Risk Management Policy

Contents

1. Introduction

1.1 The ICMT, like any business, has its own set of inherent risks. These risks can interfere with the ICMT's ability to achieve its strategic and operational goals. As a result of its commitment to risk management, the ICMT will make better-informed decisions and increase the probability of achieving its strategic and operational goals.

2. Governance

2.1 The ICMT is responsible for fulfilling its role in governance by demonstrating appropriate financial controls.

2.2 This includes demonstrating the organisation's commitment to fostering a healthy risk culture aligned with the ICMT's strategic objectives. Developing such a culture requires integrating risk management in day-to-day decision-making processes linked to the governance and management of the organisation through its structures, roles, and responsibilities.

This means:

- The ICMT should follow a continuous process that links identifying and managing risk to achieving its strategic and operational goals.
- Internal control should be a risk-based and event-based approach, assessing risks for their likelihood and impact.
- All risk areas must be considered in the review procedure, not just financial risk.
- Operational procedures should incorporate risk assessment and internal control.
- A regular report on internal control and risk should be received by the Senior Management Team or relevant committee throughout the year.
- A systematic approach to identifying, evaluating, managing, and monitoring risk should be adopted by the organisation as a whole. The Senior Management Team should be informed about the effectiveness of the risk management system and be asked to review it.
- Where appropriate, the Senior Management Team is expected to provide details regarding actions taken or proposed to address significant internal control issues.

3. Purpose

3.1 The purpose of this policy is to acknowledge the ICMT's commitment to risk management. This policy does not aim to eliminate all risks from the ICMT activities but rather to ensure that the ICMT makes every effort to manage risks to maximise opportunities and minimise adverse effects.

3.2 The ICMT has developed this policy to ensure that all levels of the organisation have a consistent means of identifying, assessing, monitoring, managing, controlling, and reporting risks.

4. Objectives

4.1 Assist the ICMT in attaining its strategic and operational goals and objectives by confirming and communicating its commitment to risk management.

4.2 Establish a reporting protocol for all the ICMT activities to formalise and communicate a consistent approach to managing risk.

4.3 To make sure that all significant risks to the ICMT are identified, assessed and treated where necessary, as well as reported to the ICMT's Senior Management Team promptly through the ICMT's Operations Committee.

4.4 To assign accountability to relevant committees and staff to manage risks within their areas of control.

4.5 Provide assurances to staff and students that risk management is an integral part of the management process.

5. Statement

The ICMT has employed Judicium Education to support in ensuring a safe working and learning environment and comply with legal requirements.

The ICMT views risk management as a fundamental principle of good management practice and an essential aspect of corporate governance. A robust risk management system will play an essential role in helping the ICMT achieve its strategic and operational goals.

Management of risk should be an integral part of the ICMT's decision-making process and routine management procedures and be reflected in all aspects of planning processes at all levels across the organisation.

Risk assessments must be carried out on new ventures and activities, including projects, processes, systems and commercial activities, to ensure that these are aligned with the ICMT's objectives and goals. Any risks or opportunities arising from these assessments will be identified, analysed and reported to the appropriate management level.

A risk register will be maintained by the ICMT that categorises risk, and the ICMT's Senior Management Team will monitor risk.

The ICMT is committed to ensuring that all employees receive adequate guidance and training regarding risk management principles and their responsibilities to implement risk management efficiently.

As part of the ICMT's risk management process, the ICMT will periodically review and track its implementation and effectiveness and develop and embed an appropriate risk management culture throughout the organisation.

6. What is Risk?

6.1 There is risk in all activities because of uncertainty, regardless of their size or complexity, industry or business sector. We must recognise that risk encompasses a much broader concept than the traditional concept of merely a threat. We must also be aware of the risks involved in taking advantage of opportunities.

6.2 The ICMT considers all types of risk, including strategic, corporate, operational, financial, reputational, regulatory and compliance.

6.3 Levels of risk can be defined as:

- Strategic: Risks that may affect the delivery of the strategic objectives or the strategy itself.
- Corporate: Risks that could impact the organisation's effectiveness but are not directly related to the strategic objectives.
- Operational: Risks relating to the efficiency of the ICMT's systems (people, processes, IT systems, infrastructure) which, if left unaddressed, can negatively impact the achievement of the organisation's strategic objectives.

7. Types and Categories of Risk

7.1 As a guide, a starting point or as a checklist for existing registers, these can be used in assessing the level of risk that will be tolerated for each threat.

7.2 Strategic Risk – Major Threats

Sources of threat that may give rise to significant strategic risk include:

- Budgeting (relates to availability or allocation of resources).
- Fraud or Theft.
- Unethical dealings.
- Product and or services failure (resulting in lack of support to business process).
- Public perception and reputation.
- Exploitation of workers and or suppliers (availability and retention of suitable staff).
- Environmental (mismanagement issues relating to fuel consumption, pollution etc.).
- Occupational health and safety mismanagement and or liability.
- Failure to comply with legal and regulatory obligations and or contractual aspects.
- Civil Action.
- Failure of the infrastructure (including utility supplies, computer networks etc.).
- Failure to address economic factors (such as interest rates, and inflation).
- Political and market factors (for management of risk, security etc.).
- Operational processes and procedures – adequate and appropriate.
- Capability to innovate (to exploit opportunities).
- Failure to control intellectual property (as a result of abuse or industrial espionage).
- Failure to take account of widespread disease or illness among the workforce.

- Failure to complete published deadlines or timescales.
- Failure to take on new technology where appropriate to achieve objectives.
- Failure to invest appropriately.
- Failure to control IT effectively.
- Failure to establish a positive culture following business change.
- Vulnerability of resources (material and people).
- Failure to establish effective continuity arrangements in the event of a disaster.
- Inadequate insurance/contingency provision for disasters such as fire, floods and bomb incidents.

7.3 Strategic/Commercial Risks

Examples of commercial risks include:

- Underperformance of service relative to specification.
- Management will underperform against expectations.
- Collapse of contractors.
- Insolvency of promoter
- Failure of suppliers to meet contractual commitments (this could be in terms of quality, quantity, and timescales on their risk exposures).
- Insufficient capital investment, a shortfall in revenue expected/planned.
- Fraud/Theft.
- Partnerships are failing to deliver desired outcomes or outputs.
- An event being non-insurable or the cost of insurance outweighs the benefit.

7.4 Economical/Financial/Market

- Exchange rate fluctuation.
- Interest rate instability.
- Inflation.
- Shortage of working capital.
- Failure to meet project revenue targets.
- Market developments will adversely affect plans.

7.5 Legal and Regulatory

- New or changed legislation may invalidate assumptions upon which the activity is based.
- Failure to register with any new regulatory body, such as OfS.

- Failure to obtain appropriate approval (e.g. planning consent).
- Unforeseen inclusion or contingent liabilities.
- Loss of intellectual property rights.
- Failure to achieve satisfactory contractual arrangements.
- Unexpected regulatory controls of licensing requirements.
- Changes in the tax structure.

7.6 Organisation/Management/Human Factors

- Management incompetence.
- Inadequate corporate policies.
- Inadequate adoption of management practices.
- Poor leadership.
- Key personnel have inadequate authority to fulfil roles.
- Poor staff selection procedures.
- Lack of clarity over roles and responsibilities.
- Vested interest creating conflict and compromising the overall aims.
- Individual or group interests are given unwarranted priority.
- Personality clashes.
- Indecisions or inaccurate information.
- Health and safety constraints.

7.7 Political

- Change of government policy.
- Change of government.
- War and disorder.
- Adverse public opinion/media intervention.

7.8 Environmental

- Natural disasters.
- Storms, flooding.
- Pollution incidents.
- Transport problems.

7.9 Technical/Operational/Infrastructure

- Inadequate design.
- Professional negligence.
- Human error/incompetence.
- Infrastructure failure.
- Operation lifetime lower than expected.
- Increased dismantling/decommissioning costs.
- Safety being compromised.
- Performance failure.
- Residual maintenance problems.
- Unclear expectations.
- Breaches in statutory/information security.
- Lack or inadequacy of business continuity.

7.10 Operational

- Lack of clarity of service requirements.
- Inadequate infrastructure to provide required operational services.
- Inadequate or inappropriate people are available to support the required service provision.
- Inappropriate contract in place and or inadequate contract management to support the required level of service provision.
- Changing requirements enabled in an uncontrolled way.
- Products passed to operational teams without due consideration to implementation, handover, subsequent maintenance and decommissioning.
- Unexpected or inappropriate expectations of service users.
- Inadequate incident handling.
- Lack or inadequacy of business continuity or contingency measures with regard to maintaining critical business services.
- Failing to meet legal or contractual obligations.

8. Approach

8.1 The ICMT's approach to risk management follows several fundamental principles:

- Make the Risk Management process as user-friendly as possible.
- Seek to embed risk management across all aspects of the organisation.

- Develop a comprehensive picture of risk across all the ICMT activities.
- Ensure consistency and transparency in risk management, using everyday language and a methodology that is widely understood.
- Control improvements are a crucial part of the risk management process; however, balancing the cost and effectiveness of controls is important. For instance, if marginal improvements in controls require substantial costs, the proposal may not be feasible.
- Risk escalation ensures that major risks are reported and closely monitored regularly at an appropriate level.

9. Roles and Responsibilities

9.1 Senior Management Team

The Senior Management Team is responsible for managing the total risk exposure of the ICMT and approves the annual risk tolerance line.

The Senior Management Team has responsibility for the total risk exposure of the ICMT by:

- Establishing a culture of risk management within the ICMT by setting the tone and influencing its implementation.
- Assessing to what degree whether the ICMT is risk-taking or risk-averse
- Approving of significant decisions affecting the ICMT's risk profile or exposure.
- Establishing the types of risk that are acceptable and non-acceptable, monitoring significant risks, and enhancing control measures to mitigate risk.
- Reviewing and approving changes or improvements to the ICMT's methods of risk management every year.
- Identifying and evaluating the significant risks faced by the ICMT.
- Implementing policies on risk management and internal control.

9.2 Staff and Students

Staff and students must be committed to and cooperative in order for risk management to be effective. Every employee plays an important role in managing risk, particularly within their areas of responsibility. Therefore, all employees are responsible for adhering to the principles outlined in this policy and are accountable for doing so.

9.3 Operations Committee

The Operations Committee is responsible for coordinating the risk management program and providing advice and guidance, including developing standard templates and tools that can assist the ICMT in the management of risk.

The Operations Committee will formulate and conduct training based on the principles of risk management, risk identification and assessment, and how to implement risk management effectively.

A risk assessment for new ventures or activities will be conducted by the Operations Committee where necessary.

The Operations Committee is responsible for maintaining the ICMT's risk register.

10. Process

10.1 Five steps are involved in the management of risks identified in the risk register:

i. Ownership and identification: Identify the risks in achieving strategic and operational objectives and identify who is responsible for managing them.
ii. Analyse: What is the actual risk, and how likely and how severe is it?
iii. Rank: Based on the risk assessment and calculation model, what is the score (gross and expected net risk after treatment)?
iv. Treat: Determining the course of action and how we will handle the risk. Next, the level of risk will be assessed, including expected risk tolerance, along with the controls in place or those that must be put in place.
v. Monitor and review: What will be done to monitor and review risk.

Note: The five steps apply to all new ventures and activities, including projects, processes, systems and commercial activities.

10.2 Identification and ownership

Risk can be identified anywhere and by anyone, using several mechanisms and timescales. Through their shared knowledge of the sector and their understanding of operational issues, the Senior Management Team and Operations Committee will identify new risks and threats

internally and externally. Additionally, they will regularly examine the correlations between strategic objectives and risks to ensure that priority activities remain focused.

Ownership will be assigned at the point the risk is identified.

10.3 Analyse

Prior to being included on the register, the risk must be appropriately articulated through risk assessment. Managing risk requires that reviewers fully understand the actual risk posed by the organisation. Furthermore, this ensures appropriate risk scores and mitigating actions are associated with the risk.

A probability and impact score can be calculated once the risk is thoroughly understood. The outcome will be an overall gross risk score before any treatment is adopted. The Senior Management Team should be alerted to risks rated at the highest level or that have significant likelihood and impact as soon as possible.

10.4 Treating

After assessing and understanding risk, owners can determine the actions required to reduce risk using five principles: avoidance, reduction, transfer, acceptance, and sharing. There may be a price to pay for the avoidance of risk (financial or otherwise), but at this point, it is important to consider this option.

Depending on the situation, treatment and actions may take the form of business as usual activities or specific initiatives that will increase the probability of achieving the strategic objectives.

In order to ensure accurate cost estimation and benefit consideration, risk owners should clarify which actions are business as usual (no additional cost) and which actions are new.

11. Review

11.1 There should be a formal risk review at least twice a year with progress on control improvements for red risks being reviewed approximately every four to six weeks.

11.2 During the risk review, each risk should be considered to determine if it is still relevant and applicable and whether the risk register has been completed (new risks are to be considered at this point). During their regular meetings, it is a good practice for the Senior Management Team to note emerging risks.

11.3 The number of risks under active management should be kept to a manageable number. Risks that are considered very low (1 probability and 1 impact) can be removed from the risk register.

11.4 The following questions should be considered in a risk review:

i. Is the risk still relevant?
ii. Is the risk owner still appropriate?
iii. Has the risk reduced to an extent where de-escalation and delegation of the risk management can be completed and the risk removed from the register?
iv. Has the risk increased to an extent where escalation needs to occur, and reassessment of the risk needs to occur?
v. What are the circumstances around the changes to risk levels, what is the explanation and evidence?
vi. What opportunities do the changes present?

Document control

Document Title	Risk Management Policy
Document Category	General Policies
Version	1
Status	Approved
Author	Operations
Date of current version	October 2021
Date of next review	October 2022
Document location	ICMT website
Communication plan	Available on the ICMT website