Enterprise Risk Management Framework

[FG012]

Department	:	Office of the Vice-Chancellor
Owner	:	Chief Financial Officer
Responsible for update	:	Director: Risk, Compliance & Relationship Management
Prior update	:	New framework, formalising processes & procedures
Approved by	:	Council
Approval Date	:	June 2025

Enterprise Risk Management Framework

[FG012]

Table of Contents

Acronyms

BIA	Business Impact Analysis
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
CFO	Chief Financial Officer
COO	Chief Operating Officer
COSO	Committee of Sponsoring Organisations of the Treadway Commission
DVC	Deputy Vice-Chancellor
ED	Executive Director
ERM	Enterprise Risk Management
ERMF	Enterprise Risk Management Framework
GSB	Graduate School of Business
HR	Human Resources
ISO	International Organisation for Standardization
VC	Vice-Chancellor
King IV	A report on corporate governance issued by the King Committee
LL	Leadership Lekgotla
KRI	Key Risk Indicators
PASS	Professional, Administrative Support Services (Staff)
RMEC	Risk Management Executive Committee
SWOT	Scenario analysis or strengths, weaknesses, opportunities, and threats
SWS	Student Wellness Service
UARC	University Audit and Risk Committee
OHSE	Occupational Health, Safety and Environment
POPIA	Protection of Personal Information Act
SARS	South African Revenue Services
LPG	Liquefied Petroleum Gas
UARC	University Audit and Risk Committee
UB&DC	University Building and Development Committee
UHRC	University Human Resource Committee
UCT	University of Cape Town

1.Introduction

Risk significantly influences all aspects of the university's operations and activities. Therefore, it is imperative that risks are effectively recognized and managed to mitigate any adverse consequences. Conversely, risks can also present opportunities for development and innovation. By comprehending these risks, the university can make informed decisions regarding its activities and potential opportunities. Through a structured risk management process, the university can not only minimize the impact of the consequences of the risk but also enhance operational efficiency.

Effective risk management cannot be implemented in isolation but must be integrated into existing decision-making structures and processes. The risk management framework is a living document that will evolve over time as the university continues to advance and mature its risk management processes and culture. The framework provides guidance on the university's philosophy and approach to risk management as a solid foundation for strategic planning aimed at achieving strategic, operational compliance, and reporting objectives. As risk management is an integral component of sound governance, integrating the risk management function into existing strategic management and operational processes will ensure that it is an integral part of the university's daily activities. The framework advocates for the integration of risk management into a business process that encourages all university stakeholders to be risk-aware and assist in the management of these risks.

The university is committed to the optimal management of risks to achieve its vision, mission, and objectives. The management of risks is done through an ongoing process by identifying, evaluating, and monitoring of strategic and operational risks and opportunities. The enterprise risk management framework will be embedded in the governance and control systems of the university processes to ensure that the organisation's response to risk remains appropriate, current, and dynamic in line with its risk appetite and tolerance levels.

2.Purpose of the framework

The overall purpose of risk management at the university is to ensure that the university uses its capabilities and resources efficiently and effectively to manage both opportunities and threats. Threats includes any damage that could put the university's operations in danger, and failure to take advantage of opportunities that could help the university achieve its objectives in the best way possible.

The framework is in support of the Risk Management Policy and will assist in an integrated enterprise-wide risk management approach that is set to proactively identify various categories of risk at the earliest opportunity to implement appropriate solution to manage the risks efficiently and effectively.

This framework outlines the link to the methodology (used techniques and tools), processes and procedures for effective risk management by promoting proactive risk management as a central component of good corporate governance and an integral part leading towards effective combined assurance. The framework also defines the roles and responsibilities of governance structures, including key committees, management, and the process for coordinated risk management to promote a sound risk culture.

3.Objectives of the framework

To meet the university's strategic goals, Council and Management must develop rigorous, structured, and effective risk management processes across the institution. The enterprise risk management framework is developed to:

- Assist management in the pursuit of academic, research and business objectives through transparent identification and management of risks and identification of potential opportunities.
- Encourage initiative-taking risk-based decision-making through an appropriate culture of integrity and risk awareness.
- Guide the university's risk management processes; and improve operational efficiency and effectiveness.
- Increased probability of achieving objectives through enterprise-wide risk management while assisting with the overall performance of the institution
- Establish a common risk language and direction related to risk management by establishing open communication with respect to risk and risk tolerance.

4.Scope of the framework

The framework applies to all staff, students, and entities of the university. The framework extends to all current and future activities, potential opportunities and business dealings involving the university.

5. Context and understanding of the university and its operations

The university mission and objective are

(i) primarily teaching and learning,

(ii) research and

(iii) community engagement as outlined in the higher education's act.

In pursuit of these objectives, the university aims to ensure that it remains economically, financially, and environmentally sustainable. In addition to these three key objectives, the university has several commercial activities all aimed at generating a return on investment to support its overall mission and objectives.

The governance of the university is the responsibility of Council and is accountable for the governance of risk through formal processes including the process of risk management. King IV requires Council to demonstrate that it has dealt with the governance of risk comprehensively. Principle 11 of the KING IV report states that, "*The governing body should govern risk in a way that supports the organisation in setting and achieving its strategic objectives*". Council is responsible for the university ERMF and the oversight of its operation by management. The day-to-day management of the university is led by the Vice-Chancellor, supported by the Executive (Deputy Vice-Chancellors, Registrar, Chief Financial Officer, and Chief Operating Officer). The Deans are responsible for the management of their respective faculties (academic departments and operations). The Deans are supported by the Heads of Departments and Heads of Divisions. Executive Directors and in some departments, directors oversee the operations of professional and administrative departments.

The decision-making in the faculties and departments are outside the remit and authority of the Vice-Chancellor in line with the devolution powers of the Deans and Executive Directors. In the decision-making process, the political, social, economic, legal, and physical environments are important in the day-to-day activities of the university. It is also essential that the internal and external environment within which the activities are conducted is considered given that the university is publicly funded but also generates its own funding from its teaching and learning activities and research.

6.Risk management approach and process

There are various steps in the risk management approach and process which entails: communication and consultation, risk identification, risk assessment, risk evaluation, risk mitigation risk monitoring and review as well as risk recording and reporting. Key in risk management is the importance of ongoing and structured communication through the process. It is essential to communicate and consult with stakeholders at each step in the risk management process in development of risk registers. Refer to ***Appendix A***.

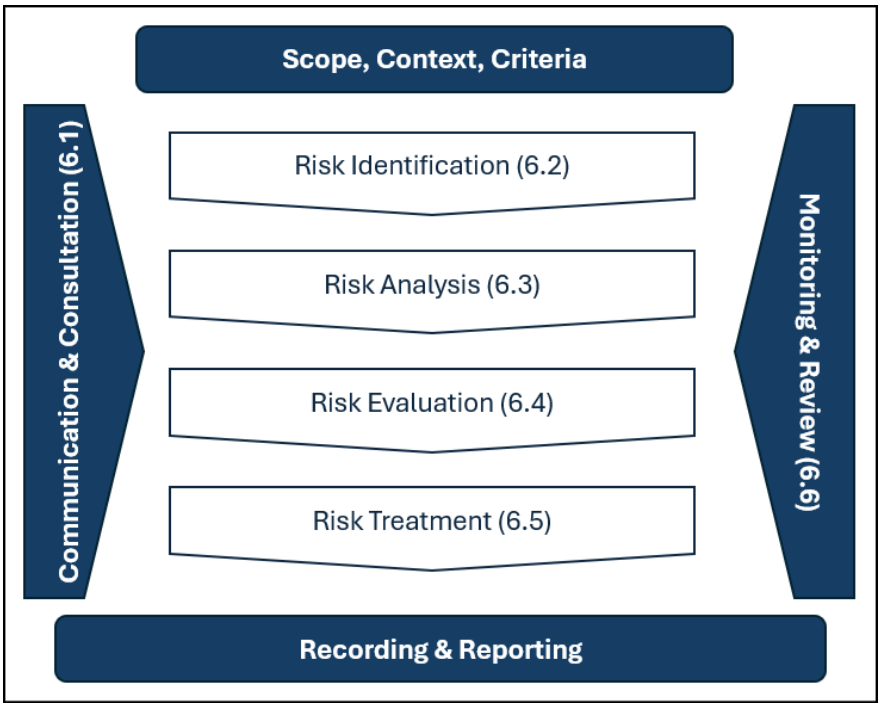

Figure 1: Risk Management process and steps

6.1 Step One: Communication and Consultation

The objective of communication and consultation is to raise awareness of the enterprise risk management across all levels of the university. Proper risk management requires structured and ongoing communication and consultation with those affected by the university's operations. The communication will seek to promote awareness and understanding of risk and the means to respond to it, whereas consultation will involve obtaining feedback and information to support decision-making.

6.2 Step Two: Risk Identification

Risk identification involves examining all sources of risk and the perception of all stakeholders, both internal and external, to develop a list of risks or opportunities which may impact on the achievement of objectives identified in the context. Risks can be internal or external to the

organisation, and the causes and implications of the risk could involve other entities with connections to the university that are abroad, as well as the wider community.

Risk identification should be a major consideration in the planning and budgeting processes at all levels in 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.

Risks, risk ratings, and key risk indicators (KRI) are identified using a variety of methods, including workshops, seminars and brainstorming sessions, consultation of similar industries, and the review of risk publications and resources for existing and emerging risks.

When identifying risk, it is important to consider it in the context of the related objective. What could happen that might impact on the success in achieving the objective and the reasons. What types of losses could occur and what kind of opportunities that are not covered. The goal of ERM is not only to look at the negative side of risk, but also the potential upside of taking a risk.

6.3 Step Three: Risk Analysis

Risk analysis involves a qualitative and/or quantitative assessment of the identified risks. Identified risks are to be rated to determine which are the most critical. The first step is inherent risk rating which is the exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors. The university has a template which is used for this process. Refer to ***Appendix B*.**

Effective ERM requires information to be obtained from all levels of the university for identifying, assessing and responding to risk. Consultation will be as broad as possible within the university community and use a variety of approaches. university personnel will be encouraged to identify risks that are both internal and external to the institution There are several ways in which risks can be identified including physical inspections; brainstorming, interview or focus group discussions, personal experience or past university experience, scenario analysis or strengths, weaknesses, opportunities, and threats (SWOT) analysis.

6.4 Step Four: Risk Evaluation

The purpose of risk evaluation is to comprehend the nature of the risk and its characteristics including, where appropriate, the level of risk. The university has a defined risk scoring formula that is utilised to evaluate the risks. Analysing the identified risk requires an assessment of impact and likelihood outcomes if the risk were to materialise. This enables each of the identified risks to be consistently rated across the university, so that the risks can be appropriately compared, and any required action can be prioritised. Refer to ***Appendix C.***

The evaluation of each risk should take into consideration current controls. Residual risk is the remaining level of risk following the development and implementation of the entity's response. Risk evaluation entails a consideration of the effectiveness of current controls to determine if they reduce the probability and/or severity of a risk. The effectiveness of controls considers key risk indicators, industry standards, benchmarking as well as audit results. Residual risk ratings are calculated by taking the inherent risk rating and discounting them to reflect the effectiveness of controls that are in place. Refer to ***Appendix D.***

6.5 Step Five: Risk Mitigation or Response

The fourth step of the process is the reduction (mitigation) of identified risks which has three aspects, planning, implementation, and progress monitoring. Once the risk has been assessed and controls have been identified there are five actions. Risk response for identified risks will be assessed according to the university's risk appetite. Risk treatment typically involves one or a combination of the strategies. The five possible risk responses are to:

- ***Accept*** the risk and make a conscious decision not to take any action. This option is frequently accompanied by a contingency plan for dealing with the impact that will arise if the risk is realised.
- ***Accept*** the risk but take some actions to lessen or minimise its likelihood and/or potential impact.
- ***Transfer*** the risk to another individual or organisation; for example, outsource the activity through contractual arrangements or partnerships. If this route is chosen, then care needs to be taken to ensure that the risk is transferred. It is important that how (and to whom) the risk has been transferred is recorded in the template.
- ***Finance*** (insure against) the risk. Be sure to record the need for insurance in the template as the university's insurance policies are updated annually and subject to change.
- ***Eliminate*** the risk by ceasing to perform the activity giving risk to the risk.

6.6 Step Six: Risk Monitoring and Review

With the ever-changing risk landscape of universities, it is vital that risk management be a continuous process. Risks must be monitored to ensure they do not increase in severity and/or probability, and that emerging risks are identified and addressed. Risks need to be monitored periodically to ensure changing circumstances do not alter the risk priorities. Few risks remain static – change may be sudden, or gradual and persistent. Factors that may affect the likelihood and consequences of a risk may change, as may the factors that affect the sustainability or cost of the treatment options.

Responsibility and accountability for monitoring and reviewing risks identified in strategic, operational and programme or project risk registers lie with risk owners, management, and governance structures. It is the expectation of Council that any strategic risks are brought to its attention of the university Audit and Risk Committee and/or portfolio by management.

Ongoing reviews of strategic and operational risk registers will be facilitated by the Risk Office, as well as an annual detailed review for all risk registers (both strategic and operational) to ensure risks and controls are still current and to ensure new or emerging risks have been identified. More frequent reviews of all strategic risks and remarkably high and high operational risks will occur, with a particular focus on progress of treatment plans.

6.7 Step seven: Recording and Reporting

The process of documenting the identified risks, their potential impacts, and the mitigation strategies put in place, then communicating this information to relevant stakeholders through a structured report, allowing for informed decision-making and effective risk management within the university.

The end results of ERM are to provide the management and Council with a regular risk profile for strategic and operational risk management in line with ISO 31000:2018.

COSO Enterprise Risk Management – Integrating with Strategy and Performance (update): 2017

The Framework itself is a set of principles organized into five interrelated components:

The five components in the updated Framework are supported by a set of principles.[4] These principles cover everything from governance to monitoring. They're manageable in size, and they describe practices that can be applied in different ways for different organizations regardless of size, type, or sector. Adhering to these principles can provide management and the board with a reasonable expectation that the organization understands and strives to manage the risks associated with its strategy and business objectives.

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Source: COSO Enterprise Risk Management—Integrating with Strategy and Performance

The COSO Framework is a system used to establish internal controls to be integrated into business processes. Collectively, these controls provide reasonable assurance that the organisation is operating ethically, transparently and in accordance with best practices and established industry standards.

To achieve the maximum benefit through its ERM activities, Council will use strategy and objective setting for both a Risk Management framework and a Performance Management Framework as each framework has a dependency on the other. There are clear overlaps in the frameworks. Strategic risks can be reduced by better managing its performance; and its performance can be improved by better managing its risks. There are synergies between both frameworks that need to be taken advantage of, and the performance management framework

should recognise this need and provide high-level detail on risk from a performance management perspective.

7.Types of risks that the university faces

There are diverse types of risks which the university faces with the responsibility and accountability of these risks based on ownership. The university community is responsible for recording and reporting emerging risks. Institutional risks must be reported to the ERM department and Risk Owners for review to determine the impact on the university. These risks are threats or opportunities that are perceived to be potentially significant to the university but may not be fully understood and assessed.

7.1 Strategic or Institutional Risks (External Environment)

Categories	Characteristics of the external environment
Political	The nature and extent of university intervention - tax policies, labour/ environmental laws, trade restrictions, tariffs, political stability.
Economic	Interest rates, inflation, foreign exchange rates, availability of credit, NSFAS effectiveness and liquidity.
Social	Customer needs or expectations; population demographics, such as age distribution, educational levels, distribution of wealth.
Technological	Digitalization and rate of technological changes or disruption, research, and development initiatives around technology.
Legal	Laws (employment, consumer, health, and safety), regulations and industry standards, ESG.
Environmental	Natural or human-caused catastrophes, ongoing climate change, changes in energy consumption regulations, attitudes toward the environment.

The university maintains a strategic risk register that identifies key strategic risks. This is maintained, formally reviewed regularly, and reported to the UARC meetings. The strategic risk register is owned by the Vice-Chancellor with the support of the Executives. The register captures critical organisational wide risks which link directly to the strategic objectives.

7.2 Operational Risks (Internal Environment)

Categories	Characteristics of the internal environment
Capital	Capital and operational assets, equipment, property, patents.
People	Knowledge, skills, attitudes, relationships, core values and culture.
Process	Policies, or procedures; changes in management, operational and supporting processes.
Technology	New, amended, or adopted technology, artificial intelligence, robotics.

Operational risk registers capture the risks at faculty and departmental levels considering internal environmental characteristics as per the above table using a SWOT analysis model and operational categories as per above table.

Project risks associated with programmes or projects that are of a specific medium or short-term in nature. These risks are associated with new teaching and learning courses, significant new research, or acquisitions, change management, integration, major IT and capital development activities.

Risks associated with programme or project management are normally delegated to programme directors or project managers for attention and action. Included among the benefits of efficiently managing programme or project risks are the avoidance of unexpected time and cost overruns. In addition, when project risks are well managed, there are fewer integration problems with assimilating required changes back into general management functions. How the university decides to manage individual risks is determined following a risk assessment based on a systematic analysis of several impact (or consequence) and likelihood ratings to each risk.

While some risks are easy to identify and measure than others, some are not as easy and apparent. Emerging risks are defined as new risks or familiar risks that become apparent in new or unfamiliar conditions. Emerging risks may include political or policy changes from funders, innovative technologies as well as economic, societal, environmental, or regulatory change. When emerging risks are identified, often key information is still unclear or unavailable to undertake a full risks assessment.

8. University Risk Management Appetite and Tolerance levels

Risk appetite is the amount of risk the university is willing to accept to achieve its objectives, in accordance with the set risk tolerance levels. Risk appetite is about taking risks and risk tolerance is about controlling those threats. Risk appetite provides an important, forward-looking perspective and is a guide to risk management activities when determining the assumptions of risk is acceptability and tolerance levels.

The university's Executive and Leadership Lekgotla will play a leading role in determining its risk appetite and tolerance and make the appropriate recommendations to Council. The university acknowledges that in different areas, the nature of risks it faces will vary; normally arising from either threat posed, or because of pursuing opportunities. In turn, the level of exposure carried by different activities will vary, and its threshold for accepting varying levels of risk will change depending on the risk area under consideration, along with its strategic objectives, the subsequent activities undertaken, and the projected benefits.

The risk appetite and tolerance will reflect the University's mission and vision, considers stakeholder expectations, and in turn, has an influence on both the culture and operations of the university. The risk appetite and tolerance must consider that the university is publicly funded (first income stream) and generates income through tuition and residence fees (second stream). In addition, the university generates research and commercial income through entrepreneur activities.

8.1 The university risk appetite and tolerance statement

The risk appetite statement, while providing useful guidelines about the university's appetite for risk, does not address tolerance and treatment levels for each risk, particularly those that are at the strategic level. Experience shows that the university has a high appetite for risk in the context of encouraging and promoting teaching and learning, research development, academic freedom, open debate and critical enquiry.

8.2 Risk Appetite and Tolerance Summary

The following table demonstrates the types of threats and opportunities that may inform the tolerances within the risk appetite on the current environment that runs from conservative (Low appetite to innovative (high appetite) view of risk.

Risk Appetite and Tolerance Summary					
			Low Appetite	Moderate Appetite	High Appetite
					
			Zero tolerance or accept a cautious (low) approach towards taking risk	*A balanced and considered approach is adopted in taking risk*	*An assertive approach to taking risks is accepted to realise strategic objectives.*
9.1	Teaching and Learning	Administration	x		
		Teaching Methods		x	
9.2	Research	Research Ethics & Compliance	x		
		Research Innovation		x	
9.3	Cyber and Information breaches		x		
9.4	Human Capital		x		
9.5	Disruption to the university operations		x		
9.6	Environmental risks		x		
9.7	Fraud and corruption risk		x		
9.8	Governance and compliance risks		x		
9.9	Finance	Financial	x		
		Commercial		x	
9.10	Health, Safety and security risk		x		

The university's risk appetite statement is broadly articulated for key activities aligned to the university's risk categories, which enable the achievement of its strategic and operational objectives. This will be an ongoing and iterative process, noting that the university's appetite for risk across such areas will evolve over time. In turn, the university's application and use of risk appetite will likewise evolve as it goes through different stages of maturity. The following broad principles will apply:

- *Low Appetite* - The University will have a low appetite for risk where the probability for regret is high because there is a likelihood of harm to students, staff, visitors or other stakeholders; significant reputational damage; financial damage; non-compliant or unethical conduct or consequences.
- *Moderate Appetite* - The University will have a moderate risk appetite for risk where a balanced level of risk, neither highly aggressive no low risk i.e. overly cautious in pursuit of the University goals while specifying an acceptable percentage of potential risks. These can include characteristics like balanced approach, calculated risks, diversification and acceptable losses.

- *High Appetite* - The University will have a high appetite for risk in respect of strategic growth, teaching innovation and research initiatives. To achieve this, it will endorse and promote award-winning research and innovative teaching programmes in fit-for-purpose facilities that attract world class students and staff.

9.Risk categories for the University

There are various categories of risks that the university faces (the list is not exhaustive) with the focus on the key ones.

9.1 Teaching and Learning Risks

The core function of the university as an academic institution is teaching and learning. This is done through innovative curriculum at the cutting edge of disciplines and professions, facilitating students' engagement with their own learning, offering socially engaged curriculum and top-end digitally enabled education at undergraduate, postgraduate and continuous education levels.

9.2 Research Risks

The second core function of the university is research. Risks related to research are two-fold: ethics & compliance and innovation. There are risks related to the university not meeting all aspects of the national and international compliance requirement of its OHS landscape including specialised areas such as complaint laboratories, and biosafety. This has significant legal risks as well as knock-on effects for research funding and reputation. Similarly, a university that does not innovate in terms of the research it does risks becoming stagnant and obsolete. This also poses significant risk for its funding and standing, both nationally and internationally.

9.3 Cyber and Information breaches

Cyber security threats are dramatically on the rise globally and the sophistication of attacks. This dramatic change is founded on the increasing move to online presence, adoption of cloud, machine learning and emerging technologies.

9.4 Human Capital Risk

The most important asset of the university is its people. The lack of an integrated workforce planning, talent identification, and retention is an ever-present risk. Complex policies, delegations of authority and multiple stakeholder interdependencies in staff recruitment which slow down decision and offer making and communication processes.

9.5 Disruption to the university operations

The continuity of business may be compromised due to various kinds of disruptions: this may include disaster recovery processes not fully developed nor at a required level of maturity. Other disruption related risks may include non-optimal uniform plan and implementation of a business continuity plan across multiple academic and operational units. To remain competitive, the organisation must be prepared to manage both external and internal forces of disruption. External forces of disruption are strategic factors that arise from outside the organisation, such as technological advancements, changes in customer preferences, and global events. On the other hand, internal forces of disruption are factors that arise within the organization itself, such as organizational culture, leadership, and business processes.

9.6 Environmental risks

Currently the only legally required reporting on climate related matters is related to the carbon tax regulation, which currently only applies to stationary fossil fuel combustion [diesel generators and Liquefied Petroleum Gas (LPG)]. Some donors already require more intensive reporting. Growing awareness of climate change, resource scarcity, and social inequality drives businesses to adopt more sustainable and socially responsible practices, impacting their operations, supply chain, and brand reputation.

9.7 Fraud and corruption risk

The strategy is designed to prevent, to deter and to detect fraud during the university's daily business operations. However, fraud and corruption are an ongoing risk which require constant improvement in the internal controls.

9.8 Governance and compliance risks

It is crucially important that Council, Senate, the executive, management and staff adhere to good governance practices. This requires adherence to legislative and regulatory requirements (including for example OHSE and POPIA), university policies and appropriate standards of best practice. Risks of non-compliance include legal liability, reputational harm and may affect the legality and/or efficiency of decisions and operations.

9.9 Financial and Commercial Risks

The University's financial sustainability relies primarily on three key sources of income: government subsidies (comprising block and earmarked grants), student fees, and designated research funding from third-party sources. These revenue streams are supplemented by private and commercial funding to support the institution's broader operations.

This financial structure exposes the University to a range of financial and commercial risks that may affect its long-term operational viability and financial health. Notable risks include changes to government funding policies, sociopolitical movements related to student affordability (such as #FeesMustFall), failure to comply with the terms and conditions attached to specific funding allocations, and the inability to achieve enrolment or performance targets.

9.10 Health, Safety and security risk

The university operates on an open campus, which inherently poses a persistent security risk. Potential risks to individuals directly affected by the ongoing work being conducted at the university.

10. Risk management communication and key principles

Risk communication is the process of sharing information to help others make better decisions. Risk management communication and principles are intended to make the risk management processes more efficient and effective. Risk communication is the responsibility of everyone involved in the project. It is an interaction of both parties to exchange information to better understand what each stakeholder needs.

10.1 Risk communication and engagement

Communication and consultation with stakeholders are an integral part of the risk management process for the university. Having a clear and effective governance structure, policy, reporting framework, and tools to convey risk assists with communication and consultation.

The continual communication and consultation with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance is part of good governance. Communication and consultation with external and internal stakeholders are key in the stages of the risk management process. Formal internal communication channels must be established and all information related to the risk management implementation needs to be communicated and shared with all stakeholders.

10.2 Risk escalation process and triggers

Risk acceptability	Escalation and management actions
Unacceptable	Immediate escalation of risk to the Executive Management for prioritisation and appropriate risk response. Management must take action to reduce risk exposure (with highest impact priority) to an acceptable level and constantly monitor the risk exposure and the effectiveness of related controls. Management must review (on regular basis) progress/status of the risk response. Ongoing UARC oversight required.
Cautionary	Escalation of risk to responsible Risk Owner for prioritisation and appropriate risk response. Risk Owner must take action to reduce risk exposure (with medium-to-high impact priority) to an acceptable level. Cost-befit analysis is required to determine if risk treatment is feasible. Risk Owner must constantly monitor risk exposure and effectiveness of related controls and review (on monthly basis) progress/ status of the risk response. Ongoing RMEC oversight required.
Acceptable	Risk Owner must control the risk exposure within an acceptable level and the risk through existing controls and normal operating procedures. Risk Owner may consider reducing the cost of control and treat only when resources are available. Risk Owner must constantly monitor the risk exposure and the effectiveness of related controls. Risk Owner must review (on monthly basis) progress/status of the risk response. Ongoing Vice-Chancellor level oversight required.

Risk escalation is the process of informing and involving the appropriate people or parties who have the authority, responsibility, or influence to deal with a risk that is beyond the control of the project team or the initial risk owner. Risk escalation can be proactive or reactive, depending on whether the risk is anticipated or realised. Risk escalation can also be formal or informal, depending on the communication channels and protocols used. The aim of risk escalation is not to negate the responsibility for risk management of individuals, management, or committees but rather to ensure proper risk treatment.

The escalation process is affected when an individual who has been assigned responsibility for a risk fails to advance, to manage or to supply relevant assurances that the risk will be adequately mitigated within a reasonable time as recorded in the risk register. This process will be followed through incident management procedures where the identified risk has materialised, and the risk owner has responded inappropriately or failed to respond appropriately to the risk.

Risk appetite limit (upper and lower) is the level of risk that, if breached by the university's risk profile, would necessitate immediate escalation and corrective action. Risk appetite trigger is the level at which escalation occurs to a higher forum, committee, or level of authority because the risk profile is sufficiently close to the risk appetite limit for corrective action to be considered. It serves as an early warning indicator.

Failure to respond appropriately to the identified risks should trigger a risk escalation. The objective of escalation is not to negate the responsibility for risk management of individuals or committees but rather to ensure proper risk treatment. The escalation process is affected when an individual who has been assigned responsibility for a risk fails to advance, to manage or to supply relevant assurances that the risk will be adequately mitigated within a reasonable time as recorded in the risk register. This process will be followed through incident management procedures where the identified risk has materialised, and the risk owner has responded inappropriately or failed to respond appropriately to the risk. The RMEC has approved a risk escalation template that should be used for all risk escalations.

10.3 Reviewing and updating of the risk register at appropriate intervals

Risks that have been identified on the strategic risk register, faculty, department /or at a project level and consolidated into a risk register must be updated and reviewed regularly. The strategic risks are reviewed at least twice a year and presented to the relevant governing structures. Faculty, departmental and project risk registers must be reviewed and updated at least annually. Risk champions will play a significant role in review and updating of all risk registers, but it is key that risk management is part of the daily activities of each faculty and department. At a strategic level, the top risks are discussed at every RMEC and UARC meetings. Faculty and departmental risks must also be discussed at the faculty and management board meetings.

10.4 Risk controls

Every risk will have several controls, mitigations or interventions that have been designed to contain the potential impact or likelihood of the risk. These controls need to be identified and evaluated.

Control Activities include the policies, procedures, reporting and initiatives performed by the university to ensure that the desired risk response is carried out. These activities take place at all levels and functions of the university. Controls are then assessed and rated for their overall effectiveness in mitigating the risk using the Risk Assessment Matrix. Controls are defined as any action currently in place to manage a risk, usually to lower it. Examples of controls could be to establish a procedure or a policy or establish quality checks and reporting, which all may be useful, for example, for a risk related to incorrect payments being made. The controls should address the causes of the risk.

There are several types of controls that can be used. Using a range of types of controls is recommended to reduce the risk more effectively and efficiently. Please see below explanation of the various categories of controls:

Directive controls are designed to encourage desired behaviours and outcomes – as such, they can reduce both the likelihood and impact of the risk including among others training and supervision. policy and procedure documents, guidelines and other manuals and position Descriptions

Preventative controls are designed to limit the possibility of an undesirable event from happening – as such, they reduce the likelihood of the risk, e.g. –access controls (either physical or system access), authorisation procedures, separation of duties.

Detective controls detect the occurrence of an undesirable event – as such, they also reduce the likelihood of the risk and checking / monitoring of exception / error reports Quality Assurance checks e.g. checking for consistency in assessments

Corrective controls are designed to restore normality after the occurrence of an undesirable event, these controls can reduce the impact of the risk: Based on the information received on the strength and effectiveness of the controls in mitigating the

risk and the overall rating of the controls, the impact ratings used to form the inherent risk rating, and the likelihood rating are re-rated.

10.5 Risk mitigations for the University

The university has identified three risk domains:

- **Risks associated with teaching and learning:** These risks are managed through academic structures of the university such as Senate, the regular external reviews of academic departments, the Quality Assurance Working Group, Faculty Examinations Committees, and the internal audit department which tests aspects such as the integrity and quality assessment of exams systems.

- **Risks associated with research:** These risks are managed through the academic structures of the university such as Senate, the university Research Committee, Research Ethics committees (for humans and animals), insistence on external peer review of research; and

- **Operation and business risks:** These risks are managed by the university leadership with oversight from RMEC and UARC.

11. Roles and responsibilities of key stakeholders

Effective risk management requires clear lines of responsibility and accountability. Every university staff member has an active role to perform in establishing and maintaining a robust risk management culture and process. However, there is added fiduciary and management responsibilities on some key stakeholders responsible for oversight, guidance and advice on risk management.

ERM Internal Stakeholders	Key ERM Roles and Responsibilities
Council	• Provide governance risk management philosophy and direction by ensuring that the university has a robust and comprehensive system of risk management. • Setting the tone and influencing the culture of risk management and the retains responsibility for risk oversight.
University Audit and Risk Committee (UARC)	• The Audit Committee is responsible for reviewing the university's risk management framework and for recommending it for approval by the Council. • Provide risk management oversight and control. • Monitor effectiveness of the risk management framework and process and ensure corrective action is taken. • Review ERM framework and process deficiencies and enhancements.

	• To review the external auditors' management letter, the internal auditors' annual report and management responses.
Executive Management	• Ensure integration of risk management into strategic and objective setting, ongoing measurement and key decision making • Issue risk management directives. • Top-down risk management communication.
The Leadership Lekgotla (LL)	• Responsible for taking appropriate risks within the risk appetite approved by the Council to create value. • The Leadership Lekgotla (LL) is responsible for taking appropriate risks within the risk appetite framework approved by the Council to create value. • Responsibility for overseeing key risk management controls, including but not limited to financial and management accounting, property, insurance purchasing, contractual liabilities, business continuity, people related, operational risk controls, and assessment of strategic risk within their areas of responsibility.
Risk management Executive Committee	• Overall ownership of ERM framework. • University-wide risk management co -ordination, collaboration, and reporting. • Central point of focus for ERM framework deficiencies and enhancements. • Key areas requiring the attention of the RMEC include: - The safety and welfare of all people employed (including third parties) and study at or for the university. - The integrity of the university's academic and administrative work. - All risks to which the university is exposed to including strategic and operational risks. - The appropriate use and safeguarding of material assets; and any other risks associated with the activities of the university.
Deans and Senior Management	• Set departments/faculties risk management strategy. • Provide University risk management oversight and guidance. • Monitor effectiveness of risk responses/mitigation
Other Council committees and structures	• Finance Committee whose primary role extends to ensuring a financially sound, viable and sustainable university and to consider the UCT financial strategy for recommendation to Council. • The university Building and Development Committee (UB&DC) reviews key risks and recommends to Council on physical development and oversees major capital projects. • The university Human Resource Committee (UHRC) reviews key risks and recommends to Council on Human Resource (HR) policies, employment equity policy and plans, staff issues, staff concerns and labour laws. • The UHRC manages the risks relating to outsourcing of certain functions and monitors the compliance of outsourced service providers to the agreed code of conduct. • The university Student Affairs Committee (USAC) reviews key risks and advise the Council on student related matters.

Internal Audit	• Regula audit reviews of the University according to the approved plan by UARC. • Provide professional independent review of key risks, controls where required. • Perform an independent evaluation of the effectiveness of the ERM process. • Responsibilities of Internal Audit in risk management include: - Providing assurance that the risk management culture in the entity is an appropriate one. - Providing assurance that the risk register is an appropriate reflection of the risks facing the University. - Providing assurance that risk management is carried out in a manner that benefits the entity; and - Providing assurance that the risk management framework, risk management implementation plan and fraud risk management plan have been effectively implemented within the entity. - Risks are appropriately identified and managed.
External Audit	• Provide additional assurance on the design and operating effectiveness of the university's risk management. This includes external consultants, accreditations, regulators, etc. Provide an independent assessment of a company's financial statements and internal controls.
Risk Office	• Responsible for developing, communicating, coordinating, and monitoring the university enterprise process and management activities. • The Risk Office assist RMEC in fulfilling its responsibilities in accordance with its terms of reference. • The Risk Office develops and revise a methodology and framework for Enterprise Risk Management (ERM) for approval by governing structures. Additionally, it will conduct reviews of the risk management process to enhance its effectiveness. • Maintenance and monitoring of strategic risk register. • Assist with the development of operational and project risk registers.
Risk Owner	• Ensures that approved risk responses to identified risks are effectively implemented.
Risk Champions	• Responsible for coordinating, reporting on and monitoring the risk management process. • Have a duty to escalate instances where risk management efforts are being hampered. • Provide guidance and support when it comes to managing "problematic" risks of a transversal nature that require a multiple participant approach and liaise with the Directorate: ERM in all activities relating to risk management.
All Staff	• Cognisance of operational and strategic risks including identification and reporting of increasing risks or new risks.

12. Related policies, guidelines and forms

- The Fraud and Corruption Prevention Policy and Response Plan
- UCT Statement of Values
- Risk Management Policy (GEN007)
- HR policies and conditions of service - disciplinary procedures (in full)
- university Student Disciplinary Tribunal procedures and guidelines
- Finance policies, guidelines, and related practice notes
- ICTS policies and guidelines
- • Research Integrity policies
- Policy on Conflict of Interests
- Whistleblowing Guideline/Policy
- Supplier Code of Conduct; and all other university policies
- The Protected Disclosures Act No 26 of 2000, as amended by Act No 5 of 2017
- Labour Relations Act
- Higher Education Act (101 of 1997) and Regulations for Reporting by Public Higher Education Institutions
- Prevention and Combating of Corrupt Activities (Act 12 of 2004)

13. References

- COSO framework
- Several ERM policies from other universities (local and international)
- ISO 31000: 2018 Risk Management

14. Contacts

Risk Management Office

riskoffice@uct.ac.za

Director: Risk, Compliance & Relationship Management

Shai Makgoba

021 650 2754

Manager: Risk & Compliance

Zonke Mbaru

021 650 5025

15. Definitions of key concepts

Risk Term	Definition / Meaning[1]
Combined assurance	Good corporate governance practice integrating and aligning assurance processes to maximise governance and risk oversight and control efficiencies and optimise overall assurance to the university Audit and Risk Committee, considering the University's risk appetite. A combined assurance model incorporates and optimises all assurance services and functions so that, taken as a whole, these enable an effective control environment, support the integrity of information used for internal decision-making by management and its committees and support the integrity of the university 's external reports.
Control	Any action taken by management to manage risk and increase the likelihood of the university achieving its objectives. Controls include any plan, process, framework, device, practice or other actions which modify risk and organise and direct the performance of sufficient actions designed to provide reasonable assurance regarding the achievement of objectives.
COSO ERM Framework	'ERM Framework: Integrating with Strategy and Performance' - published by The Committee of Sponsoring Entities of the Treadway Commission (COSO) in 2017.
Enterprise Risk Management (ERM)	The culture, capabilities and practices integrated with strategy and execution that university 's rely on to manage risk in creating, preserving, and realising value. at organizations rely on to manage risk.
Event	Occurrence or change of a particular set of circumstances. An event can be one or more occurrences and can have several causes. An event can consist of something not happening. An event can sometimes be referred to as an "incident" or "accident".
Impact	The potential effects and consequences that a given event could have on the university and its strategic and/or operational objectives. An event can lead to a range of consequences differing in nature, overall size, value, etc. A consequence can be certain or uncertain and can have positive or negative effects on objectives.
Inherent risk	The risk to the university in the absence of any actions management might take to alter the risk's likelihood or impact (i.e., in the absence of controls and mitigation strategies). Inherent risks may result from the UNIVERSITY's strategy and/or external factors.
Internal control review	Overall assessment of the UNIVERSITY's internal control system across all departments (business units) to determine if it is working as intended and if it can manage the risks the university might face daily. The term can refer to the review of a small subset of controls, such as those around a specific process or processes.
ISO 31000	'Risk Management - Guidelines: ISO 31000:2018' – published by the international university for Standardization (ISO) in 2018.
King IV™ Code	King IV™ Code on Corporate Governance – included as Part 5 of the 'King IV Report on Corporate Governance™ for South Africa' – published by the Institute of Directors South Africa (IoDSA) in 2016.
Likelihood	Probability (possibility or frequency) of a given event materialising or occurring.
Residual risk	Amount of risk that the university is exposed to after controls and mitigation strategies have been implemented. Residual risk comprises acceptable risk and unidentified risk. Management must decide whether this residual risk is within the university 's risk appetite. Residual risk is known as "retained risk".
Risk	The possibility of an event occurring that will influence the achievement of a university 's strategic and/or operational objectives. An effect is a deviation from the expected (positive and/or negative). Objectives

[1] Definitions and meanings for risk terms are sourced from the COSO ERM Framework (2017), ISO 31000 ERM Standard (2018) and King IV™ Code on Corporate Governance (2016).

Risk Term	Definition / Meaning[1]
	can have several aspects (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic University-wide, project, process and activity).
Risk analysis	Risk analysis looks at the strengths and weaknesses of existing systems and processes designed to help control the risk. Knowing what controls are already in place and whether they are adequate and/or effectively helps to determine what - if any - further action is needed.
Risk appetite	Amount (aggregate level) and type of risk that the university is willing and prepared to assume (accept), retain or tolerate, within its risk capacity, to achieve its objectives. Naturally, this amount will be lower than the maximum amount and type of risk it can take on - risk capacity.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk capacity	Maximum amount (aggregate level) and type of risk that the university can take on (or tolerate) in pursuit of its objectives. Risk capacity is the maximum amount of risk which the university is technically able to assume before breaching one or more of its capital bases, liquidity, borrowing capacity, reputational and regulatory constraints.
Risk champions	Employees who are not necessarily risk owners but preferably reporting directly to the risk owners and appointed by Management to lead the process of identifying and managing risks in their respective departments or functional areas.
Risk criteria	Terms of reference against which the significance of risk is evaluated. This includes the criteria for determining 'risk likelihood' and 'risk impact'.
Risk culture	The set of shared attitudes, values and practices that characterise how the university considers risk in its day-to-day activities. The risk culture typically flows from the university 's risk philosophy and risk appetite. If the university does not explicitly define its risk philosophy, the risk culture may form haphazardly, resulting in different risk cultures within the university or even within a particular department, business area or function.
Risk evaluation	The third and last step in risk assessment - the process of deciding whether the residual risk is acceptable or unacceptable. The RAS will inform the level of tolerance that is acceptable and whether the risk is outside of the university 's appetite. Whether a risk is acceptable or unacceptable relates to a willingness to tolerate the risk - that is, the willingness to bear the risk after it is assessed to achieve the desired objectives.
Risk identification	The first step in risk assessment - the process of identifying the risks and/or opportunities that might have an impact on the objectives of the university (as a whole), its department, function, project, process or activity.
Risk limit	A threshold to monitor that actual risk exposure does not deviate too much from the risk target and stays within the university 's risk tolerance/risk appetite. Exceeding risk limit(s) will typically act as a trigger for management action.
Risk matrix or probability-impact matrix	A series (combinations) of discrete risk estimates calculated as 'risk = probability-impact = probability x impact' represented in a matrix. Probability-impact is a basic risk measurement that can be used to estimate the costs of risks.
Risk philosophy	The university 's beliefs about risk and how it chooses to conduct its activities and deal with risks. The university recognises that effective risk management preserves and creates value and thus its risk philosophy reflects the value it seeks from ERM and influences how components of the Framework are applied.
Risk profile	A summary that lists estimates for all the risks associated with the university 's strategy, department, function, project, or activity. Risk profiles are documented and visualised using different methods but are typically based on estimates for the probability and impact of a list of identified risks. The most common visualisation of a risk profile is a risk heat map (known as a risk map).

Risk Term	Definition / Meaning[1]
Risk register	A document used as a tool to capture risk management status - record risks and facilitate management and reporting of risks at diverse levels and areas across the UNIVERSITY. A risk register, known as a risk log, acts as a repository for all risks identified and includes information about each risk such as linked objectives, risk description, root cause of the risk, risk category, risk rating, risk owner, risk response measures, action owner, risk outlook, etc.
Risk rating	The allocation of a classification to the impact and likelihood of a risk. Risk ratings, based on pre-established risk criteria, are calculated for inherent risk, residual risk and target risk.
Risk target	The optimal level of risk that the university wants to take in pursuit of a specific objective.
Risk tolerance	The specific maximum risk that the university is willing to take regarding each relevant risk and related objective. This is a measure of how comfortable the university is with varying levels of risk, a high-risk tolerance allows for significant risk, while low risk tolerance allows for only a small amount of risk.
Risk treatment	Method or means by which the university elects to manage individual risks. Risk treatments are referred to as risk responses, they involve identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them. Risk treatment can involve risk avoidance (terminating the risk), risk mitigation (controlling the risk), risk transfer (sharing the risk) and/or risk acceptance (tolerating the risk). Risk treatments that deal with negative consequences are sometimes referred to as risk mitigation, risk elimination, risk prevention or risk reduction. Risk treatment can create new risks or modify existing risks.
Risk trigger	An event or condition that causes a risk to occur, a risk trigger is known as a root cause of a risk materialising. In some cases, risk triggers are identified in advance as part of risk management, in other cases the exact triggers of a risk may be unknown in advance.
Strategic objectives	- An aim or desired result that the university wants to achieve for the entire institution.
Target risk or target residual risk	The desired level of risk after the assessment of the residual risk.
Action owner	Risk owner or suitable employee who is responsible for carrying out the risk treatment action (or activities). For every treatment action, an individual must be assigned as action owner to execute such action (or activities).

Appendix A: Development of risk registers

Process	Inputs	Types of approaches	Outputs
Identifying risk	- Strategic and operational objectives - Risk appetite and acceptable variation in performance Business context	- Data tracking/ Interviews - Facilitated workshops - Questionnaires and surveys - Process analysis - Leading indicators	Risk universe
Assessing risk	- Risk universe - Risk severity measures	- Probabilistic modelling - Sensitivity analysis - Judgmental evaluations - Benchmarking	Risk assessment results
Prioritizing risk	Risk assessment results Prioritization criteria	- Judgmental evaluations - Quantitative scoring methods	Prioritized risk assessment results
Responding to the risk	Prioritized risk assessment results	- Risk profile templates or pro forma risk profile. - Cost benefit analysis	- Deployed risk responses - Residual risk assessment results
Develop a portfolio view	Prioritized risk assessment results	- Judgmental evaluations - Quantitative scoring methods	Portfolio view of risk
Monitoring performance	- Residual risk assessment results - Portfolio view of risk	- Dashboards - Performance Reports	Corrective actions

The development of risk registers follows a systemic approach, and the registers are a management tools that documents and tracks risks. The register document the results of the risk assessment and management process, any contributing factors impacting the risks, the current controls to mitigate those risks and any action plans to further mitigate the risks, along with an assessment of the consequence and likelihood of these risks occurring from an inherent, residual and tolerable perspective. In the development of a risk register, it should be noted that reputational risk is embedded in all the risks. While the university has little appetite for sustained media attention that damages its reputation, it does support initiatives that promote its mission to contribute as a world class teaching and research university to wider

societal objectives of economic development, social and community development, and environmental enhancement. The university, therefore, considers its risk appetite in this area to be moderate in nature.

Risk ownership and responsibility

Risk owners are imperative for each risk identified; their role is to ensure that the risk is managed appropriately on a real-time basis as prescribed by the risk management strategy as defined in the UCT risk framework. Risk owners at the university were identified as per below guidance:

Project owners are responsible for initiating and maintaining a process of risk management consistent with the university's ERM Framework. They also ensure that all scoping documents include an initial risk assessment and that proposals for funding are accompanied by a risk assessment.

Primary Owner: The individual who is accountable for ensuring the risk is managed appropriately.

Secondary Owner: The individual who has the responsibility for undertaking the treatment plan or the treatment strategy that they have been directed to do (e.g. Chief Financial Officer). All risks in the risk register are 'owned' by a single named individual in the understanding that it may take shared responsibility to mitigate the risk successfully. The Chief Operating Officer assigns ownership of operational risks. The Deans assigns ownership of faculty risks. The executive Directors assigns ownership of departmental risks.

Task Owner: The individual who has the responsibility for completing the action plan for the risk as identified in the risk register.

INHERENT RISK RATING

The exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors.

In proceeding with the second step of the workshop, the Facilitator in conjunction with the workshop members assessed the inherent risk nature of each on the risks confirmed above. The inherent risk ratings to be used for this assessment are included in the tables below.

Inherent risk was assessed on impact and likelihood as described below:

Impact - Severity

This is the potential magnitude of the impact on your operations, should the risk occur. This must be assessed on the basis that management has no specific controls in place to address the risk, ***i.e., without any controls in place, what will the impact of this risk be on the University?***

Likelihood - Probability of occurrence

This is the likelihood that the identified risk will occur within a specified period (between 1 and 3 years) on the basis that there are no specific controls in place to address the risk. Inherent risk is assessed and rated to assist management in identifying which process needs resources required to control the related risk and to assist internal audit in identifying where their focus area should be when conducting their risk based internal audits.

Inherent Impact

Impact	Continuity of Operations	Safety & Environment	Technical Complexity	Financial	Score
Catastrophic Disaster with potential to lead to the collapse of UCT and is fundamental to the achievement of objectives	Widespread and lengthy reduction in continuity of operations to customers of greater than 5 days.	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 interdependencies between system /project components.	Significant cost overruns of >20% over budget. Effect on revenue / asset base of >10%.	**5**
Critical Critical event which can be endured but which may over a period have a negative impact and extensive consequences	Reduction in operations or disruption for a period ranging between 2 – 4 days over a significant area.	Significant injury of personnel or public. Significant environmental damage. Significant negative media coverage.	Use of new technology not previously utilised by the entity for critical systems / project components.	Major cost overruns of between 10% & 20% over budget. Effect on revenue / asset base of between 5% & 10%.	**4**
Serious Major events which can be managed but requires additional resources and management effort	Reduction in operations or disruption for a period between 1 – 2 days 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 and assets base	**3**
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 and assets base.	**2**
Minor Consequences can be readily absorbed under normal operating conditions.	No impact on operations 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.	**1**

Likelihood

Likelihood	Qualification Criteria	Score
Almost Certain	The risk is almost certain to occur in the current circumstances. The risk is already occurring or is likely to occur more than once within the assessment timeframe.	5
Likely	More than an even chance of occurring. The risk could easily occur and is likely to occur at least once within the assessment timeframe.	4
Possible	Less than even chance of occurring. The risk is expected to occur at least once within two subsequent assessment timeframes.	3
Unlikely	Small likelihood but could happen. The risk therefore occurs infrequently and is unlikely to occur within the assessment timeframe.	2
Rare	Not expected to happen - Event would be a surprise. The risk is conceivable but is only likely to occur in extreme circumstances.	1

Inherent Risk Levels

INHERENT RISK LEVELS						
IMPACT	Catastrophic	5	10	15	20	25
	Critical	4	8	12	16	20
	Serious	3	6	9	12	15
	Significant	2	4	6	8	10
	Minor	1	2	3	4	5
		Rare	Unlikely	Possible	Likely	Almost Certain
		LIKELIHOOD				

Appendix C: Control Effectiveness Table

Having established which controls are in place to manage the risks in question, the next step was to assess the perceived effectiveness of the controls using the below control effectiveness table. This is a measure of how well management perceives the identified controls to be working and effectively managing the risks.

Adequacy Factor	Adequacy Qualification Criteria	Rating
Very Good	Risk exposure is effectively controlled and managed	**90% +**
Good	Majority of risk exposure is effectively controlled and managed	**70%**
Satisfactory	There is room for some improvement	**50%**
Weak	Some of the risk exposure appears to be controlled, but there are major deficiencies	**30%**
Unsatisfactory	Control measures are ineffective	**10%**

Appendix D: Residual Risk Rating

Once all risks were documented with their corresponding Inherent risk ratings the residual risk rating was determined for a select few risks. Residual risk is the risk left over after controls are implemented to manage the risk to an acceptable level within the risk appetite as defined. Controls can consist of methods, procedures, equipment, or other actions implemented by management (either consciously or unconsciously) to increase the likelihood that the objectives will be achieved. Each risk may be mitigated by one or multiple mechanisms to effectively reduce the risk to a level that is acceptable to management and other stakeholders.

The “four T” principle is applied, i.e.

a. **T**ransfer the risk,
b. **T**reat the risk,
c. **T**olerate the risk, and
d. **T**erminate the risk.

Existing controls were then documented on the risk register and assessed on their effectiveness using the control effectiveness tables as included in the below paragraph. This information assists decision makers in assessing the acceptability of the residual risk exposure and in deciding whether further management action is required to reduce the risk exposure.

Residual Risk Rating Heat Maps

RESIDUAL RISK LEVELS						
Inherent risk Exposure	**Extreme**	5	10	15	20	25
	High	4	8	12	16	20
	Moderate	3	6	9	12	15
	Low	2	4	6	8	10
	Insignificant	1	2	3	4	5
		Very Good	**Good**	**Satisfactory**	**Weak**	**Unsatisfactory**
	Control Effectiveness					

Post Residual Risk Treatment

Based on the value of the residual risk exposure, management will decide whether it is willing to accept the identified level of residual risk exposure. If the residual risk is too high, then an action plan should be prepared to reduce the risk to a target risk or a level that is more acceptable to management and stakeholders. Management actions may include the re-examination of the control design for the risks identified.

The action plans must clearly identify:

a. The required actions.
b. The person(s) responsible for implementing the action, and
c. The applicable dates/timeframes.