|  |  |
| --- | --- |
| Tshwane University of  Technology | |
| University Risk Management Policy Framework |
| 13 November 2007 |

|  |
| --- |
|  |
|  |
|  |
|  |

Contents

1. Introduction 1

1.1 Background and purpose 1

1.2 Definition 1

1.3 Background to URM Policy Framework 1

1.4 Benefits of URM 2

1.5 Organogram for risk management within TUT 3

2. Risk Management Policy Statement 4

3. Risk Management Standards 5

3.1 Committee Responsibilities 5

3.2 Reporting Responsibilities 5

3.3 Risk Assessment Responsibilities 7

3.4 Control Responsibilities 7

3.5 Governance and Assurance Responsibilities 8

4. Guidelines 9

4.1 Accountability and responsibility guidelines 9

4.1.1 Roles and responsibilities of the Council 9

4.1.2 Roles and responsibilities of the Council Risk Management Committee 11

4.1.3 Roles and responsibilities of the Audit Committee 11

4.1.4 Roles and responsibilities of the Risk Working Group 11

4.1.5 Roles and responsibilities of Management 13

4.1.6 Roles and responsibilities of the Chief Risk Officer 14

4.2 Reporting requirements 16

4.2.1 Internal reporting processes for risk information 16

4.2.2 The frequency of risk monitoring 16

4.2.3 Incident reports must be generated for unacceptable losses or events 17

4.2.4 Normal management reporting processes 17

4.3 Risk Assessments 17

4.3.1 Profile the context 17

4.3.2 Profile the objectives of the faculties and support functions 18

4.3.3 Profile the stakeholders of the University 18

4.3.4 Profile the University’s value creation processes 19

4.3.5 Identify and profile the University’s key assets and performance

drivers 19

4.3.6 Map the University’s strategy 19

4.3.7 Profile the key processes 20

4.3.8 Identify potential sources of risk associated with the University’s

profile 20

4.3.9 Assess the impact of risk across the University 20

4.3.10 Identify any influencing factors that may contribute to or shape the

risk profile 21

4.3.11 Evaluate recent and imminent internal changes as possible sources

of risk 21

4.3.12 Identify external changes and identify associated risks 21

4.3.13 Identify the potential root causes of risk events 21

4.3.14 Identify the key controls currently implemented for the identified

risks 21

4.3.15 Identify the perceived shortcomings in current measures to mitigate

the impact of risks 22

4.3.16 Calculate the probability of risk events 22

4.3.17 Calculate the potential impact of the identified risk scenarios 23

4.3.18 Rank the risks in order of priority (inherent risk) 23

4.3.19 Control requirements 23

4.3.20 Take decisions on the acceptability of identified risks and controls 25

4.3.21 Document your action plans for risk mitigation 25

4.3.22 Use the outputs of risk assessments for budgeting and capital

allocation processes 25

4.4 Governance requirements 26

4.4.1 Establish an organisational framework of assurance for key risks

and controls 26

4.4.2 Internal Audit provides assurance that management processes are

adequate for the identification and monitoring of significant risks 26

4.4.3 The outputs of risk assessments are used to direct internal audit

plans 26

4.4.4 Internal Audit provides an evaluation of risk management processes 26

4.4.5 Internal Audit provides objective confirmation that the Council

receives the right quality of assurance and reliable information

from management regarding risk 27

4.4.6 Safety, environmental, health and hygiene management 27

A Risk Ratings 28

B Risk Definitions 30

C Risk Categories 32

D References 33

1 Introduction

1.1 Background and purpose

The underlying premise of University Risk Management (URM) is that every institution exists to provide value for its stakeholders. All universities face uncertainty and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. URM enables management to deal effectively with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

Value is maximised when management sets objectives to achieve an optimal balance between growth and related risks, and effectively deploys resources in pursuit of the University’s objectives.

This document sets out Tshwane University of Technology’s (TUT) University Risk Management Policy Framework. It describes TUT’s risk management policies, structures, processes and standards.

1.2 Definition

URM deals with risks and opportunities affecting value creation or preservation and is defined as follows:

*University Risk Management is a process, effected by the Council, the Senate, executive management and personnel, applied in strategy setting and across the operations of the University, designed to identify potential events that may affect the University, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of University objectives of teaching, learning, research and community engagement [[1]](#footnote-1)*

1.3 Background to URM Policy Framework

It is acknowledged that the new style of risk management in the King II Code of Corporate Governance (King II) and the Public Finance Management Act (PFMA) addresses a much wider spectrum of risk than in the past. In addition, the corporate governance drivers behind risk management today require new ways of reporting and monitoring the University’s risk exposure.

The TUT Council is responsible and accountable for directing and monitoring the University’s risk management activities and related performance in a structured framework. All faculties, departments, sections and units support the Council in assuming maintenance of an effective system of risk management.

The risk management standards herein set out the rules embedded within the University’s Risk Management Policy Framework. These are the mandatory requirements established by the Council for the management of risk in the University. The standards are based on current recognised business practices and standards, and corporate governance principles.

It is important to note that the University Risk Management Policy Framework is, of necessity, an evolving document. The contents of the Framework reflect the current risk management requirements of the University. Future versions of this document will reflect advances and developments in the University’s risk management strategies and processes. The document must be reviewed and updated, initially every 6 months for the first 18 months, and thereafter annually.

1.4 Benefits of URM

The benefits of URM to TUT encompass:

* Aligning risk appetite and strategy – TUT management considers their risk appetite in evaluating strategic alternatives, setting related objectives and developing mechanisms to manage related risks. This should be approved by the Council.
* Enhancing risk response decisions – URM provides the rigour for management to identify alternative risk responses – risk avoidance, reduction, sharing, transfer and acceptance.
* Reducing operational surprises and losses – TUT gains enhanced capability to identify potential events and establish responses, thereby reducing surprises and associated costs or losses.
* Identifying and managing multiple and cross-campus risks – TUT faces a myriad of risks affecting different parts of the Institution and URM facilitates effective responses to the interrelated impacts and enhances an integrated response to multiple risks.
* Seizing opportunities – By considering a full range of potential events, TUT management is positioned to identify and proactively realise opportunities.
* Improving deployment of capital – Obtaining robust risk information allows TUT management to effectively assess overall funding requirements and enhance funding allocation.
* Ensuring compliance with laws and regulations – URM contributes to effective reporting and monitoring of compliance with laws and regulations and assists with the limitation of damage to TUT’s reputation and associated consequences.
* Increasing probability of achieving objectives – URM helps management achieve TUT’s performance and financial targets and assists with the prevention of loss of resources. Controls and risk interventions will be chosen on the basis that they increase the likelihood that TUT will fulfill its intentions/commitments to its stakeholders.

*Every employee of TUT has a part to play in this important endeavour.*

TUT – RISK MANAGEMENT GOVERNANCE STRUCTURE

(ORGANOGRAM)

TUT

COUNCIL

**MONITORING**

- CEO (in attendance)

- CRO (in attendance)

Council

Audit

Committee

CRMC

--------------- Through the CRO

Internal

Audit

RWG

Through the DVCs (EMC)

e.g. through policies, rules & regulations

NB: EMC AGENDA

University-wide embedding

of risk management

(TUT’s daily activities)

CRO = CHIEF RISK OFFICER

RWG = RISK WORKING GROUP

CRMC = COUNCIL RISK MANAGEMENT COMMITTEE

**Risk Management Policy Statement**

***Policy Statement***

At Tshwane University of Technology (TUT) we are committed to the optimal management of risk in order to achieve our vision, our principal tasks and key objectives and to protect our core values.

The Council of TUT has committed the University to a process of risk management that is aligned to the principles of the King II Report on Corporate Governance, 2002. The features of this process are outlined in the University’s Risk Management Policy Framework. It is expected that all faculties, departments, processes, projects and controlled entities will be subject to the Risk Management Policy. TUT managers will be formally assessed on their contribution to, and implementation of the University’s Risk Management Policy.

Effective risk management is imperative to the University with reference to its risk profile. The realisation of TUT’s strategy depends on the University being able to take calculated risks in a manner that does not jeopardize the direct interests of stakeholders. Sound management of risks will enable management to anticipate and respond to changes in the education environment, and to make informed decisions under conditions of uncertainty.

A University-wide approach to risk management will be adopted by the University, which means that every identified key risk in each part of the University will be included in a structured and systematic process of risk management. All identified key risks will be managed within a unitary framework that is aligned to the University’s corporate governance responsibilities.

It is expected that risk management processes will become embedded in all the University’s systems and processes to ensure that its responses to risk remain current and dynamic. All key risks associated with major changes and significant actions by the University will also fall within the processes of risk management. The nature of its risk profile demands that the University adopt a prudent approach to corporate risk, and its decisions regarding risk tolerance as well as risk mitigation will reflect this. Nonetheless it is not the intention to slow down the University’s growth with inappropriate bureaucracy. Controls and risk interventions will be chosen to assist the University in fulfilling its commitments to stakeholders.

Every employee has a part to play in this important endeavour and we look forward to working with you in achieving these aims.

Signed: …………………………………………. ………………………………………..

Chairperson of the Council Vice-Chancellor and Principal

(Mr RV Matlhare) (Prof EM Tyobeka)

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

………………………………………....

Chairperson, Risk Management Committee

(Prof MS Mokgokong)

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3 Risk Management Standards**

**3.1 Committee Responsibilities**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Standards** | **Responsibility** | **Frequency** |
| 01 | The Council Risk Management Committee (CRMC) will meet on a quarterly basis | Committee Chairperson | Quarterly |
| 02 | The Audit Committee must review the risk management progress at each meeting. Risk management must be a standard agenda item at every Audit Committee meeting. | Chairperson of the Audit Committee | Quarterly |
| 03 | The Executive Management Committee (EMC) should receive the minutes of RWG meetings, and must review risk management progress on a quarterly basis | Vice-Chancellor | Quarterly |
| 04 | The RWG must meet on a quarterly basis. The RWG is a sub-committee of the EMC | Chairperson of the RWG | Quarterly |
| 05 | The faculties and support functions’ management committees are responsible for risk management in their respective line functions and must review risk management formally at every meeting. | Deans and directors | Quarterly |

**3.2 Reporting Responsibilities**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Standard** | **Responsibility** | **Frequency** |
| 06 | The Council will include statements regarding risk management performance in the University’s Annual Report to the Minister of Education. | Chairperson of the Council and Vice-Chancellor | Annually |
| 07 | The EMC will submit a risk management report to the CRMC on a quarterly basis. The report must focus on the following:   * The top 15 strategic risks facing the University * Any risk developments or losses * Summary of key risks and the related responses within faculties and departments. | Vice-Chancellor | Quarterly |

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Standard** | **Responsibility** | **Frequency** |
|  | Note: Submission of report to Audit Committee |  |  |
| 08 | The RWG will draft a risk management submission to the EMC on a quarterly basis. This must focus on the following:   * The top 15 strategic risks * The top 20 risks facing the faculties and support functions on a consolidated basis * Any risk developments or losses | Chairperson of the RWG (CRO) | Quarterly |
| 09 | Each faculty and support function will submit a risk management submission to the RWG on a quarterly basis. This will focus on the following:   * The top 5 risks facing each of the faculties and support functions * Any risk developments or losses. | Deans and  directors | Quarterly |
| 10 | The heads of departments will submit a risk management submission for the departments under their control to the faculty/support function management team on a quarterly basis. This must focus on the following:   * The top 5 risks facing the departments * Any risk developments or losses | Heads of  departments | Quarterly |
| 11 | Decisions made at the CRMC and the RWG will be communicated to the deans, directors and heads of departments  Note: Decisions of the RWG will be considered and endorsed by the EMC | Chairperson of the CRMC and Chairperson of the RWG (CRO) | Quarterly |
| 12 | The CRO will be responsible for developing standardised reporting templates and report collation at all levels | CRO | As scheduled |

**3.3 Risk Assessment Responsibilities**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Standard** | **Responsibility** | **Frequency** |
| 13 | The Council must independently review the key risks of the University and management’s strategy to mitigate the risks, at least once a year | Chairperson of the Council | Annually |
| 14 | The RWG together with the CRO will arrange for the University’s key risks to be formally re-evaluated once a year through a facilitated process | CRO | Annually |
| 15 | The faculties and support units will formally re-assess their top 5 risks annually | Deans and directors | Annually |
| 16 | The heads of departments/units will formally re-assess their top 5 risks annually | Heads of departments | Annually |
| 17 | All Committees will review their risk registers at each management meeting and update the contents of the risk registers to reflect any changes | All Committee Chairpersons | As scheduled |
| 18 | The CRO will be responsible for the facilitation of all risk assessments, populating the risk registers and co-ordination of reporting by the various committees | CRO | As scheduled |

**3.4 Control Responsibilities**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Standard** | **Responsibility** | **Frequency** |
| 19 | The Council must consider the report of the Audit Committee and the EMC concerning the effectiveness of internal controls at least once a year for annual reporting purposes | Audit Committee Chairperson | Annually |
| 20 | The Audit Committee and the EMC must exchange minutes of meetings.  The performance of internal controls in mitigation of risks documented in the risk registers must be reviewed and communicated to the Council | Chairpersons of the Audit Committee and the EMC | Quarterly |
| 21 | The deans and directors will report to the RWG regarding the performance of internal controls for those risks documented in the faculties/support units’ risk registers | Deans and directors | Quarterly |

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Standard** | **Responsibility** | **Frequency** |
| 22 | The heads of departments will report to their respective deans or directors regarding the performance of internal controls for those risks documented in the departmental risk registers | Heads of departments | Quarterly |
| 23 | All risk registers must contain action plans for improving risk controls and risk interventions. Each committee must review progress made with these action plans | Deans, directors, and heads of departments | As scheduled |

**3.5 Governance and Assurance Responsibilities**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Standard** | **Responsibility** | **Frequency** |
| 24 | Each risk must have a nominated owner, who will be responsible for the following:   * Updating risk information, * Providing assurance regarding the effectiveness of the risk’s controls, * Co-ordinate the implementation of action plans for the risk, and * Reporting on any developments regarding the risk | All | As scheduled |
| 25 | The Internal Audit function will use the outputs of the risk assessments to compile audit coverage plans.  The CRO, together with the Vice-Chancellor, Chief Internal Auditor and Chief Financial Officer will use the outputs of risk assessments to identify the relevant assurance provider, who will in turn evaluate the effectiveness of controls, associated with his/her field of expertise. | Internal Audit | Annually around April/May |
| 26 | The Internal Audit function, in consultation with the CRO, will formally review the effectiveness of the University’s risk management processes once a year. | Internal Audit and CRO | Annually, in time for inclusion in the University’s Annual Report |

**4. Guidelines**

**4.1 Accountability and responsibility guidelines**

**4.1.1 Roles and responsibilities of the Council**

The Council is ultimately accountable for risk management. These responsibilities include:

* The Council is responsible for the identification of major risks, the total process of risk management, and for forming its own opinion on the effectiveness of the process. Management is accountable to the Council for designing, implementing and monitoring the process of risk management and integrating it into the day-to-day activities of the University.
* The Council should identify, evaluate and monitor the risk issues and key performance indicators affecting the ability of the University to achieve its strategic purpose and objectives.
* The Council should ensure that appropriate systems have been implemented to manage the identified risks, measure the potential impact and probability and to proactively manage the risks to ensure that the University’s assets and reputation are suitably protected.

Each member of the Council must understand his/her accountability for risk management within the University. Although the Council may choose to nominate one member of the Council as the co-ordinator of risk management reporting requirements, it is clear that all members have accountability for risk management in the University.

The Council is responsible for disclosures in the annual report regarding URM.

***4.1.1.1 The Council of TUT will provide stakeholders with assurance that key risks are properly identified, assessed, mitigated and monitored.***

The Council should receive credible and accurate information regarding the risk management processes of the University in order to give the necessary assurance to stakeholders. The reports from the Audit Committee and RWG must provide an evaluation of the performance of risk management and internal control. The Council should ensure that the various processes of risk management cover the entire spectrum of risks faced by TUT. The assurance process includes statements regarding the appropriateness of the University’s risk/reward trade-off.

As a result of the fluid nature of risk in the University and the related education environment, it is imperative that risk is confronted in a systematic and structured manner. In a complex environment where there are literally thousands of technical, process and strategic risks, it is vital that the management of risk is undertaken in a formalised manner.

The Council of TUT will provide stakeholders with the assurance that management has a pre-emptive approach to risk.

***4.1.1.2 The Council of TUT will maintain a formal risk management policy for the University***

Stakeholders need to understand the Council’s standpoint on risk. The Council, therefore, should maintain the University’s Risk Management Policy. The Risk Management Policy Statement underpins the development of the University’s URM process. The Policy can be used as a reference point in matters of dispute and uncertainty such as risk tolerance and appetite for risk.

***4.1.1.3 The Council will formally evaluate the effectiveness of the University’s risk management process on an annual basis***

The Council will independently assess the effectiveness of the University’s risk management processes. Success with risk management will be evaluated from CRMC reports, internal and external audit reports, variance reports, speed of progress, the University’s risk culture, unexpected losses, internal control effectiveness and financial success. The Council’s evaluations will be formally recorded in the minutes of Council meetings.

It is recognised that risk management has evolved into a complex management discipline in its own right. The Council’s evaluation of risk management, therefore, will be based primarily on an independent review to be performed by the University’s Internal Audit function. The annual review will be undertaken by qualified staff, with the ability to review all aspects of risk management.

Management must ensure that sufficient independence is maintained in conducting the annual review. Criteria for the evaluation have been established (Refer to Appendix A for the tables to be considered for the assessment). Assurance of the processes surrounding key risks must be given. This implies some knowledge of the processes of risk management and assumes that it has been witnessed to some degree.

***4.1.1.4 The Council of TUT will confirm that the risk management process is accurately aligned to the strategy and performance objectives of the University***

The Council of TUT will ensure that the risk management processes address risk in a balanced way, giving due attention to all types of risk. The Council will evaluate whether appropriate resources are being applied to the management of the various categories of risk. The Council will evaluate whether risk management processes are aligned to the strategic and performance objectives of TUT. A balanced perspective of risk and risk management is required in proportion to the weighting of the potential risk impact across the University. Council members must ensure that there is a forward-looking orientation included in the consideration of risk.

**4.1.2 Roles and responsibilities of the Council Risk Management Committee**

The CRMC will be responsible for addressing the corporate governance requirements of risk management and monitoring TUT’s risk management activities. The CRMC has a defined mandate and terms of reference (Charter), which covers the following aspects:

* Constitution;
* Purpose;
* Responsibilities and duties;
* Authority;
* Membership;
* Meetings; and
* Approval

The CRMC will meet on at least a quarterly basis.

**4.1.3 Roles and responsibilities of the Audit Committee**

Even though the Council has formed a CRMC to assist in the discharge of its responsibilities with regards to business risk, the Audit Committee has an interest in risk management through its focus on internal controls. It is recognised in the COSO Enterprise Risk Management Framework, that there will be a small degree of overlap between the two areas in auditing processes and reporting protocols. In certain cases the Audit Committee will provide an assurance role concerning risk management processes. It is necessary to ensure that the Audit Committee is kept fully informed regarding the performance of risk management.

**4.1.4 Roles and responsibilities of the Risk Working Group**

The RWG will monitor the University’s risk management processes.

The RWG will be responsible for addressing the corporate governance requirements of risk management and monitoring the University’s performance with regard to risk management. The Committee has a defined mandate and terms of reference, which covers the following aspects:

* Constitution;
* Membership;
* Authority;
* Terms of reference; and
* Meetings.

The RWG will meet on at least a quarterly basis. Functions and responsibilities of the RWG include:

* Establishment and monitoring the implementation of the risk management strategy;
* Ensuring that the responsibilities for and co-ordination of risk management are clear;
* Advising the EMC and the Council through the CRMC on urgent risk management issues and required initiatives as part of its quarterly reporting process;
* Overseeing the implementation and maintenance of the ongoing process of risk identification, quantification, analysis and monitoring throughout TUT;
* Ensuring that risk management induction, training and education programmes are targeted appropriately for all levels of personnel and that they are established and implemented;
* Reviewing and recommending action for improvement regarding outstanding actions on risk management plans;
* Evaluating the risk profile of the University, as well as for major projects and new ventures requiring the approval of Council;
* Reviewing issues for consideration, as identified by the EMC and the Audit Committee;
* Assisting with the development of an integrated approach to financing and managing risk to minimise cost;
* Facilitating the sharing of post-loss analysis information, thereby improving prevention and control measures;
* Reviewing the risk assessments on a quarterly basis to take note of the material risks to which the University may be exposed, and consider, note and, if necessary, comment on the strategy for managing those risks;
* Considering, noting and, if necessary, commenting on management’s responses to significant risks;
* Keeping abreast of all changes to the risk management and control system and ensuring that the risk profile and common understanding is updated, as appropriate.

**4.1.5 Roles and responsibilities of management**

Management is accountable to the Council for designing, implementing and monitoring the process of risk management and integrating it into the day-to-day activities of the University.

Management is responsible for appointing a CRO to assist management in discharging its responsibilities.

More specifically, management is responsible for:

* Designing a URM programme in conjunction with the CRO;
* Deciding on the manner in which risk mitigation will be embedded in management processes;
* Inculcating a culture of risk management at TUT;
* Providing risk registers and risk management reports pertaining to risk and control to the CRO;
* Identifying positive aspects of risk that could evolve into potential opportunities for TUT;
* Assigning a manager to every key risk for appropriate mitigation and to determine an action date:
* Viewing risk as an opportunity by applying the risk/reward principle in all decisions impacting on the University;
* Utilising available resources to compile, develop and implement plans, procedures and controls within the framework of TUT’s URM Policy to effectively manage the risk within the University and more specifically within the faculties and support functions;
* Ensuring that adequate and cost-effective risk management structures are in place;
* Identifying, evaluating and measuring risks and, where possible, quantifying and linking each identified risk to key performance measurement indicators;
* Developing and implementing risk management plans including:

- Actions to optimise a risk/reward profile to maximize reward with risk, as contained within the Council’s approved risk tolerance (risk appetite);

- Implementation of cost-effective preventative and contingent control measures; and

- Implementation of procedures to ensure adherence to legal and regulatory requirements.

* Monitoring of the URM processes on both a detailed and macro basis by evaluating changes, or potential changes, to risk profiles;
* Implementing and maintaining adequate internal controls and monitoring their continued effectiveness;
* Implementing those measures as recommended by the internal/external auditors which, in their opinion, will enhance control at a reasonable cost; and
* Reporting to the RWG on the risk process and resultant risk/reward profiles.

**4.1.6 Roles and responsibilities of the Chief Risk Officer**

The role of the CRO is to develop, communicate, co-ordinate and monitor the institution-wide risk management activities within the University. It should be stressed that this function could be delegated to an official currently in the employ of the University with a wide knowledge of the operations of the University.

Although management may appoint a CRO to assist in the execution of the risk management process, accountability to the Council remains with management and effective risk management is the responsibility of every employee. The risk management process does not, however, reside in any one individual or function, but requires an inclusive team-based approach for effective application across the University.

The following are the responsibilities of the CRO:

* Assists the CRMC to fulfill its responsibilities in terms of its charter;
* Communicates with the CRMC regarding the status of institution-wide risk management;
* Takes overall responsibility for the common risk framework and co-ordinates risk management activities across TUT;
* Proposes a methodology and framework for URM for approval by the Council;
* Periodically perform a gap analysis of TUT’s URM process;
* Performs reviews of the risk management process to improve the existing process;
* Facilitates quarterly risk management and risk assessments for all major changes and incidents, such as accidents, purchases of capital equipment, restructuring of operational processes, etc;
* Develops systems to facilitate risk monitoring and risk improvement;
* Ensures that all risk categories are included in the assessment;
* Ensures that key risk indicators are included in the risk register;
* Aligns the risk identification process with TUT’s strategic objectives and business plan;
* Agrees on a system of risk quantification;
* Compiles a consolidated risk register on a quarterly basis;
* Formally reviews the occupational health, safety and environmental policies and practices;
* Creates mechanisms for identifying nodes of change;
* Consolidates all information pertaining to all risk-related functions, processes and activities;
* Provides input into the development and implementation of business continuity management plans;
* Transfers knowledge in respect of an effective and sustainable process of risk identification, quantification and monitoring to management;
* Records the decisions regarding mitigation for every risk facing TUT in the risk register;
* Formulates central solutions for common risks and for risks where central facilities are available, for approval by the EMC;
* Liaises closely with the Internal Audit function to devise a risk auditing programme, based on the information reflected in the risk registers;
* Benchmarks the performance of the risk management process to the risk management processes adopted by other universities, both in South Africa and abroad;
* Implements a formalised risk information system;
* Ensures that risk management training is conducted at appropriate levels within TUT, to inculcate a risk management culture;
* Assists in the compilation of risk registers for all faculties and support functions;
* Communicates the risk strategy to all management levels and employees; and
* Ensures that the necessary risk management documentation is developed in respect of the risk management process.

**4.2 Reporting Requirements**

**4.2.1 Internal reporting processes for risk information**

A tiered structure of risk reporting must be followed. The purpose of internal reporting on risk is to ensure that higher levels of management, as well as governance bodies, understand and monitor developments regarding risk and risk management. The tiered structure of risk reporting should include amongst others:

* Each operating unit is required to submit its top 5 risks on the register to their respective faculty/support function’s dean/director on a quarterly basis;
* Each of the faculty/support function’s deans/directors is required to submit the top 5 risks facing each of the faculties and support functions to the RWG on a quarterly basis;
* The RWG is required to submit the top 20 risks facing the faculties and support functions, on a consolidated basis, to the EMC and the Audit Committee on a quarterly basis; and
* The EMC is required to submit the top 15 strategic risks facing the University to the CRMC.

The CRO will assist with the execution of the risk reporting process.

**4.2.2 Frequency of risk monitoring**

The risk registers should indicate how often a key risk should be monitored and reviewed. In the realm of financial risk, exposure may be monitored on a continual real-time basis. Other risks, such as regulatory change, may only need formal review once a year. For the majority of risks it is prudent to choose monitoring periods that span between 1 and 3 months. Risks with an unknown pattern and risks that are new to the University should receive more frequent attention. Results of the monitoring processes must be documented in a pre-defined format.

**4.2.3 Incident reports must be generated for unacceptable losses**

This is an internal management function and must form part of the URM Policy Framework. The destination of incident reports must be determined by the nature of the loss, but losses that originate from risks contained in the key risk registers must always be elevated to higher levels of management. Variance reports are incorporated in routine management reporting processes. The inclusion of risk-related variances can be incorporated.

**4.2.3 Normal management reporting processes**

Normal management processes such as monthly management accounts, Safety, Health Environment and Quality (SHEQ) and other similar reporting that contains risk and control issues should still be reported on in the current prescribed manner.

**4.3 Risk Assessments**

Once a year, before the end of March, Executive Management, together with the faculties and support functions, should undertake a **thorough re-assessment** of its risks using the following methodology.

*The first part of conducting a structured risk assessment is to profile the key building blocks of the University’s business model. This will highlight dependencies and the critical parts of the University, and start to pinpoint vulnerabilities.*

**4.3.1 Profile the context**

The risk assessment processes begin with the profiling of the University’s context. The outputs of this task must be documented and includes, but is not limited to the:

* Academic environment;
* Total size of the faculties/support functions;
* Key players;
* Substitute courses;
* Key suppliers;
* Key student groupings; and
* Market’s driving forces.

**4.3.2 Profile the objectives of faculties and support functions**

The objectives should include, but not be limited to the:

* Fee targets;
* Costs assigned;
* Objectives and targets related to students; and
* Other business objectives.

**4.3.3 Profile stakeholders of the University**

Stakeholders may include the following:

1. Department of Education;
2. Students;

3. Employees (both academic and support staff);

4. Employee organisations;

5. Authorities;

6. Industry bodies;

7. Communities;

8. Social organisations;

9. Debtors; and

10. Creditors.

**4.3.4 Profile the University’s value creation processes**

The manner in which economic value is generated by the University should be identified and interpreted. This contributes to the understanding of potential risk within the University. The drivers of value must be identified. Methods of valuation must be understood. The University’s values of risk can be identified, calculated and profiled. These values will relate to all classes of asset and liability within the business. The following aspects should be profiled:

* Asset values;
* Revenue and expenditure streams;
* Service portfolios; and
* Socio-economic processes.

**4.3.5 Identify and profile the University’s key assets and performance drivers**

The key assets and performance drivers should be profiled and should include amongst others:

* Critical success factors;
* Core competencies;
* Competitive strengths and weaknesses; and
* Asset performance.

**4.3.6 Map the University’s strategy**

The University’s strategy must be specifically verified and interpreted in the context of risk. The future direction and intent of the University must be understood. For example, the University may be seeking to become the leading university of technology. Investments in technology, new academic programmes or innovation may be the strategic direction of the University. Growth tactics in specific sectors must be profiled.

When mapping the strategy, risk appetite must be considered where the desired return from a strategy should be aligned with the University’s risk appetite. Different strategies will expose the University to different risks.

**4.3.7 Profile the key processes**

The key activity chains must be profiled and documented. For example:

* The processes that generate cash must be profiled.
* The drivers of the University’s processes and the key features of these processes must be identified and interpreted.
* Incoming actions such as recruitment, purchasing and procurement must be identified.
* Outgoing processes such as public relations, investments and branding should be profiled.
* Inherent and cyclical processes such as budgeting, information systems and staffing matters must be incorporated in the University’s risk profile.

The deliverable steps 4.3.1 to 4.3.7 will result in a business/dependency profile of TUT and its related activities.

*The next part of the risk assessment process is to identify threats and risks to all of the elements of the University’s model, as profiled above. This can be done using the following processes:*

**4.3.8 Identify potential sources of risk associated with the University profile**

Having established the University profile, the risk assessment process must then identify the potential sources of risk associated with each element of it. The University will follow a top-down approach. Risk is apparent in sudden and unforeseen events, in variances, volatility and failure. The King II Code defines risk as *“the possibility of something happening that will have an impact upon the achievement of the company’s objective.”*

Risk will be apparent in non-linear change, weakness and non-performance. Risk will also be reflected in dimensions of non-conformance. Sources of risk will be classified into external and internal factors. The risk assessment process must select a time period within which risks will be considered, but projecting 18 months into the future is recommended for most key risks. The process must have a future orientation as well as examining the facts of today’s business profile.

**4.3.9 Assess the impact of risk across the University**

Risks do not normally exist in isolation. They usually have a potential knock-on effect on other functions, processes and risk categories. These cause-and-effect relationships must be identified and understood. This principle must become a deliberate and formal part of the risk assessment process. The results of the process must be documented. The aggregated effect of these risk groupings and linkages should be profiled. Many cross-functional effects of risk may not be immediately apparent without deliberate and systematic analysis, so a formal approach is required.

**4.3.10 Identify any influencing factors that may contribute to or shape the risk profile.**

Having identified a key risk exposure (e.g. increasing competition for student enrolments, lack of funding) the risk assessment must identify the factors that influence and shape the risk (e.g. barriers to entry). Every key risk will have influencing factors or variables. Such factors may relate to inherent risk dynamics such as aggregation, accumulation and correlation. Others may relate to timing and cyclical factors. Other influences will be reflected in volatility, dependencies and criticality. The degree of diversification and spread of value may also shape the risk profile. All influencing factors must be documented as part of the process.

**4.3.11 Evaluate recent and imminent internal changes as possible sources of risk**

Recent changes in the University may be a source of present risk. Equally, imminent change may alter the risk profile. The nature of the changes may relate to the launch of new academic programmes. New initiatives may be embarked on and operations commenced. Mergers and partnerships are another potential source of risk. Major changes in the University’s organisational structure can change the dynamics of risk. Retrenchments, cut-backs and layoffs are obvious sources of risk. Significant shifts in strategic direction may increase the values at risk in the University.

**4.3.12 Identify external changes and associated risks**

Risk assessment processes must not only focus on existing dynamics prevailing in the University. Near-future changes must also be included in the process. Time horizons should be determined for this. Anticipated changes that are self-generating will be easily identifiable, such as investments, capital projects or launching of new programmes. Their associated risks must be assessed as part of the risk framework. Certain changes in the educational sector, outside of the University’s control, can also be anticipated such as regulatory change and competitive movements. Associated risks must be assessed.

**4.3.13 Identify the potential root causes of risk events**

Exposure could indicate the potential for risk materialising. Perils or triggers cause actual events. Such triggers or events must be identified and documented. For example, the University may face a risk of a decrease in funding. The trigger for such an event would be the decision made by the government and the extent of the decrease in funding. The purpose of identifying potential root causes is to give direction to risk intervention measures. This process of identifying root causes of events may be left until after the first round of risk assessments has been completed.

**4.3.14 Identify the key controls currently implemented for the identified risks**

The existing controls implemented for identified risks must be documented. The term “control” should not be construed as a financial term only. It is now the commonly accepted term to describe any mitigating measure for any particular type of risk. Controls may take the form of financial mitigations such as hedges, insurance or securities.

They may be managerial in nature, such as compliance procedures, policies and levels of authority. Controls may be strategic in nature, such as diversification related. Controls could also be legal, such as contracts and indemnities.

**4.3.15 Identify the perceived shortcomings in current measures to mitigate the impact of risks**

Management must embark upon a formal process to evaluate the appropriateness of current controls. The levels of risk appetite and limits of risk tolerance will provide the framework for gauging these. Executive observation and judgment is often sufficient to identify shortcomings in control measures, and the level of desired control effectiveness can be expressed. Operational and technical risks lend themselves to a more rigorous process of evaluating control effectiveness. Management must consider all categories of mitigation in this process. Results must be recorded in the relevant risk registers.

**4.3.16 Calculate the probability of risk events**

The probability of occurrence must be assessed for every identified risk. Different methods of calculating probability can be considered, depending on the nature of the risk, but the attached tables must be used in final reporting. Financial risks may lend themselves more readily to statistical interpretations of probability. It might be possible to utilise probabilistic risk analysis techniques in the case of engineering risks (e.g. air-conditioning failure). Other risks, particularly those with a managerial or strategic character, may be best interpreted using simple ranking scales and expert-based interpretations. Please refer to the attached table to guide your risk calculations **(Annexure A).**

A realistic evaluation of the probability of a risk materializing is essential, as it will guide the allocation of resources in the University. When deciding upon a probability factor from the table, the following guidelines should be considered:

* Consider how many similar incidents have occurred at the University;
* Consider, and research if necessary, how many similar incidents have occurred in the educational sector;
* Consider how many similar incidents have occurred at other universities; and
* Consider the effectiveness of the existing preventative controls for the risk.

**4.3.17 Calculate the potential impact of the identified risk scenarios**

This is the potential magnitude of the impact on the University’s operations, should the risk/threat actually occur. This is assessed on the basis that management has no specific/focused controls in place to address the risk/threat (therefore before any controls).

The consequences of risk are not only characterised in financial terms. Management must consider the various scales of impact that are relevant according to the prevalent categories of risk. These may include the scales for reputational damage, personal injuries and fatalities, media coverage and operational impact.

From a strategic viewpoint, management should determine the scale of potential impact upon defined objectives of the strategy. Scales of financial impact are invariably the most common form of risk quantification and must be reflected using the same scales as financial reporting expectations. For purposes of a university, total cost or total income may be the preferred measure.

**Please refer to the attached table to guide your risk calculations (Annexure A).**

**4.3.18 Rank the risks in order of priority (inherent risk)**

Inherent risk is the risk to the University in the absence of management actions to alter either the risk’s likelihood or its impact.

Inherent risk is the product of the impact of a risk and the probability of that risk occurring before the implementation of any direct controls. The score for inherent risk assists management and Internal Audit alike to establish relativity between all the risks/threats identified.

The ranking of risks in terms of net potential effect provides management with some perspective of priorities. This should assist in the allocation of capital and other resources in the University. Although the scales of quantification will produce an automated ranking of risks, management may choose to raise the profile of certain risks for specific reasons. This may be justified because of non-financial influences such as media implications, social responsibilities or regulatory pressures. The ranking of risks should be shaped by strategic objectives.

**4.3.19 Control requirements**

Every risk will have a number of controls, mitigations or interventions that have been designed to contain the potential impact of the risk. These controls need to be identified and evaluated. They will form the basis of an assurance plan for the Council and may be tested by the internal audit process or other independent means of evaluation.

The following aspects of the control environment should be considered.

***4.3.19.1 Verify and evaluate the controls currently in place for key risks***

It is vital that all the existing controls for identified risks are in turn identified and evaluated. Such controls may take the form of policies, procedures and instructions. The controls must be evaluated in two essential ways. Firstly, an evaluation of the **appropriateness** and **adequacy** of the existing controls for the risk must be undertaken. Secondly, the **performance** of the existing controls must be evaluated. Desired levels of control effectiveness must be determined. The gap between existing control effectiveness and desired effectiveness must result in a remedial action plan.

***4.3.19.2 Evaluate the strategic mitigations in place for key risks***

A specific review of the University’s strategic position in the context of risk must be conducted. The degree of strategic flexibility in response to a risk event must be considered. The robustness of the strategy in the context of the risk assessment findings must be evaluated. Likely strategic responses to risk and their performance are aspects that must be fully understood. This process may require separate processes of scenario planning regarding strategic intent.

***4.3.19.3 Identify and evaluate the post-event measures in place for response to risk***

The ability of the University to respond to a risk event must be evaluated in detail and the results recorded as a control in the risk register. Post-event measures include crisis management capabilities, emergency planning, business continuity plans and contingency planning. These responses should incorporate planned measures that cover the basic types of managerial response, such as finance, people, technology and students. The criteria for performance will include speed of response, comprehensiveness of response and degree of readiness.

***4.3.19.4 Review the financial risk protection measures in place to respond to the consequences of risk events***

The University’s financial measures in response to a risk may include an insurance portfolio, self-insurance policies and funds, financial provisions, and operating budgets for the funding of losses or variances. Management must compare the results of the risk assessment processes with the current risk financing arrangements. This will highlight the potential net financial effect of risk events on the University. It will also influence the decisions relating to the structure of risk financing. Certain risks may be deemed intolerable and may require a self-insurance facility or provision to manage the risk. Low risks may lead to greater risk retention limits.

***4.3.19.5 Verify the levels of compliance with regulatory requirements***

Adherence to legislation and regulatory frameworks is not negotiable. It is essential that risk-related requirements are incorporated into control frameworks. Relevant requirements must be verified. It is the responsibility of management to build compliance processes around these requirements. Any material breaches must be reported as deemed appropriate through the appropriate reporting structures.

*Having ascertained the suitability, appropriateness and effectiveness of risk controls, management will decide upon further action plans for actual and possible risks.*

**4.3.20 Take decisions on the acceptability of identified risks and controls**

A distinct and conscious process of decision-making for each key risk must be implemented. The decisions made for every key risk must be recorded. Decision options include the possibility to tolerate, treat, transfer or terminate risks. The potential impact upon strategic objectives will influence the outcomes of decision-making processes.

**4.3.21 Document your action plans for risk mitigation**

The action plans for improving or changing risk mitigation measures must be documented in the risk registers. It is important that a process of tracking progress made with risk interventions is followed. Such a process provides a trail of information that may prove to be necessary in future (good governance practices would expect this). Because risk is often a process of perception, misunderstandings can arise where no record is kept. The action plans must be unambiguous and provide target dates and the names of responsible persons. A process of follow-through must be used.

**4.3.22 Use the outputs of risk assessments for budgeting and capital allocation processes**

It is important that risk information is factored into budgeting decisions. The variability of budgeted targets must be considered, and one must assume that the risks associated with key objectives in the budgets have been evaluated as part of the risk assessment processes. Considerations around budgeting should also be put in the context of cost-of-risk evaluations.

**4.4 Governance requirements**

**4.4.1 Establish an organisational framework of assurance for key risks and controls**

A framework of assurance must be developed for your risks. Key players in the University will combine to provide assurance to the Council that risks are being appropriately managed. This combined approach to assurance normally involves the External Auditors, Internal Auditors and management working together through the Audit and Risk Management Committees. Other experts must be chosen to provide assurance regarding specialised categories of risk, such as environmental management and occupational health and safety management. The assurance framework must be formalized and must incorporate appropriate reporting processes.

**4.4.2 Internal Audit provides assurance that management processes are adequate to identify and monitor significant risks**

The Internal Audit function must examine the techniques used to identify risk. The categories and the scope of risk assessments should be considered. The methodologies used to extract risk information must be reviewed. A consensus view of the University’s risk profile should be apparent. Monitoring processes should be wholly aligned with the results of risk assessments.

The Internal Audit function should particularly seek evidence that the processes of risk identification are dynamic and continuous, rather than attempts to comply with governance expectations.

**4.4.3 The outputs of risk assessments are used to direct internal audit plans**

Internal audit plans depend greatly on the outputs of risk assessments. Risks from risk assessments must be incorporated into internal audit plans according to management and Audit Committee priorities. The risk assessment process is useful for Internal Audit staff, because it provides the necessary priorities regarding risk as opposed to using standardised audit sheets.

The audit activities will focus on adherence to controls for the key risks that have been identified. In addition, Internal Audit staff may direct management towards the need for improved controls relating to key risks.

**4.4.4 Internal Audit provides an evaluation of risk management processes**

The Internal Audit function must verify that risk reports are credible and offer a balanced assessment of risks. It is vital that an institution-wide view of risk management is adopted by the University and the Internal Audit function will examine this. The reliability of risk information, particularly the information regarding controls, should be scrutinised by the Internal Audit function. The Internal Audit function should also work with specialist providers of assurance, where necessary.

**4.4.5 Internal Audit provides objective confirmation that the Council receives the right quality of assurance and reliable information from management regarding risk**

The process of assurance must of necessity involve the Council, the Audit Committee, management, the External Auditors, regulators and the Internal Audit function. The advice of other subject matter experts will also be incorporated into the process of providing assurance.

The Internal Audit function plays a key role in co-ordinating the key players in the risk management process to provide assurance to the Council of TUT. The Internal Auditor is not the only provider of assurance. The function does, however, have an important role in evaluating the effectiveness of control systems.

**4.4.6 Safety, environmental, health and hygiene management**

A formal safety management programme is essential for the University. The risks will vary according to faculties and departments, but the principles of risk management will always apply, i.e. risk identification, risk assessment, formal action plans for mitigation, monitoring, reporting and assurance. The scope of the safety management programme should include administrative aspects, safety awareness and training, health, hygiene, electrical safety, physical safety, micro-environmental exposure and legislative requirements.

**A Risk Ratings**

**Qualitative assessment of potential impact**

The following table is to be used to assist management in quantifying the potential impact that risk exposure may have on the University.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Severity Ranking*** | ***General*** | ***Continuity of Supply*** | ***Safety & Environment*** | ***Technical Complexity*** | ***Financial*** |
| **Catastrophic** | A disaster with a potential lead to collapse/cancellation of the organisation and is fundamental to the achievement of objectives | Risk event will result in widespread and lengthy reduction in continuity of supply to customers of greater than 48 hours | Major environmental damage  Serious injury (permanent disability) or death of personnel or members of the public  Major negative media coverage | Use of unproven technology for critical system/project components  High level of technical inter-dependencies between system/ project components | Significant cost overruns of >20% over budget.  Significant loss in revenue >30% |
| **Critical** | Critical event which can be endured but which may have a prolonged negative impact and extensive consequences | Reduction in supply or disruption for a period ranging between 24 & 48 hours over a significant area | Significant injury of personnel or public  Significant environmental damage  Significant negative media coverage | Use of new technology not previously utilised for critical systems/project components | Major cost overruns of between 10% & 20% over budget  Significant loss in revenue >20% |
| **Serious** | Major events, which can be managed but requires additional resources and management effort | Reduction in supply or disruption for a period between 8 & 47 hours over a regional area | Lower level environmental, safety or health impacts.  Negative media coverage | Use of unproven or emerging technology for critical systems/project components | Moderate impact on revenue, assets base and expenditure |
| **Significant** | Event, which can be managed under normal operating conditions | Brief local inconvenience (work around possible)  Loss of an asset with minor impact on operations | Little environmental, safety or health impacts  Limited negative media coverage | Use of unproven or emerging technology for systems/ project components | Minor impact on revenue, assets base and expenditure |
| **Minor** | Consequences can be readily absorbed under normal operating conditions | No impact on business or core systems | No environmental, safety or health impacts and/or negative media coverage | Use of unproven or emerging technology for non-critical systems/project components | Insignificant financial loss |

**Qualitative assessment of probability of occurrence**

The table below is to be used to assist management in quantifying the probability of a specific risk occurring in the University.

|  |  |
| --- | --- |
| **Probability Factor** | **Qualification Criteria** |
| **Almost Certain** | The risk is almost certain to occur in the current circumstances |
| **Likely** | More than an even chance of occurring |
| **Possible** | Could occur quite often |
| **Unlikely** | Small likelihood but could happen |
| **Rare** | Not expected to happen – Event would be a surprise |

**Qualitative assessment of perceived control effectiveness**

The table below is to be used to assist management in quantifying the perceived effectiveness of controls to mitigate or reduce the impact of specific risks on the University.

|  |  |
| --- | --- |
| **Effectiveness Factor** | **Qualification Criteria** |
| **Very Good** | Risk exposure is effectively controlled and managed |
| **Good** | Majority of risk exposure is effectively controlled and managed |
| **Satisfactory** | There is room for some improvement |
| **Weak** | Some of the risk exposure appears to be controlled, but there are major deficiencies |
| **Unsatisfactory** | Control measures are ineffective |

**B Risk Definitions**

|  |  |
| --- | --- |
| **Risk** | Risks are uncertain future events (threats and opportunities) that could influence the achievement of the goals and objectives of the University. |
| **Risk Management** | Risk management is a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues and opportunities. |
| **Risk Assessment** | The overall process of identifying, analyzing and evaluating risk.  The risk assessment process should consider risks that are significant to the achievement of the University’s objectives. This is a continuous process, requiring regular reviews, as and when internal and external changes influence the University’s strategies and objectives. |
| **Enterprise Risk Management (URM)** | University risk management is a structured and consistent approach across the University that aligns strategy, processes, people, technology and knowledge with the purpose of evaluating and managing the risks (threats and opportunities) that the University faces to create stakeholder value  or  Choices made under conditions of uncertainty, bound by acceptable levels of risk, designed to sustain/maximise shareholder value. |
| **Residual Risk** | Risk after considering the effectiveness of management’s risk responses |
| **Risk Mitigation** | The process of selecting and implementing measures to modify risk (encompasses risk avoidance, risk reduction, risk retention and risk transfer) |
| **Risk Categories** | Grouping of risks with similar characteristics used in establishing the clients risk portfolio (see risk profile). Ultimately determined by the client, the characteristics used to define risk categories typically reflect the client’s business model, industry or other factor that drives risk within the organisation. |
| **Risk Profile** | Identification and listing of risks, typically in order of highest to lowest based on a qualitative or quantitative measurement approved by client management |
| **Risk Strategy** | The approach adopted for associating and managing risks based on the University’s objectives and strategies |

|  |  |
| --- | --- |
| **Risk Appetite** | The amount of risk taken in pursuit of value |
| **Key performance indicators (KPIs)** | Key performance indicators (KPIs) are quantitative measurements, both financial and non-financial, of the process’s ability to meet its objectives and of the process’ performance. They are usually analysed through trend analyses within an organisation or through benchmarking against a peer of the organisation or its industry |
| **Process** | Structured set of activities within an entity, designed to produce a specified output |
| **Impact** | This is the magnitude of the impact on the University should the risk actually materialize |
| **Probability** | This is the likelihood that the risk will materialize |
| **Inherent risk** | This is the product of the probability of occurrence and the severity of outcome, prior to control measures |
| **Hazard** | The source of or exposure to danger |
| **Incident** | An undesired event as a result of a risk behavior, or high-risk conditions, without resulting in loss, but has the potential for losses |
| **Accident** | Undesired event as a result of a risk behavior or high risk conditions resulting in personal injury, property damage and or service delivery interruption |

**C Risk Categories**

The University’s risks are classified within the following broad categories:

* Strategic
* Funding
* Academic Excellence
* Operational
* Reputational (including short learning programmes)
* Infrastructure and Facilities
* Financial
* Human Resources
* Information Technology
* Student Affairs and Residence Operations
* Compliance (Legal and Regulatory)
* Safety, Health and Environmental
* Business Continuity

**D References**

The following documents were used extensively in the drafting of the enclosed guidelines:

1. Enterprise Risk Management Integrated Framework; COSO, 2004; and

2. Enterprise Risk Management Code of Practice, Institute of Risk Management South Africa, 2003.

3. Guide to Enterprise Risk Management: frequently asked questions (Protiviti).

4. King II Code of Corporate Governance, 2002.

1. *1* Adapted from COSO (The Committee of Sponsoring Organisations of the Treadway Commission) [↑](#footnote-ref-1)