability / Growth		X							
	Q	Enabling Operations / Efficiency			X						
	R	Staff Engagement / Development				X					
	S	Innovation in Service Delivery							X		
	T	Change Management					X				
	U	Digital Strategy					X				
	V	Web / Online Services					X				

1.5 Responsibilities

All staff must understand the nature of risk and accept responsibility for risks associated with their area of work.

Employees with responsibility for achieving objectives and making decisions, are responsible identifying and assessing risks, implementing controls and warning mechanisms as well as reporting the risk as appropriate. The Risk Officer is responsible for ensuring that the policy is effectively executed and that there is an effective process in place for the identification, assessment, control and monitoring of risks. Senior Managers have the primary responsibility for identifying and managing risk in conjunction with the Senior Management Team. Senior Managers are responsible for ensuring that proper controls are in place, that resources are used appropriately and that RCPI's strategic and operational objectives are achieved.

The President should ensure immediate action by Senior Management if the nature of a new/emerging risks requires such action. The response to the risk should be reported to the subsequent meeting of the Executive Board.

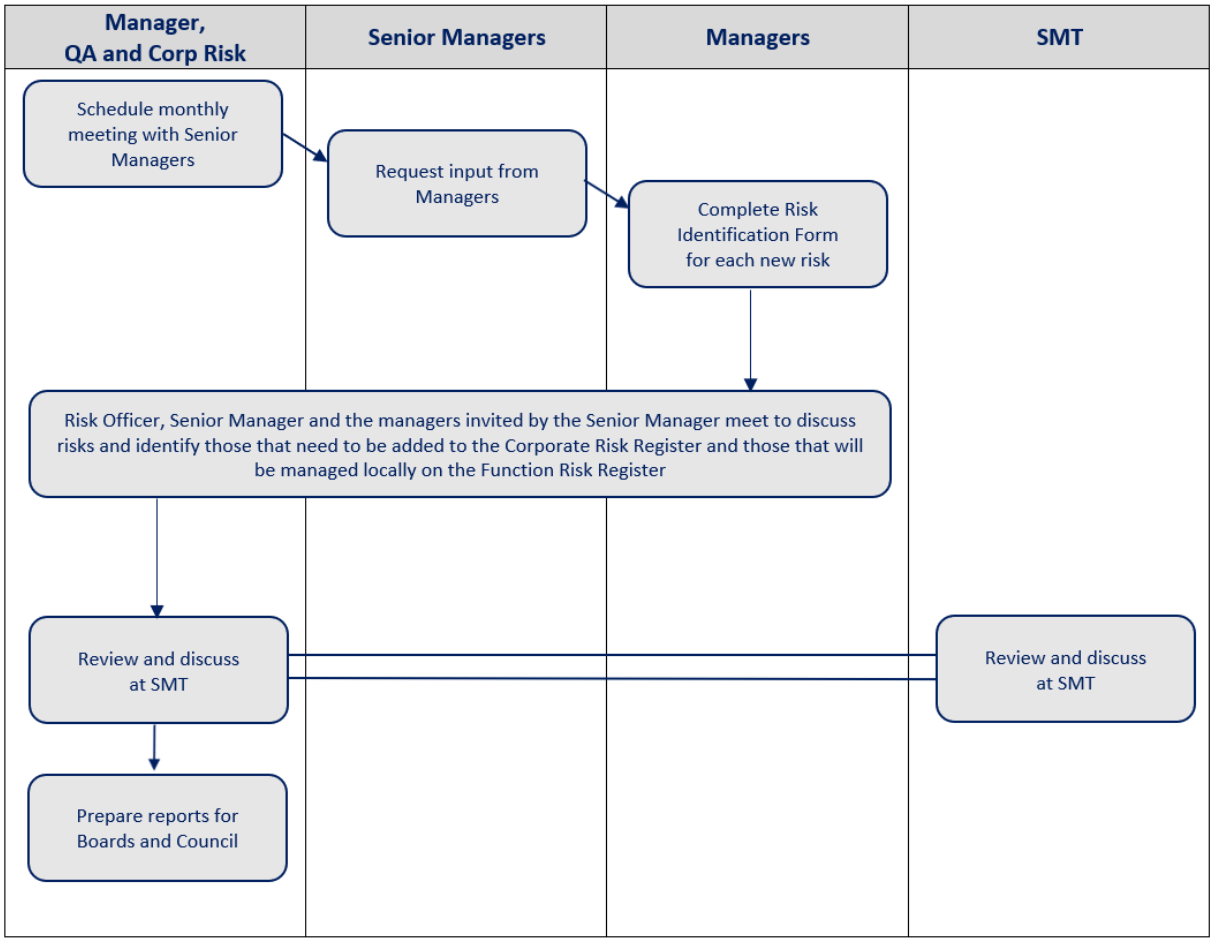
Finance Audit and Risk Committee is responsible for the primary consideration of RCPI's Risk Register with a view to providing assurance to the Executive Board on the management of risk in the organisation. FinARc also makes an annual report to the RCPI Council which includes a section on Corporate Risk Management. The Executive Board must regularly include Risk Management on its agenda, thereby giving the opportunity to provide input to the risk management process following consideration of the Corporate Risk Register.

2. Risk Management Process and Guidelines

2.1 Monthly Update of the Corporate Risk Register

The Risk Register is an important tool for the general management of RCPI and as a source of information in decision-making. It is critical, therefore, that the register contains quality data that is accurate and up to date. The Corporate Risk Register is maintained on a continual basis, through the process illustrated below.

NB - If you are concerned about a risk at any time contact the Risk Officer directly, you do not need to wait until the next reporting cycle.



2.2 Identifying Risks

a. Horizon Scanning

An important aspect of updating the Risk Register is identifying risks that are not immediately obvious. This process is called Horizon Scanning, a methodical review of the influences on the department, the department's own scope of influence, routine processes as well as project and ad-hoc work. Here are some sample questions to use when probing for new risks

- What routine processes are due to start?
    - What went well last month/ quarter/ year? Will the department have the same vantage point this time?
    - What went badly last month/ quarter/ year? Is there are risk that these issues could recur?
    - What has changed since last month/ quarter/ year? e.g.
        - Technology
        - Regulations
        - Logistics
        - Resources
        - Personnel

- What projects or ad-hoc work are underway?
    - If the department is dependent on the successful delivery of the project, what might happen if it is late?
    - Will the mitigation of project risks within the project, adversely impact on the work of the department?
    - Has any stakeholder feedback highlighted potential risks?
    - Are the demands of the project placing an unforeseen burden on staff time or delaying the execution of a process?

b. Describing Risks

Where possible, when describing a risk, it is best to use an "if…then…result" structure (or something similar). Such risk statements are easy for senior managers and clinicians, who are not familiar with the details of your department, to understand the issue of concern. Here are some examples of risk statements:

- If we use an unfamiliar technology, then unexpected design problems may occur, resulting in overspending on the project.
- If we commit to a project design we have never utilised, then we may misunderstand the requirements, resulting in a project which does not meet the performance criteria.

2.3 Assessing Risks

Having identified the risks it is then necessary to determine the **likelihood** of a risk occurring, the **impact** that might result and the resulting **total risk**. These scores are not intended to provide precise measurements of risk but to provide a useful basis for identifying vulnerabilities and ensuring that any necessary actions are undertaken.

As part of the Risk Register maintenance cycle, risk rating is reviewed by the Senior Management Team to check that existing controls are effective, to assess any changes should new controls be established and to adjust the risk rating accordingly.

c. Estimating Likelihood of Occurrence

Using the five-point scale below, assess the **likelihood of each risk**. The risks should be assessed by considering the **controls which are currently in place** to mitigate each risk.

Rating	Score	Threat
Almost Certain	5	Expected to occur or a common occurrence e.g. 80% or above chance of occurrence
Likely	4	Will probably occurs in most circumstances e.g. 70-79% or above chance of occurrence
Possible	3	Might occur at some point e.g. 40-69% or above chance of occurrence
Unlikely	2	Small chance of occurring at some point e.g. 10-39% or above chance of occurrence
Remote	1	Only in exceptional circumstance e.g. Less than 10% chance of occurrence

d. Estimating the Potential Impact

Having estimated the likelihood of the risk, the next step requires **envisaging the effects or impact of a risk** should come to pass. The table below illustrates the severity ratings for the different categories of risk:

Rating	#	Strategic	Financial	Reputational	Operational
Severe	5	Achievement of strategic and operational goals in the medium term are jeopardised. Existence of the RCPI is under threat.	> 10% of Annual Income	Loss of member/trainee confidence. Reputation and standing of RCPI adversely affected nationally /internationally. Serious public outcry and/or international coverage. Reputation adversely impacted with majority of key stakeholders.	Complete disruption or loss of service.
Major	4	Significant effect on operational performance that will require operational resource reallocation (financial, assets and or people) to manage and resolve the issue in the medium term to avoid non achievement of strategic goals.	5 - 10% of Annual Income	Reputation adversely impacted with a significant number of stakeholders. Breakdown in strategic and or business partnership.	Loss of service functions for between 2 weeks and 2 months.
Moderate	3	Some impact on operational performance. Less impact on strategic goals in the medium term.	< 5% of Annual Income	Adverse national media coverage and external criticism. Reputation adversely impacted with some stakeholders.	Loss of business functions for between 1 and 7 days.
Minor	2	Disruption to operations with no permanent or significant effect.	< 1% of Annual Income	Issue raised by stakeholders and/or local press. Adverse local public or media attention and complaints. Reputation is adversely affected by a small number of affected people. Mainly an internal matter.	Loss of business functions for 1 full day.
Insignificant	1	Some localised inconvenience, but no impact to the College.	< 0.5% of Annual Income	Issue resolved promptly by operational management processes. Minimal or no stakeholder interest. Individual grievances	Loss of business functions for less than 1 day.

e. Calculating the Total Risk

Impact x Likelihood = Total Risk

Impact	**Severe (5)**	**5 Low**	**10 Medium**	**15 High**	**20 Extreme**	**25 Extreme**
	Major (4)	**4 Low**	**8 Low**	**12 Medium**	**16 High**	**20 Extreme**
	Moderate (3)	**3 Low**	**6 Low**	**9 Medium**	**12 Medium**	**15 High**
	Minor (2)	**2 Insignificant**	**4 Low**	**6 Low**	**8 Low**	**10 Medium**
	Insignificant (1)	**1 Insignificant**	**2 Insignificant**	**3 Low**	**4 Low**	**5 Low**
		Rare (1)	**Unlikely (2)**	**Possible (3)**	**Likely (4)**	**Almost Certain (5)**
		Likelihood				

2.4 Implementing Controls for the Risk

Effective implementation of controls requires that the following questions can be answered clearly:

- What current controls are in place to reduce the risk?
- What future actions must be done to reduce the risk?
- What else do you need to do about the risk?
- Who owns the risk?
- To whom will the risk owner report?

f. Risk Control Requirements

Management of Risks at Corporate Level

Risk Level	Level of Concern	Target Resolution	Review Period	Review by	Approach
Extreme	An **Extreme** risk is unacceptable. Notification to the next Executive Board meeting or, where necessary, immediately by email. Senior Management consideration is required, and a detailed mitigation plan **must** be put in place and reviewed by the Board.	3 - 6 months	Twice monthly	SMT **Report to:** FinArc Exec Board	Terminate Transfer Treat
High	A **High Risk** is unacceptable. Senior Management consideration is required, and a detailed mitigation plan **must** be developed as soon as possible. Ongoing monitoring by the FinARC and reporting to the Executive Board	6 - 12 months	Monthly	SMT **Report to:** FinArc Exec Board	Terminate Transfer Treat
Medium	**Medium** risks must have a mitigation plan that is developed and implemented locally	12 - 24 months	Every second month As & when a significant change occurs	SMT **Report to:** FinArc	Terminate Transfer Treat
Low	**Low** risks are tolerable. Manage by well established, routine processes	Ongoing monitoring	Every 6 months As & when a significant change occurs	Risk Officer **Report to:** SMT	Tolerate

Depending on the nature of the risk, according best practice in the area, there are four main Risk Approaches. At an operational level, the Risk Approach is typically to **treat** the risk, decisions on major risks requiring **transfer** or **termination** are escalated to the Senior Management Team

Approach	Description	Course of Action
Terminate	A decision is made not to undertake the activity that is likely to trigger the risk. Where the risks outweigh the possible benefits, terminate the risk by doing things differently and thereby removing the risk.	Avoid the risk by withdrawing as the organization is not in a position to carry the risk
Transfer	Share the exposure, either totally or in part, with a partner or contractor, or through insurance. Any partnership will need to be carefully monitored as it may not be possible to transfer all risks and certain aspects	Transfer or share the risk via: - Insurance - Partnerships - Outsourcing
Treat	The most common approach is to introduce preventative actions to reduce the probability or impact if the risk occurs.	Use of Internal Controls - Training - Oversight - Risk Awareness Diversification
Tolerate	The ability of an effective action against some risks may be limited or the cost of taking such action may be disproportionate to the potential benefits gained.	Manage with routine processes

2.5 Monitoring & Review of Risks/ Controls

Few risks remain static, therefore Risk Management is a continuous and dynamic process. New issues are likely to emerge, existing risks may change, the impact or likelihood will be reviewed following the implementation of controls and some risks will be eliminated. It is essential that they are routinely monitored to fully understand our risk landscape and to assess the effectiveness of our risk management process.

Monitoring progress and critical review of the process provides:

- Assurance that progress is being made towards controlling risks
- Assurance that controls are effective
- Knowledge of any changes to the risk due to shifting circumstances or business priorities.

When undertaking the monitor and review process, guidance is given below on the sorts of questions that should be considered:

- Are the risks still relevant?
- Has any event occurred that could impact on them?
- Are performance indicators appropriate?
- Are the controls in place effective?
- Have risk scores changed, and if so, are they decreasing or increasing?
- If risk profiles are increasing, what further controls might be needed?
- If risk profiles are decreasing, can controls be relaxed?

Where objectives have not been achieved or are not on programme to be achieved, the cause should be investigated to inform and improve the risk assessment process.

The monitoring and review process should be integrated into existing business processes so that it adds value and supports the successful achievement of objectives and is not just seen as a 'bolt on'. In RCPI, the Risk Reporting Structure ensures that these reviews are integrated and regular.

Glossary and Definitions

Risk:

Risk is the chance or possibility of loss, damage, injury or failure to achieve objectives caused by an unwanted or uncertain action or event. It is important to differentiate between risks (uncertainties) and management issues.

Risk Management:

Risk management is the planned and systematic approach to the identification, evaluation and control of risk. The objective is to secure the assets and reputation of RCPI and to ensure continued financial and institutional well-being. Effective Risk Management is about identifying what might go wrong, what the consequences might be and deciding what can be done to reduce the possibility of something going wrong. If it does go wrong, as some things inevitably will, the impact must be kept to a minimum. Risk Management supports better decision making through a good understanding of risks and their likely impact and ensuring that the learning from any risk situation is incorporated to prevent similar occurrences in the future.

Risk Appetite:

Risk Appetite is the amount and type of risk that an organisation is willing to pursue or retain.

Corporate Governance:

Governance is the system by which the College fulfils its purpose and achieves the intended outcomes for its Members, Trainees and Staff and operates in an effective, efficient, economic and ethical manner. It comprises a framework of rules and practices by which the Executive Board ensures accountability, fairness and transparency in an organisation's relationship with its stakeholders. Good governance leads to:

- Good management
- Good performance
- Good stewardship of funds
- Good public engagement and, ultimately good outcomes.

Horizon Scanning:

Horizon scanning is defined as a systematic examination of information to identify potential threats, risks, emerging issues and opportunities.

Internal Control:

A term to describe the totality of the way the RCPI designs, implements, tests and modifies controls in specific systems, to provide assurance to the corporate level that it is operating efficiently and effectively. Systems of internal control focus on and encompass the policies, procedures, processes, tasks and behaviours within the RCPI. Control activities are designed to ensure that the activities of RCPI operate in an orderly and efficient manner, comply with management and statutory requirements, assets are safeguarded and the corporate records are completeness and accurate. Ultimately, the control environment helps to identify and correct issues when something has gone wrong.

Control-environment:

The control environment comprises the systems of governance, risk management and internal controls. The key elements of the control environment include:

- Clarity of RCPI's strategic operational objectives and monitoring of their achievement
- Documented policies and procedures
- Laws and regulations
- Financial management of RCPI its reporting to ensure the economic, effective and efficient use of resources as well as fully Informed decision making
- The culture of RCPI including effective leadership of the risk management process, training staff and equipping them to manage risk in a way appropriate to their authority and duties.
- Performance monitoring to ensure risk management in RCPI is exercised with regard to a combination of economy, efficiency and effectiveness

Performance Monitoring:

Performance monitoring of risk management activity will ensure that the treatment of risk remains effective and the benefits of implementing risk control measures outweigh the costs of doing so. Performance monitoring is a

continual review not only of the whole process, but also of individual risks or projects and of the benefits gained from implementing risk control measures. Effective performance monitoring is dependent on Data Quality

Data Quality:

The RCPI needs to ensure that the data we use for performance monitoring and to inform decision making is accurate, reliable and fit for purpose. If the information is misleading, decision making may be flawed, resources may be wasted, poor services may not be improved upon and policy may be ill-founded. Any of these could represent significant risks to the RCPI. There is also a danger that good performance may not be recognised and rewarded.

Emergency Planning and Business Continuity:

An Emergency Planning and Business Continuity process is essentially risk management applied to the whole organisation and its ability to continue with its service provision in the event of a catastrophic event