

Risk Management Policy (RC-Pol-022)

Document Title	Risk Management Policy
Document Number	RC-Pol-022
Version	3.0
Department	Executive Office
Owner/Responsible for Implementation	Manager, Compliance and Risk
Approving Body	Executive Board
Effective date:	April 2024
Next Review date:	April 2027
Related Documents	<p>QA-Pol-023 – Quality Assurance and Enhancement Policy</p> <p>ED-SOP-098 – Programming Monitoring and Review Procedure</p> <p>Gov-TOR-004 – Finance, Audit and Risk Committee TOR</p>

Contents

1. Risk Management Policy	3
1.1 Policy Statement.....	3
1.2 Purpose	3
1.3 Objectives.....	3
1.4 Scope.....	4
1.5 Responsibilities.....	5
2. Risk Management Framework, Process and Guidelines	6
2.1 Risk Management Framework	6
2.2 Risk Management Process	7
2.3 Identify Risks	8
2.4 Describe Risks.....	8
2.5 Determine Risk Category	9
2.6 Determine Inherent Risk Rating	9
2.6.1 <i>Estimate Likelihood of Occurrence</i>	9
2.6.2 <i>Estimate the Potential Impact</i>	10
2.6.3 <i>Calculate Total Risk</i>	11
2.6.4 <i>Risk Target</i>	12
2.7 Risk Treatment	12
2.7.1 <i>Risk Controls</i>	13
2.7.2 <i>Risk Mitigation Actions</i>	13
2.8 Monitoring & Review of Risks, Controls and Actions	14
2.8.1 <i>Maintenance of Corporate Risk Register</i>	14
2.8.2 <i>Annual Review</i>	14
3. Glossary and Definitions	15
Appendix 1 – RCPI Risk Appetite / Tolerance	17

1. Risk Management Policy

1.1 Policy Statement

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

It is the policy of RCPI to ensure that threats and opportunities are managed in a systematic and transparent manner, thereby supporting RCPI in the fulfilment of its obligations and the delivery of its strategic and operational objectives.

RCPI's Risk Management Framework, which is aligned with the ISO 31000:2018 Risk Management Guidelines, incorporates best practice in the identification, evaluation and control of risks and reflects RCPI's commitment to:

- adopting a proactive approach to the management of risk
- implementing the necessary structures and processes for the identification and control of risks
- providing the required supports to embed risk management as part of normal day-to-day business.

1.2 Purpose

The purpose of this policy is to:

- Outline the objectives of RCPI's risk management practice
- Set out the structures and processes for the proactive management of risk
- Assist staff in understanding their role in the proactive management of risk

1.3 Objectives

The objectives of RCPI's risk management practices are to:

- Proactively identify risks
- Mitigate and reduce the likelihood and/impact of risks
- Anticipate and respond to changes within RCPI's field
- Facilitate oversight of risk for RCPI's FinARC and Executive Board

These objectives will be achieved by:

- Maintaining a register of risks linked to the RCPI's business, strategic and operational objectives.
- Implementing a proactive approach to the identification of risks and integrating risk consideration with decision making structures and processes.
- Tracking the implementation of risk mitigation and auditing/ monitoring risk controls.
- Periodic review of the effectiveness of RCPI's Risk Control Framework
- Clearly defining the roles, responsibilities and reporting lines within the RCPI for Risk Management.
- Training staff on the principles of risk management and its application in RCPI
- Reinforcing the importance of effective risk management as part of the everyday work and 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?

1.4 Scope

This policy applies to all staff, managers and Heads of Function when participating in the structured risk management process and, also, in the general course of their work in RCPI.

1.5 Responsibilities

The Manager, Compliance and Risk 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.

All staff must complete all Risk Management Training as provided. Staff must engage with the structured risk management process in the interest of enhancing their understanding of risk management and their role in identifying and escalating risks.

Managers are responsible for maintaining a Departmental Risk Register for their area and for ensuring all risk related actions are prioritised and completed.

Heads of Function are responsible for ensuring that their managers have sufficient capacity to allow the work required for effective risk management to be carried out.

Heads of Function are responsible for identifying risks for inclusion in the Corporate Risk Register i.e. risks to related to RCPI's achievement of its objectives, fulfilment of its obligations or risks emerging in RCPI's external environment.

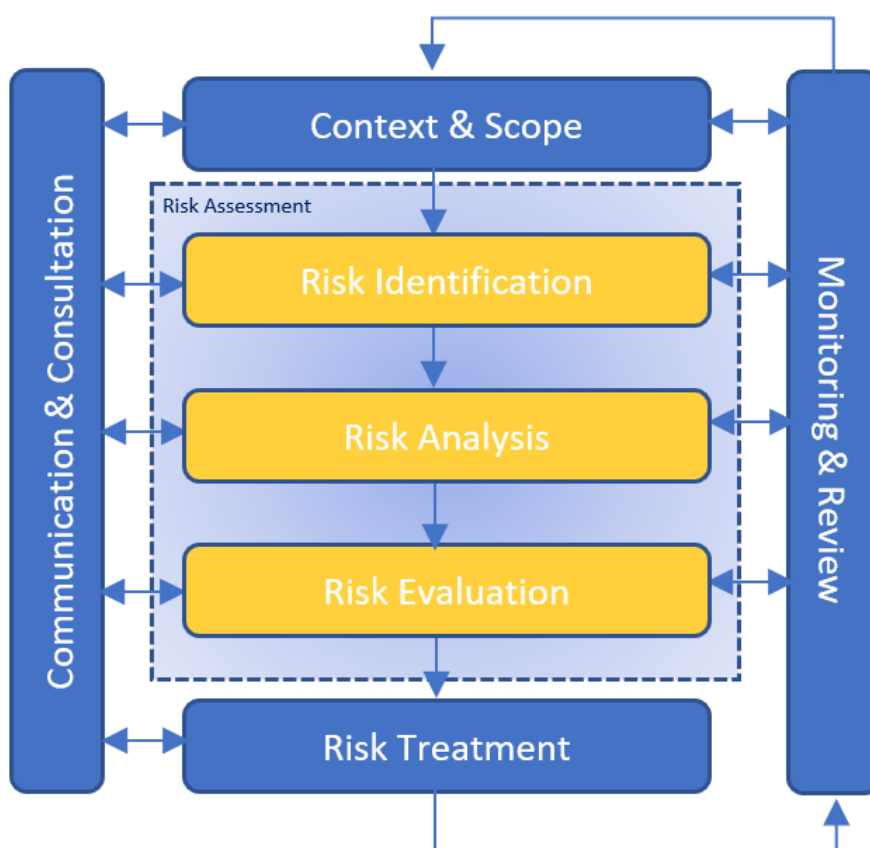
The CEO is responsible for overseeing the effectiveness of the Risk Management Framework and supporting the implementation of this policy.

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.

The Executive Board must regularly include The Corporate Risk Register on its agenda with a view to providing input on particular risks or RCPI's risk landscape.

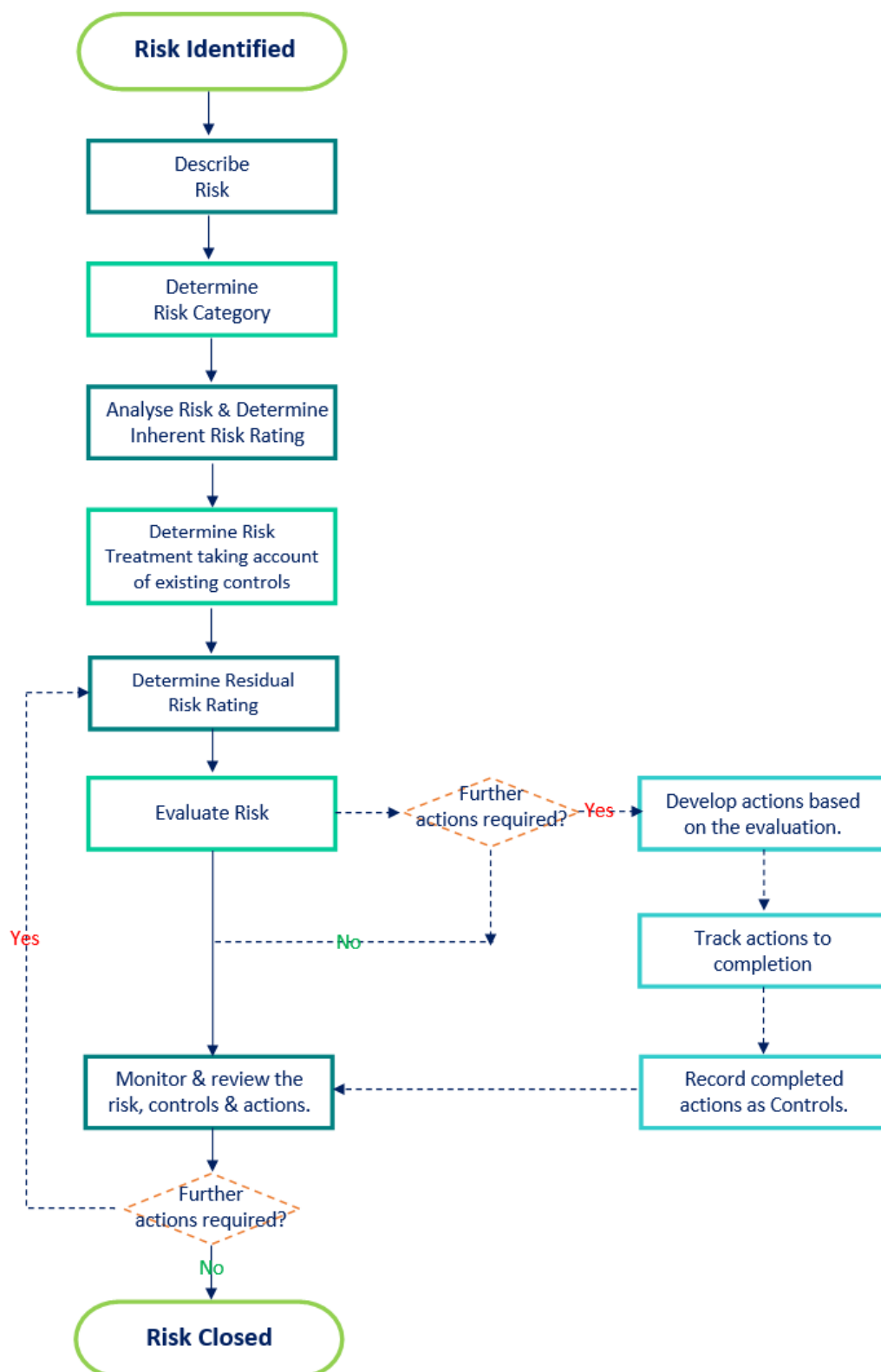
2. Risk Management Framework, Process and Guidelines

2.1 Risk Management Framework



Adapted from ISO 31000:2018 Risk Management Guidelines

2.2 Risk Management Process



2.3 Identify Risks

The identification of risk in RCPI is facilitated by the following structures:

- Departmental/Team Meetings
- Senior Management Team Meetings
- Relevant Committees and Board Meetings
- Integration of Risk Management with project processes and Change Control structures.
- Integration of Risk Management with the Business Planning Process
- Internal Audit/ Departmental Assessment
- Risk assessments such as DPIAs, Health and Safety Assessments etc
- Maintenance of the RCPI Risk Universe and escalation of items within the Risk Universe for active monitoring

2.4 Describe Risks

When documenting a risk it is important that the description is a structured statement. A structured statement is beneficial because it:

- Enables accurate assessment and analysis of the risk and current controls.
- Ensures that relevant and effective actions are identified for the mitigation of the risk.
- Makes it easier for senior managers and clinicians, who are not familiar with the all operational details, to understand the concern.

In accordance with best practise, a structured risk statement has three components:

- 1. Risk Event** a specific tangible event that could prevent an objective being achieved
e.g. cyber-attack
- 2. Causes of the Risk** weaknesses in current controls/systems, external factors, changes in status quo
- 3. Impact** potential consequences/outcomes of the Risk Event materialising

Risk Statement Examples	Risk Statement = Risk Event + Causes + Impact
	There is the risk of a cyber-attack due to poor access controls resulting in potential breach of data
	There is a risk of acquiring an infection associated with receiving healthcare due to poor infection prevention and control practices resulting in harm to patients, service users or staff

2.5 Determine Risk Category

Once described, the Risk must be assigned a Risk Impact Category. Only one Category should be chosen as the primary category, even though a risk may impact many of the categories (secondary impacts).

The correct categorisation of a risk helps with the identification of all potential causes, all likely consequences and, in turn, the appropriate risk responses.

Putting risks in categories also provides an overview of RCPI's risk landscape and helps to determine where the greatest concentration of threats lie and to analyse common risk causes.

For these purposes, RCPI has identified the following risk categories:

- Training / Exams Standards
- Trainee / Trainer Experience
- Member Engagement
- Stakeholder Relationship (IMC, HSE, QQI)
- Business Partnership
- Strategic Objectives
- Financial Stability / Growth
- Operational
- Compliance
- Cyber Security
- Infrastructure / Property
- Safety
- Reputation

2.6 Determine Inherent Risk Rating

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.

2.6.1 Estimate Likelihood of Occurrence

Using the five-point scale below, assess the **likelihood of each risk**. The risks should be assessed, in the first instance, without taking account of 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

2.6.2 Estimate 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 to guide discussion:

Rating \ Category	Sub-minor	Minor	Moderate	Major	Severe
Category	1	2	3	4	5
Training/Exams Standards	Room for procedural /practice improvement	Sub-optimal in delivery, but requirements met	Remedial action required, but manageable	Some requirements at risk of not being met	Reputation of RCPI Programmes/Exams adversely affected
Trainee/Trainer/ Member Engagement	Room for procedural /practice improvement	Unsatisfactory experience but resolvable at staff/ departmental level	Unsatisfactory experience that requires system/practice review and improvement	Unacceptable challenges/ consequences for individuals resulting from RCPI's weaknesses	Loss of trainee/ member confidence
Critical Stakeholder Relationship (HSE, IMC, QQI)	Room for procedural /practice improvement	Could be a concern for stakeholder(s)	Reporting/ Explanation to stakeholder(s) required	Reputation adversely impacted with some stakeholder(s)	Sanctions/ Restrictions imposed
Business Partnership	Settling in / teething issues	Refinement of engagement processes and standards required	Unsatisfactory service level fulfilment by business partner	Challenges in business partnership requiring resolution before continuing with planned business	Significant breakdown in business partnerships with significant impact on RCPIs fulfilment of strategic objective/ operational obligation.
Strategic Objectives	Small challenge in achieving an objective	Minor compromise on achievement of strategic objective but no overall impact on scope, quality, or timeframe	Material compromise on achievement of strategic objective with temporary impact on scope, quality, or timeframe	Revision/reduction in scope, quality, or timeframe of strategic objective	Failure to fulfil strategic objective
Financial Stability/Growth	< 0.5% of Annual Income	< 1% of Annual Income	< 5% of Annual Income	5 - 10% of Annual Income	> 10% of Annual Income
Operational	Disruption to service for less than 1 day.	Disruption to service for 1 full day.	Disruption to service for between 2 and 7 days.	Disruption to service for more than 7 days.	Disruption to service for more than 14 days.
Compliance	Room for procedural /practice improvement	Non-compliance with internal policies.	Material non-compliance with internal policies.	Partial failure to meet compliance obligations.	Gross failure to meet compliance obligations.

Cont.

Rating Category	Sub-minor	Minor	Moderate	Major	Severe
	1	2	3	4	5
Cyber Security	No risk of compromise Room for procedural / practice improvement	Low risk of security controls being compromised	Moderate risk of security controls being compromised with measurable negative impacts	Elevated risk of security controls being compromised with significant measurable negative impacts	High risk of security controls being compromised with potential for catastrophic negative impacts
Infrastructure /Property	Disruption to use of property/equipment/artifacts that requires little or no remedial action.	Inconsequential damage to property/equipment/artifacts	Recoverable, damage to property/equipment/artifacts	Recoverable, but costly, damage to property/equipment/artifacts	Permanent damage to loss of property/equipment/artifacts
Safety	No harm. No need for treatment.	Discomfort / Bruising type injury	First aid treatment could be required. Very short recovery period.	Hospital treatment could be required. Medium to prolonged recovery period.	Serious Injury / Death.
Reputation	Individual grievances Issue resolved promptly by operational management processes	Reputation is adversely impacted with a small number of affected people Mainly an internal matter	Reputation is adversely impacted with many affected people or partners/collaborators/peer organisations	Reputation adversely impacted with a key stakeholder(s)	Reputation and standing of RCPI adversely affected nationally /internationally

2.6.3 Calculate 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				

2.6.4 Risk Target

Having calculated the Total Inherent Risk, an acceptable risk target should be agreed taking account of RCPI's Risk Appetite Statement. The Target Risk should be documented as shown below to allow progress to be monitored:

Risk	RCPI's Current Exposure to the Risk					Risk Exposure Since Last Report
Risk 1	8		12		16	↓
Risk 2			12	15	15	→
Risk 3	6	10	12			↑

-  Inherent Risk
-  Residual
-  Target

2.7 Risk Treatment

Taking account of the likelihood and impact of a risk, and with reference to the RCPI's Risk Appetite / Tolerance an appropriate risk treatment approach must be selected. Typically, treatment options are as follows:

- Terminate** A decision is made not to proceed with the planned activity.
- Transfer** Risk exposure is to be limited by insurance, outsourcing etc. Such a treatment plan requires close monitoring will be required as it may not be possible to transfer all aspects of the risk.
- Tolerate** In some cases, on analysis of existing information, a level of risk may be tolerated in the interest of pursuing an opportunity
- Treat** The most common approach is to introduce preventative actions to reduce the probability or impact if the risk occurs. Treating a risk entails:
- Reviewing, improving or developing **Risk Controls** such as training, oversight, technical restrictions etc.
 - Implementing **Risk Mitigation Actions** such as diversification, deploying additional resources etc

2.7.1 Risk Controls

A risk control is a measure which has been implemented to reduce the likelihood or impact of a risk. If a Risk Control has not been fully implemented, it is a Risk Mitigation Action.

There are four different type of controls which may be implemented individually or in combination to reduce the likelihood or impact of a risk. In order of preference, they are:

Pro-active Control	Preventative Controls	Aim to restrict the possibility of an undesirable event e.g. Passwords / MFA Physical Security Measures Formal Approval Processes
	Directive Controls	Aim to give direction on practice and standards e.g. Policies Procedures Training
Reactive Control	Detective Controls	Aim to proactively identify risks e.g. Audit Monitoring / performance reports Incident reviews
	Corrective Control	Aim to minimise undesirable consequences after a risk event occurs e.g. Data Breach Procedures Disaster Recovery Plans Fire sprinklers

2.7.2 Risk Mitigation Actions

A valid Risk Mitigation Action must fulfil the following criteria:

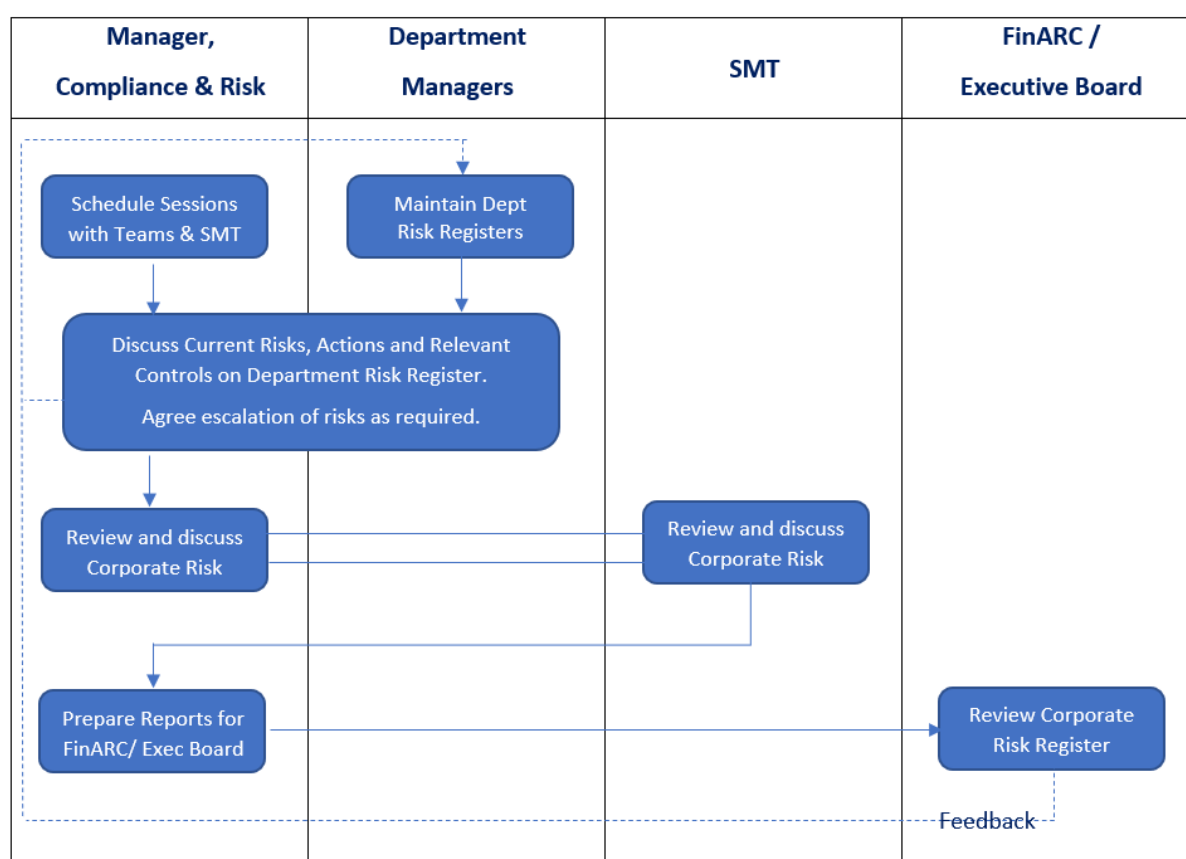
- Its implementation will have a direct impact on the likelihood or the impact of the risk.
- It has an assigned owner, where there are multiple subtasks, one person is identified as lead responsible.
- Due dates are within a reasonable timeframe balancing current workloads with the seriousness of the risk.
- On completion of the action, the risk will be reassessed to determine if further actions are required
- Where appropriate, the action will be formalised as an ongoing Risk Control.

2.8 Monitoring & Review of Risks, Controls and Actions

Risk Management is a continuous and dynamic process because new risks emerge, existing risks may change, the impact or likelihood of risks should change following the implementation of effective controls and some risks will be eliminated. It is essential that Risk Registers are routinely monitored to fully understand our risk landscape and to assess the effectiveness of our risk management process.

2.8.1 Maintenance of Corporate Risk Register

The Corporate Risk Register is maintained on a continual basis, through the process illustrated below:



2.8.2 Annual Review

An annual review of the Risk Register is carried out by the Senior Management Team to assess the effectiveness of the RCPI Risk Management Framework with reference to the identification of risks, implementation of risk mitigation and control plans and the effectiveness of risk controls. The Annual Review also includes an appraisal of the Risk Appetite/Tolerance Statement. On completion of the review an Annual Risk Review Report is submitted to FinARC.

3. Glossary and Definitions

Action	An action is a future measure to further reduce either the likelihood or impact of a risk.
Controls	A control is a measure that is in place, is working effectively and operating to reduce either the likelihood or impact of a risk.
Detective Controls	Detective controls are designed to proactively identify potential risks so that corrective actions can be taken before an event occurs.
Directive Controls	Directive controls give direction i.e. policies, procedures, work instructions and training.
Impact	The outcome or consequence(s) of a risk event.
Inherent Risk	Inherent risk is the level of risk before consideration of control and/or action measures
Issue	A relevant event that has happened was not planned and requires management action.
Likelihood	The chance of something happening (also described as the probability or frequency of an event occurring).
Preventative Controls	Preventative controls are controls designed to stop, discourage, pre-empt or limit the possibility of an undesirable event before it occurs.
Residual Risk	Residual risk is the level of risk remaining after consideration of existing controls

Risk	Risk is the effect of uncertainty on objectives. It is any condition, circumstance, event or threat which may impact the achievement of objectives and/or have a significant impact on the day-to-day operations. This includes failing to maximise an opportunity
Risk Appetite Statement	A Risk Appetite Statement is a broad overarching statement of the level of risk an organisation is willing to pursue or retain.
Risk Assessment	The overall process of risk identification, risk analysis, and risk evaluation.
Risk Categories	Risk criteria relate to the identification of risk as either strategic or operational and to further categorise a risk based on the area upon which it impacts.
Risk Description	A structured statement of risk usually containing three elements: risk event, cause and impact.
Risk Management	Risk management is the planned and systematic approach to the identification, evaluation and control of risk. 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.
Risk Universe	Consists of every risk that could affect your organisation, on every level. Anything that could harm an organisation's ability to function.

Appendix 1 – RCPI Risk Appetite / Tolerance

Risk Appetite / Tolerance												
Risk Category	None			Limited Tolerance			Balanced Appetite			High		
Training / Exams Standards												
Trainee Experience												
Trainer Experience												
Member Engagement												
Stakeholder Relationships												
Partnerships												
Strategic Objectives												
Financial Stability / Growth												
Operational												
Compliance												
Cyber Security												
Infrastructure / Property												
Safety												
Reputational												

Risk Appetite / Tolerance Guidance	
None	Avoidance of risk is core objective. Very low tolerance for uncertainty. When faced with multiple options, lowest risk option is always sought.
Limited Tolerance	Benefits must heavily outweigh risk. Risk manageable by the robust controls. Low tolerance for uncertainty. When faced with multiple options, preference for lowest risk option
Balanced Appetite	Moderate levels of risk may be acceptable. Willing to accept uncertainty under certain conditions. When face with multiple options, risk impact of chosen option must be manageable.
High	Will take justified risks. A degree of uncertainty is fully anticipated. When faced with multiple options, willing to choose the option with highest return, accepting some possibility of failure.