ANNEXURE A

ENTERPRISE RISK MANAGEMENT POLICY FRAMEWORK

CONTENTS

1. ENTERPRISE RISK MANAGEMENT POLICY COMMITMENT

At the University of South Africa we are committed to the optimal management of risk in order to achieve our vision and mission, our principal tasks and key strategic objectives and to protect our core values.

The University Council has committed UNISA to a process of risk management that is aligned to the principles of the King III Report on Corporate Governance 2009. The features of this process are outlined in the Enterprise Risk Management Policy Framework of the University. It is understood that all colleges, support functions, processes, projects and entities under the control of the University will be subject to the Enterprise Risk Management Policy.

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

The University adopts an enterprise wide approach to risk management, which means that every key risk in each part of the University must be included in a structured and systematic process of risk management. All 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 systems and processes of the University, to ensure that our 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 our risk profile demands that UNISA adopt a prudent approach to corporate risk and our decisions regarding risk tolerance as well as risk mitigation will reflect this. None the less, it is not the intention to slow down the growth of the University with inappropriate bureaucracy. Controls and risk interventions will be chosen to assist us in fulfilling our commitments to stakeholders.

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

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

Chairperson of Council Principal and Vice Chancellor

Date: ____________________________ **Date:** ___________________________

2. INTRODUCTION

This document sets out the University of South Africa's (UNISA) Enterprise Risk Management Policy Framework. It describes the risk management policies, roles, responsibilities, processes and requirements established by Council for the management of risk in the University. These requirements are based on best practice standards and good corporate governance.

Enterprise Risk Management (ERM) deals with risks and opportunities affecting value creation and preservation and is defined as follows (with the required changes to make it applicable to UNISA):

Enterprise Risk Management is a process, effected by Council, Senate, the Principal and Management Committee and employees, 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 the University's objectives.[1]

It is acknowledged that the new style of risk management in the King III Code, Higher Education Act, 1997 (Act 101 of 1997) and other applicable legislation 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 risk exposures of the University.

The UNISA Council is responsible and accountable for directing and monitoring the risk management performance of the University in a structured framework. All divisions, operations and business functions must support Council to maintain a system of risk management.

It is important to note that this Enterprise 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 risk management strategies and processes of the University. The document must be updated annually.

The benefits of enterprise risk management to UNISA encompass:

Aligning risk appetite and strategy

UNISA Management Committee considers its risk appetite in evaluating strategic alternatives, setting related objectives and developing mechanisms to manage related risks.

Enhancing risk response decisions

ERM provides the rigour for the Management Committee to identify and select among alternative risk responses, risk avoidance, reduction, sharing and acceptance.

Reducing operational surprises and losses

UNISA gains enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.

Identifying and managing multiple and cross-enterprise risks

UNISA faces a myriad of risks affecting different parts of the organisation, and ERM facilitates effective response to the integrated responses to multiple risks.

Seizing opportunities

By considering a full range of potential events, UNISA Management Committee is positioned to identify and proactively realise opportunities.

[1] *COSO (The Committee of Sponsoring Organisations of the Treadway Commission)*

Improving deployment of capital

Obtaining robust risk information allows UNISA Management Committee to effectively assess overall capital needs and enhance capital allocation.

Ensuring compliance with laws and regulations

ERM helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to reputation and associated consequences of UNISA.

Increasing probability of achieving objectives

ERM helps the Management Committee achieve performance targets of UNISA and prevent loss of resources. Controls and risk interventions will be chosen on the basis that they increase the likelihood that we will fulfill our commitments to stakeholders.

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

3. REPORTING REQUIREMENTS

3.1 Internal reporting processes for risk information

The tiered structure of risk reporting must be followed.

The purpose of internal reporting on risk is to ensure that Council and the Management Committee can form a proper understanding of and monitor developments regarding risk and risk management at UNISA.

3.2 The 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 the exposures 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 – 3 months. Risks with an unknown pattern and risks that are new to the University should receive more frequent attention. The results of monitoring processes must be documented in a pre-defined format.

3.3 Incident reports must be generated for unacceptable losses

The generation of incident reports for unacceptable losses is an internal management function and forms part of the Enterprise Risk Management 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. Risk-related variances can be incorporated into routine management reporting processes.

4. RISK ASSESSMENTS

Once a year, Extended Management must undertake a thorough reassessment of risks of UNISA using the following methodology.

The first part of conducting a structured risk assessment is to profile the key building blocks of the business model of the University. This will highlight dependencies, critical parts of the University and start to pinpoint vulnerabilities. This can be done using the following processes:

4.1 Map the University's strategic direction and objectives

The strategic direction and objectives of UNISA must be specifically verified and interpreted in the context of risk. The future direction and intent of the University must be understood.

4.2 Profile the University's context

The total context of the University, external and internal, must be profiled. The outputs of this task must be documented.

4.3 Profile the objectives of colleges and departments

The objectives of colleges and departments within the context of the overall strategic objectives of the University must be profiled and the outputs documented.

4.4 Profile stakeholders of the University

Stakeholders may include the following: students, suppliers, employees (both academic and support employees), employee organisations, authorities, industry bodies, communities, social organisations, debtors and creditors.

4.5 Identify and profile the University's key assets and performance drivers

The following aspects should be taken into account:

- critical success factors,
- core competencies,
- competitive strengths and weaknesses, and
- asset performance.

4.6 Profile the key processes

The key activity chains of UNISA must be profiled and documented. The processes that generate revenue must be profiled. The drivers of the processes and the key features of these processes of the University 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 employee matters must be incorporated into the risk profile of the University.

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

4.7 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. Risk is apparent in potential, sudden and unforeseen events, in variances, volatility and failure. Risk will be apparent in nonlinear change, weakness and nonperformance. Risk will also be reflected in dimensions of nonconformance. 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. The process must have a future orientation and should examine the facts of today's business profile.

4.8 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.

4.9 Identify any influencing factors that may contribute to or shape the risk profile of UNISA

Having identified a key risk exposure (e.g. increasing competition, lack of funding) the risk assessment must identify the factors that influence and shape the risk. Every key risk will have influencing factors or variables. Such factors may relate to inherent risk dynamics. Others may relate to timing and cyclical factors. All influencing factors must be documented as part of the process.

4.10 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. Major changes in for example the organisational structure of the University can change the dynamics of risk. Retrenchments, cutbacks and layoffs are obvious sources of risk. Significant shifts in strategic direction may increase the values at risk in the University.

4.11 Identify external changes and identify 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 the introduction of new programmes, investments and capital projects. Their associated risks must be assessed as part of the risk framework. Certain changes in the educational sector beyond the control of the University should also be anticipated, for example regulatory change and competitive movements. Associated risks must be assessed.

4.12 Identify the potential root causes of risk events

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

4.13 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 only as a financial term. It is now the commonly accepted term for describing any mitigating measure for any particular type of risk. Controls may take the form of financial mitigations such as insurance or effective budget control. They may be managerial in nature such as compliance procedures, policies and levels of authority. Controls may be legal, for example contracts and indemnities.

4.14 Identify the perceived shortcomings in current controls and measures to mitigate the impact of risks

The Management Committee 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 to assess 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 more to a rigorous process of evaluating control effectiveness. The Management Committee must consider all categories of mitigation in this process. Results must be recorded in the risk registers.

4.15 Calculate the probability of risk events

The probability that an identified risk may occur must be assessed in every instance. Depending on the nature of the risk, different methods of calculating this probability could be considered. Statistical methods may be suitable to calculate the probable occurrence of financial and mechanical risks. On the other hand, risks with a managerial or strategic character may be better interpreted using simple ranking scales and expert-based interpretations.

The attached table (Annexure "A.2") is a guide to risk ratings. A realistic evaluation of the probability of a risk materialising is essential, because it guides 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 in the University;
- Consider, and research if necessary, how many similar incidents have occurred in the higher educational sector;
- Consider how many similar incidents have occurred at other universities;
- Consider the effectiveness of the existing preventative controls for the risk.

4.16 Calculate the potential impact of the identified risk scenarios

The consequences of risk are not just characterised or expressed in financial terms. The Management Committee must consider the various scales of impact that are relevant according to the prevalent categories of risk. These may include the scales for reputation damage, personal injuries and fatalities, media coverage and operational impact. From a strategic viewpoint, the Management Committee 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 the University, besides total cost or income, success in its core business (student throughput, research output and achieving its strategic aims) would be an important measure.

4.17 Rank the risks in order of priority

The ranking of risks must be shaped by strategic objectives. The ranking of risks in terms of net potential effect on the strategic objectives of UNISA will provide the Management Committee with some perspective of priorities. This should assist in the allocation of capital and 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 other reasons. This may be justified because of non-financial influences such as operational demands, media implications, social responsibilities or regulatory pressures.

5. 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 to Council, and should from time to time be tested by the internal audit process or other independent means of evaluation. The following aspects of the control environment should be considered:

5.1 Verify and evaluate the controls currently in place for key risks

It is vital that all of 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. First, 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 an action plan.

5.2 Evaluate the strategic mitigations in place for key risks

A specific review of the strategic position of the University 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.

5.3 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.

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

The risk finance measures of the University may include an insurance portfolio, self-insurance policies and funds, financial provisions and operating budgets for the funding of losses or variances. The Management Committee must compare the results of risk assessment processes with the current risk financing arrangements. This will highlight the net financial effect of risk events upon 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.

5.5 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 structures of reporting developed for this.

Having ascertained the suitability, appropriateness and effectiveness of risk controls, the Management Committee must decide on further action plans for actual and possible risks.

5.6 Take decisions on the acceptability of identified risks and controls

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

5.7 Document 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 at some future stage. 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 names of responsible persons. A process of follow-through must be used.

5.8 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 risk assessment processes. Considerations around budgeting should also be put in the context of cost-of-risk evaluations.

6. GOVERNANCE REQUIREMENTS

6.1 Establish a framework of assurance for key risks and controls

A framework of assurance must be developed for key risks. Key players in the University must combine to provide assurance to Council that risks are being appropriately managed. This combined approach to assurance normally involves external auditors, internal auditors and management working together through the Audit and Enterprise Risk Management Committee of Council. 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 formalised and must incorporate appropriate reporting processes.

6.2 Internal audit provides assurance that management processes are adequate to identify and monitor significant risks

Internal Audit Department must examine the techniques used to identify risks. 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 risk profile of the

University should be apparent. Monitoring processes should be wholly aligned with the results of risk assessments. The Internal Audit Department should particularly seek evidence that the processes of risk identification are dynamic and continuous, rather than mere attempts to comply with governance expectations.

6.3 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 the Management Committee and Audit and Enterprise Risk Management Committee of Council priorities. The risk assessment process is useful for internal audit employees, 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 employees may direct the Management Committee towards the need for improved controls relating to key risks.

6.4 Internal Audit provides an evaluation of risk management processes

The internal auditors must verify that risk reports are credible and offer a balanced assessment of risks. It is vital that an enterprise-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 Internal Audit Department.

6.5 Internal Audit provides objective confirmation that Council receives the right quality of assurance and reliable information from Management regarding risk

Internal Audit Department plays a key role in co-ordinating the key players in the risk management process to provide assurance to Council. The internal auditor is not normally the only provider of assurance. The function does, however, have an important role in evaluating the effectiveness of control systems. The process of assurance must of necessity involve Council, the Audit and Enterprise Risk Management Committee of Council, the Management Committee, external auditors, regulators and Internal Audit Department. The advice of other subject matter experts will also be incorporated into the process of providing assurance.

6.6 Safety, health and hygiene management

A formal safety management programme is essential for the University. The risks will vary according to colleges 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 exposures and legislative requirements.