

RISK MANAGEMENT POLICY

Owner: Tony Harris

Approved by Board: 19 January 2022

Version 1.1

PURPOSE OF RISK MANAGEMENT

1. The Board of Directors of CoMA exercise responsibility and guardianship over the use of the organisation's resources and ensure that said resources are managed, controlled and used appropriately in the pursuit of the organisation's legitimate objectives.
2. This Risk Management Policy (the Policy) is promoted by the Board of Directors to contribute to the fulfilment of these objectives as part of the internal control and governance arrangements of the organisation.
3. Risk Management is a process that demonstrates that CoMA is acting appropriately in order to avoid excessive risk, and that CoMA's response to risk – whether by insurance, active control measures or avoidance of risk – is proportionate and effective.
4. The purpose of Risk Management is:
 - 4.1. to assist staff and the Board of Directors in planning and decision-making by identifying potential barriers, costs and rewards;
 - 4.2. to allow CoMA to anticipate and adapt to changing circumstances; and
 - 4.3. to identify areas of concern (or opportunity) where action is needed.
5. In general, all Risk Management activity should:
 - 5.1. be in proportion to the scale of risk under consideration;
 - 5.2. drive actions and changes in policy or practice; and
 - 5.3. provide information and reassurance to all stakeholders on current risks.

RESPONSIBILITIES FOR RISK MANAGEMENT

6. The Board of Directors has responsibility for overseeing Risk Management for CoMA and is ultimately accountable for it. It shall exercise its responsibility through an annual review of risk to provide assurance that CoMA is acting appropriately to identify risks and taking action to mitigate or eliminate them.
7. Staff members shall also have particular responsibilities for Risk Management in their designated areas of responsibility.

RISK REGISTER

8. The Board of Directors will oversee through delegation to relevant staff the preparation of a Risk Register, to be reviewed annually.
9. The Register will identify all risks and implications, and set out the detail of the CoMA's plans for the early identification, intervention and mitigation of the risks.

ASSESSMENT OF RISK

10. The Register requires an assessment of the level of risk, allowing the Board of Directors and staff to prioritise action and resources in the most critical areas.
11. Risk is assessed in terms of (a) likelihood and (b) impact. A multiplier of the two provides CoMA with a 'risk rating' for each identified risk. See appendix 1 for guidance on assessing risk.

APPENDIX 1: GUIDANCE ON THE ASSESSMENT OF RISK

A: ASSESSMENT OF LIKELIHOOD OF RISK

Likelihood can be considered in relation to: (i) Probability; and (ii) Frequency.

Frequency and probability definitions

Score	Chance	Frequency
1	May occur only in exceptional circumstances	Has occurred or can reasonably be considered to occur only a few times in 100 years.
2	Could occur at some time	Has occurred 2 or 3 times over 10 years in this organization or similar organizations
3	Might occur at some time	Has occurred in this organization more than 3 times in the past 10 years or occurs regularly in similar organizations or is considered to have a reasonable likelihood of occurring in
4	Will probably occur in most circumstances	Occurred more than 7 times over 10 years in this organization or in other similar organizations or circumstances have such that it is likely to happen in the next few years
5	Is expected to occur in most circumstances	Has occurred 9 or 10 times in the past 10 years in this organization or circumstances are in train that will almost certainly cause it to happen

B: ASSESSMENT OF IMPACT OF RISK

Impact should be considered in relation to (i) financial, (ii) operational, and (iii) reputational.

Financial

Score	Description
1	1% of budget
2	2-5% of annual budget
3	5-10 % of annual budget
4	> 10% of budget
5	> 30% of project or organizational annual budget

Operational

Score	Description
1	Minor impact. Minimal impact on non-core operations. The impact can be dealt with by routine operations.
2	Some impact on organizational capability in terms of delays, systems quality but able to be dealt with at operational level
3	Impact on the organization resulting in reduced performance such that targets are not met. Organization's existence is not threatened, but could be subject to significant review.
4	Breakdown of key activities leading to reduction in performance (eg. service delays, revenue loss, client dissatisfaction, legislative breaches).
5	Protracted unavailability of critical skills/people. Critical failure(s) preventing core activities from being performed. Survival of the project/activity/organization is threatened.

Reputational

Score	Description
1	Insignificant – Very little significant (immaterial) impact on brand/reputation (nothing to worry about)
2	Fairly Serious – Little significant (limited) impact on brand/reputation (possibly important but can be managed although would take up some time and resources)
3	Serious - Some impact on brand reputation (it would cause us some reputational problems and would definitely take up time and resources)
4	Very Serious – Significant impact on brand/reputation (would damage the brand in the internal and external environment, would take considerable time and resource to deal with and would hinder achievement of strategic objectives)
5	Major Crisis – Very significant impact (major/severe) on brand/reputation (could seriously undermine the standing and position of the organisation and could lead to major loss of income)

C: CALCULATING A RISK RATING SCORE (RSS)

The multiplier of Likelihood and Impact provides CoMA with a Risk Rating Score (RSS) for each identified risk.

An overall RSS of 1-6 represents a **low level risk**

An overall RSS of 8-12 represent a **moderate level of risk**

An overall RSS of 15-25 represent a **high level of risk**

		Impact				
		1	2	3	4	5
Likelihood	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25