COLLEGE OF
CAPE TOWN
Inspiring minds

# QUALITY MANAGEMENT SYSTEM

## PL-001A-RSK

## Risk Management Policy

| | | |
|---|---|---|
| Document title:<br>**Risk Management Policy** | Formal document number | **PL-001A-RSK** |
| | Revision | **A** |
| Purpose of Document:<br>**Governance and oversight of identification, mitigation and management of risk in the College.** | Commencement date | **23 August 2018l** |
| | Scheduled review by | **Five years from commencement** |
| Approved by the College Council. Decision number 179, 23 August 2018 | | |

Book design by Andrew J. Winks

The template for this document was developed with support from **Deutsche Gesellschaft für Technische Zusammenarbeit (GTZ) GmbH :** Copyright © 2006 **GTZ.** Effective January 2011, GTZ has been incorporated into *Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH*.

# PL-001A-RSK
# RISK MANAGEMENT POLICY

CONTENTS

## 1. PURPOSE

Risk management has been adopted as a governance requirement in order to address all factors that may hinder or prevent the College of Cape Town from achieving any of its goals and objectives.

## 2. SCOPE

This document presents the policy and guidelines of the College for managing risk. The policy framework for the management of risks within the College considers:

2.1 Responsibility for promoting awareness of risk management;
2.2 Mechanisms for assessing the state of risk management;
2.3 Responsibility for improving risk exposures; and
2.4 Mechanisms for monitoring and reporting the state of risk management.

## 3. CET ACT AND THE PFMA

3.1 Section 25(1)(c) of the CET Act requires that internal audit and risk management shall be implemented to a standard not inferior to those of the PFMA.

3.1 The PFMA requires that the Accounting Authority (the College Council) has and maintains effective, efficient and transparent systems of financial and risk management and internal controls.

3.2 The Internal Audit Function is required to adopt a risk-based strategic planning approach that includes a process of linking risk analysis to audit planning, and to coordinate audit activities with identified risks as part of audit project risks.

## 4. ACCOUNTABILITY

4.1 The implementation of this policy is the responsibility of Council, overseen by the Audit Committee and effected by the College Management.

4.2 The Management of the college is responsible for applying the risk management framework and techniques in their planning, operating and reporting activities.

4.3 The Audit Committee has responsibility for representing Council's obligation to all relevant committees of Council.

4.4 Council actively participates in risk and control monitoring and analysis by considering and reviewing the enterprise wide risk profile and management environment.

4.5 Reporting of risk management performance against policy and strategic targets is conducted routinely as appropriate depending on the nature of the risk.

4.6 The underlying strategies to this policy are reviewed annually by Council to ensure its continued application and relevance.

4.7 A regular external independent review of the policy adoption and execution is performed to provide objective feedback to Council on its effectiveness.

## 5. OBJECTIVES

The objectives of this policy are to:

5.1 Define accountabilities at Deputy Principal level;
5.2 Define responsibilities for Risk Management; and
5.3 Indicate core Risk Management activities and services.

## 6. ROLE OF COUNCIL

6.1 The members of Council must be responsible for identifying the risks associated with the environment within which the College operates and for establishing a risk tolerance policy. Council is responsible for the governance of risk as provided in Chapter 4 of the King III Report on Governance.

6.2 Council has delegated the oversight of risk governance to the Audit Committee.

## 7. ROLE OF AUDIT COMMITTEE

The Audit Committee is responsible for oversight of the institution's control, governance and risk management. Furthermore, the Committee should provide Council with independent counsel, advice and direction in respect of risk management.

## 8. ROLE OF COLLEGE MANAGEMENT

8.1 Management is to identify risks as per Council's risk tolerance policy and to help define, promote and implement the risk management policy and plan which is consistent with the approach, aims and strategic goals of the College, and is designed to safeguard the organisation's assets while allowing sufficient operational freedom to use those assets optimally to achieve those goals.

8.2 College Management ("the Executive") assists Council and the Audit Committee to discharge their responsibilities. The Executive has the responsibility for providing a framework for managing risks across the Organisation. The Executive is required to facilitate the risk management process, create awareness of the need for risk management and establish a risk management infrastructure.

8.3 Development of risk management structures is also consistent with the aims and strategic goals of the organisation. Ultimately, a structured approach to the consideration of risk management will enable management across the College to make fully informed decisions to further enhance stakeholders' value, without exposing the College to unacceptable levels of risk.

8.4 A sound system of internal control depends on a thorough and regular evaluation of the nature and extent of risks to which the College is exposed. Since there are rewards for successful risk–taking in business, the purpose of internal risk management is to help manage and control risk rather than eliminate it.

## 9. DEFINITIONS

### *9.1 Risk*

Risks are defined as uncertain future events which could negatively influence the achievement of the objectives of the College, including strategic, operational, financial and compliance objectives.

### *9.2 Business risk*

A business risk is the threat that an event or action will adversely affect an organisation's ability to maximise stakeholder value and to achieve its business objectives. Business risk arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.

### 9.3 Risk appetite

Risk appetite is defined as the informed selection of risks the Council will engage in.

### 9.4 Risk tolerance

Risk tolerance defines the sensitivity of the College to risk exposure. How sensitive are the College's operating and economic imperatives to its business risks?

## 10. STRUCTURE

Council recognises that it has overall responsibility to safeguard the assets of the College and to prevent and detect fraud and other irregularities. Responsibility and accountability is delegated by Council to the Executive.

### 10.1 Senior Management

Senior management's role is to:

10.1.1 Ensure that clear roles and responsibilities are defined within their units;

10.1.2 Be accountable for the maintenance of adequate ongoing risk assessment;

10.1.3 Be responsible for assessing and managing risk in their units;

10.1.4 Be responsible for making staff at all levels aware of the operational and risk control environment within each business function; and

10.1.5 Ensure that control manuals and other key documents reflect policies regarding risk and that mechanisms are in place to ensure that such policies, manuals and documents are maintained.

In order to support senior management in discharging their responsibilities, the following Risk infrastructures have been established.

### 10.2 Audit Committee

10.2.1 The Audit Committee is established by Council. Council will also decide the composition of the committee.

10.2.2 The Committee maintains the visibility of and commitment to effective risk management at the most senior management level.

10.2.3 The Committee provides a forum for sharing strategic initiatives in order to ensure that Internal Audit is able to support future change in a proactive manner.

10.2.4 The Audit Committee has been established within the College with the responsibility for providing a framework for managing risks across the organisation.

10.2.5 The Audit Committee is required to help identify and define risks as per Council's policy for risk management and its risk tolerance policy, create awareness of the need for risk management and establish a risk management infrastructure within the College.

10.2.6 The Audit Committee assesses the results of internal reporting mechanisms for monitoring relationships with external stakeholders. Information generated by different departments is compared and any trends investigated. This assists the Committee to identify risk areas based on potentially fragmented feedback from external sources.

10.2.7 The Audit Committee is responsible for addressing the Risk Management (RM) of business processes which may cross the boundaries of business functions, directorates and locations.

10.2.8 The Audit Committee is responsible for:

10.2.8.1 Facilitating and maintaining the organisations' framework for risk management;

10.2.8.2 Promoting and implementing the risk policy by enhancing the level of awareness within the College;

10.2.8.3 Providing guidance on the management of risk;

10.2.8.4 Raising the awareness of risk management across the College of Cape Town;

10.2.8.5 Assisting the directors and senior management to make fully informed decisions to further enhance stakeholders' value, without exposing the College to unacceptable levels of risk;

10.2.8.6 Assisting management in the monitoring of risks across the College and acting as a conduit for reporting these on a consolidated basis to the Management Risk Committee;

10.2.8.7 Identifying and monitoring trends and common themes across the College in order to address organisation-wide issues and facilitate the sharing of information;

10.2.8.8 Working with senior management to improve the management control environment;

10.2.8.9 Providing senior management with practical recommendations for risk improvement

10.2.8.10 Interacting with the various business units within the College.

# 11. RISK MANAGEMENT PROCESSES

## *11.1 Risk management responsibilities*

11.1.1 The following are identified as being the core responsibilities that are vital to effective risk management:

| | |
|---|---|
| 11.1.1.1 | Risk awareness |
| 11.1.1.2 | Risk assessment |
| 11.1.1.3 | Risk mitigation |
| 11.1.1.4 | Risk monitoring and reporting |

11.1.2 All risks and opportunities relating to the business objectives of the College must be identified and evaluated.

11.1.3 Control measures are then applied for the various risks to enhance, reduce or minimise their impact and probability.

11.1.4 Residual risk may be transferred to an insurance company or contracts where applicable.

## *11.2 Awareness*

11.2.1 Awareness is a key component for identifying, and subsequently taking appropriate action to mitigate risks.

11.2.2 On-going training and communication of the threats to the business, together with business and task-orientated skills training, are essential components of risk mitigation measures.

11.2.3 The College policies regarding training and communication issues are:

11.2.3.1 To promote risk awareness throughout the College;

11.2.3.2 To ensure appropriately skilled resources are made available to manage risk to an acceptable standard;

11.2.3.3 To ensure management encourage a “risk awareness culture” within the organisation; and

11.2.3.4 Where appropriate, to provide training regarding regulatory, legal and task-related issues.

## *11.3 Assessment*

### 11.3.1 The assessment of risks

The assessment of risks is based on:

11.3.1.1 Identification of threats to business processes;

11.3.1.2 The impact of those threats; and

11.3.1.3 The subsequent evaluation of controls in place to mitigate the subsequent risk.

### 11.3.2 The Principal and senior management

The Principal and senior management ensure that:

11.3.2.1 Risk is assessed within a formal risk management methodology, as facilitated by the Executive;

11.3.2.2 The inherent risks or business risk profiles associated with individual business functions and processes under their control are adequately and regularly assessed;

11.3.2.3 The financial cost of controlling risk is appropriately balanced against the potential cost should the threat materialise;

11.3.2.4 The controls currently in place over a business unit are operating effectively;

11.3.2.5 There is close liaison with the Executive in assessing risk;

11.3.2.6 Control systems are in place to assess the risk of changes to operations (for example, new services, products, system changes);

11.3.2.7 Appropriate performance indicators are developed and maintained for assessing and reporting risk;

11.3.2.8 The scope of the risk assessment covers not just the internal environment but addresses external dependencies;

11.3.2.9 Critical success factors are identified within each directorate and priority is given to mitigating risk in those key areas;

11.3.2.10 Procedures are in place to ensure that other parties dealing with risk in the College are notified when a relevant risk is identified;

11.3.2.11 Incidents of operational failure and associated losses are recorded; and

11.3.2.12 Risk is transferred when insurable, subject to financial viability.

### 11.3.3 The Executive

The Executive is responsible for assisting line management with the assessment of risks within their business function and for providing guidance on the framework used for this assessment.

## *11.4 Mitigation*

Risk Management is a continuous rather than "once-off" process. Management ensures that risks are reviewed on a regular basis and appropriate countermeasures implemented. As a minimum, the Principal periodically considers the following:

11.4.1 The need for improved measures to address control failures or the relevance of measures in over-controlled areas;

11.4.2 That feedback from internal audit reports is effectively assessed and appropriate action taken;

11.4.3 That incidents and issues are logged and documentation of their resolution maintained;

11.4.4 Measures to reduce the overall risk profile of the College;

11.4.5 That fully documented business continuity plans are in place, and are regularly tested under different scenarios; and

11.4.6 That procedures are in place to ensure all critical systems are regularly reviewed.

The Executive provides support to the Principal in addressing these concerns. In addition, the Executive seeks to make improvements on an organisation wide level with the benefit of consolidated information.

## *11.5 Monitoring and Reporting*

The reporting process is critical to ensure that control over the management of risks is maintained and that issues are addressed. Central to this are the following principles:

### 11.5.1 Strategic Level

The Audit Committee is informed by both Council and the Principal of any developments in organisational strategy that may have a significant effect on the risks associated with the College. Where there is an incident of a sensitive or confidential nature, the Audit Committee is advised at the earliest possible opportunity. The Executive provides a forum for keeping the Audit Committee and the Internal Audit Function informed of strategic decisions which could impact on risk.

### 11.5.2 Operational Level

The Executive is informed by managers at the earliest possible date regarding:

11.5.2.1 Significant proposed new or amended operating procedures, products, computer systems or applications;

11.5.2.2 Material, or potentially material, breakdowns of security or controls in computer systems resulting in the threat of computer outage, hacking or virus infection (any breakdown is reported whether or not the threat materialises);

11.5.2.3 Evidence or suspicion of material or potentially material internal fraud, employee dishonesty, or any situation where deliberate or negligent employee conduct has compromised the security of College assets; and

11.5.2.4 Evidence or suspicion that a control weakness has placed College assets or resources at risk to external fraud or threat.

Where research into new strategies and new services is being performed, the Executive is informed and involved at an early stage.

### 11.5.3 Other Management Reporting Principles

Other key requirements for the reporting of risk are that:

11.5.3.1 A framework has been set up within the existing line management of the College to report areas of risk arising from business processes and regulatory reporting on individual business units;

11.5.3.2 An appropriate package of performance indicators has been developed and maintained for assessing and reporting risk;

11.5.3.3 Systems are in place to ensure that action is taken to mitigate reported risks appropriately;

11.5.3.4 Regular monitoring reports are received from all areas within the organisation on a pre-determined and regular basis;

11.5.3.5 A suitable framework exists to ensure that all risk related issues raised by Functional Managers are assessed by the Executive, and the Internal Audit Function; and

11.5.3.6 Losses, from whatever part of the Organisation, are reported and assessed within a risk management framework.