



**JARAMOGI OGINGA ODINGA UNIVERSITY  
OF SCIENCE AND TECHNOLOGY**

**RISK MANAGEMENT POLICY**

**December, 2013**

## Jaramogi Oginga Odinga University of Science and Technology

### Risk Management Policy

2013

© Copyright JOOUST 2013

This policy was written and produced by Jaramogi Oginga Odinga University of Science and Technology

P.O. Box 210-40601 Bondo, Kenya

Telephone: + 254 - 57 2501804 / 2058000

Fax: + 254 - 572523851

Email: [vc@jooust.ac.ke](mailto:vc@jooust.ac.ke)

Website: <http://www.jooust.ac.ke>

**Policy Title:** Risk Management Policy

**Policy Theme:** To manage risks involved in all the University activities so as to maximize opportunities and minimize adversities

**Policy Contact:** Internal Auditor

**Approval Authority:** The Council

**Category:** Risk Management

**Reference No:** JOOUST/VC/LO/P/004

**Status:** Approved by Council  
20<sup>th</sup> December, 2013  
Minute: 8/05/12/13

**Commencement Date:** 20<sup>th</sup> December, 2013

Signed:

Vice-Chancellor, Secretary to Council  
Prof. S. G. Agong'

24<sup>th</sup> Jan 2014

Date

Chairman of Council  
Dr. B. J. Mwandotto

24<sup>th</sup> Jan. 2014

Date

**TABLE OF CONTENTS**

PREAMBLE ..... 5

LIST OF ABBREVIATIONS AND ACRONYMS ..... 6

1.0 AIM AND PURPOSE ..... 7

1.1 Aim of Risk Management Policy ..... 7

1.2 Purpose of Risk Management ..... 7

1.3 Objectives of Risk Management ..... 7

2.0 RATIONALE AND SCOPE ..... 8

2.1 Key Definitions in Risk Management..... 8

2.2 Relevance of Risk Management ..... 10

2.2.1 Uncertainty ..... 10

2.2.2 Value ..... 10

2.3 Benefits of Risk Management ..... 11

2.4 Activities included in Risk Management ..... 11

3.0 APPROACH TO RISK MANAGEMENT ..... 12

3.1 Risk Management Policy Framework..... 12

3.2 University Risk Management Principles ..... 13

3.3 Generic Sources of Risk..... 13

4.0 RISK MANAGEMENT PROCESS ..... 14

4.1 Risk Register/Plan..... 15

4.2 Risk Spectrum..... 16

4.3 Categories of Risk ..... 16

4.4 Areas of Impact..... 17

5.0 RESPONSIBILITIES ..... 18

5.1 University Council..... 18

5.2 Audit, Governance and Risk Management Committee of Council ..... 18

5.3 The Management Board..... 19

5.4 Risk Management Committee ..... 19

5.5 Internal Audit ..... 20

5.6 Other Employees..... 20

6.0 BUSINESS CONTINUITY PLANNING ..... 20

7.0 TRAINING AND DEVELOPMENT ..... 21

8.0 REVIEW OF POLICY ..... 21

9.0 INTERNAL AUDIT ORGAN GRAM..... 22

## PREAMBLE

Jaramogi Oginga Odinga University of Science and Technology (JOOUST) was established by the Government of Kenya as the successor of Bondo University College through the Jaramogi Oginga Odinga University of Science and Technology Charter 2013. In its endeavor to achieve its mission and uphold its core values, the University has adopted a systematic Risk Management approach. The development of this policy also follows the Government of Kenya Treasury circular No. 3/2009 in which the Permanent Secretary, office of the Deputy Prime Minister and Ministry of Finance directed all Accounting officers, Chief executives of state corporations and Clerks to Local Authorities to develop and implement institutional Risk Management Policy Framework in the public sector.

The management of risk is an integral part of good management practice. There is a direct relationship between risk and opportunity in all business activities, and as such, an organization needs to be able to identify, measure and manage its risks in order to be able to capitalize on those opportunities and achieve its goals and objectives.

The risk management process does not encourage managers to be risk averse. In fact, it is designed to provide managers with a degree of confidence to be able to manage risk to an acceptable level and to take a level of risk commensurate with the opportunity. The key element in managing risk is correctly balancing risk and reward. A culture which is risk averse will create inflexibility in the business and erect barriers to the achievement of the organization's goals. Alternatively, the acceptance of disproportionately high risk can have significant impacts on the business.

Risk is inherent in all support, administrative and business activities. Every member of Jaramogi Oginga Odinga University of Science and Technology fraternity continually encounters and manages risks. Overtime, formal and systematic approaches to managing risks have evolved and they are now regarded as good management practice. In the same direction, Jaramogi Oginga Odinga University of Science and Technology acknowledges that the adoption of a strategic and formal approach to risk management will improve decision-making and enhance outcomes and accountability.

## LIST OF ABBREVIATIONS AND ACRONYMS

<b>COBIT</b>	-	Control Objectives for Information and related Technology
<b>COSO</b>	-	Committee for sponsoring Organizations of the Tread way Commission
<b>DVC</b>	-	Deputy Vice Chancellor
<b>ICT</b>	-	Information and Communication Technology
<b>JOUST</b>	-	Jaramogi Oginga Odinga University of Science and Technology
<b>MB</b>	-	Management Board
<b>OPS</b>	-	Operations
<b>RM</b>	-	Risk Management

## 1.0 AIM AND PURPOSE

### 1.1 Aim of Risk Management Policy

The aim of this policy is not to eliminate risk, but rather to manage the risks involved in all the University activities so as to maximize opportunities and minimize adversities. Effective risk management requires a strategic focus, forward thinking and active approaches to management; balance between the cost of managing risk and the anticipated benefits; and contingency planning in the event that mission critical threats are realized. Risk management will also enable the University to successfully achieve its goals. With the growing need for transparent decision-making, a structured, systematic risk management process demonstrates the due diligence that is required and provides an audit trail for decision making. A comprehensive understanding of the risk exposures facing the University also facilitates effective planning and resource allocation, and encourages a proactive management culture, with flow-on benefits for every aspect of University operations.

Risk management will also provide the University with a system for the setting of priorities when there are competing demands on limited resources.

### 1.2 Purpose of Risk Management

Risk Management is a core component of University Governance. The purpose of this policy is to:

- i. Develop a culture of risk awareness whilst maintaining a culture of innovation and realization of opportunities within the University;
- ii. Ensure compliance with risk management processes that are mandated by Government;
- iii. Integrate and align risk management systems with University's activities and business processes;
- iv. Encourage continual review and improvement of the University's risk assessment and management processes.

### 1.3 Objectives of Risk Management

- i. Ensure that the University risks are taken into account when making strategic management decisions;
- ii. Ensure the management of operational risks is integrated into standard management and accountability processes; and

- iii. To develop an environment where staff assume responsibility for managing risks.

## 2.0 RATIONALE AND SCOPE

This policy outlines the University's commitment to facilitating strategic and operational goals and objectives through risk management, enabling continuous improvement in decision-making and performance;

The University will promote continuous improvement and review of risk management through regular training, monitoring, audit and reporting processes;

Employees in all areas and activities of the University are responsible for applying risk management principles and practices in their work areas;

Employees in supervisory and managerial positions are responsible for ensuring that risk management principles and practices are applied by those under their supervision.

### 2.1 Key Definitions in Risk Management

The University defines the following terms used in this policy as;

**Risk:** The threat or possibility that an action or event will adversely or beneficially affect University's ability to achieve its goals. Risk is measured in terms of likelihood and impact;

**Raw Risk:** The level of risk faced by an organization before any internal controls is applied;

**Risk Management:** The culture, processes and structures that are directed towards the effective management of potential opportunities and possible adverse effects within the University's environment;

**Risk Management Process:** The systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk;

**Residual Risk:** The risk remaining after implementation of risk treatment;

**Risk Appetite:** The degree of risk, on a broad-based level, that a company or other entity is willing to accept in pursuit of its goals;

**Internal Controls:** The processes, policies and procedures we use to govern the University's work, or any additional mitigating actions that we take to deal with a particular, or potential situation;



**Risk Treatment:** The process of selection and implementation of measures to modify risk;

**Strategic Risks:** Risks that affect the ongoing work of the University as outlined in the University's Strategic Plan;

**Operational Risks:** All other corporate risks associated with the operations of the University;

**Risk Identification:** The process of determining what might have happened, how, when and why;

**Risk Analysis:** The systematic process applied to understand the effect of the uncertainty of the risk on our goals and objectives;

**Risk Evaluation:** The process of comparing the significance of the risks to define the order in which they should be dealt with;

**Risk Mitigation:** Refers to actions that must be taken to lower the likelihood of the risk occurring and/or to minimize the impact if the risk did occur. Risk can never be totally eliminated, but it can be mitigated to lessen its likelihood and or impact;

**Risk responses:** The means by which an organization elects to manage individual risks. The main categories are to tolerate the risk; to treat it by reducing its impact or likelihood; to transfer it to another organization or to terminate the activity creating it. Internal controls are one way of treating a risk;

**Transfer of risk:** Foresees the persuasion of another party to accept the risk, through a contract. This is a typical case that concerns insurance companies, which is applied often when possible even if at times it is done in a general manner and not, rather, in function of the specific organization (Tailored covering);

**Risk exclusion:** Foresees the non-execution of the activity that involves a risk that cannot be transferred and/or is considered to be unacceptable. Naturally, the result is a loss of opportunity that the activity at risk would have represented in any case;

**Risk reduction:** Involves the adoption of managerial, technological and behavioral actions that lower the probability of risk and/or the seriousness of the possible consequences. The persistence of residual risk is often, in any case, unavoidable both for reasons inherent to the context (institutional, managerial, technological, etc.) in which the organization operates, as well as for the possible simplifications and/or omissions of the analysis;

**Risk Acceptance:** Involves acceptance of risks that are not transferred and/or excluded. The conscious acceptance of residual risk occurs, in general, when at least one of the following conditions applies;

- a) Sufficiently low probability of the event;
- b) Consequences of the event are proportionally of little relevance;

- c) Great benefits if successful.

## 2.2 Relevance of Risk Management

The underlying premise of risk management is that every organization exists so as to provide value to its stakeholders. Such value is manifested on the quality of service delivery to the customers. All organizations face uncertainty, and the challenge for management is to determine how much uncertainty the organization is prepared to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. This policy provides a basis for Management Board to effectively deal with uncertainty and its associated risk and opportunity, thereby enhancing its capacity to build value.

### 2.2.1 Uncertainty

The University operates in an environment where factors such as globalization, technology, regulation, restructuring, changing markets, and political influence create uncertainty. Uncertainty emanates from an inability to precisely determine the likelihood that potential events will occur and the associated outcomes.

### 2.2.2 Value

Value is created, preserved or eroded by management decisions ranging from strategic planning to daily operations of the University. Inherent in decisions is recognition of risk and opportunity, requiring that management consider information about the internal and external environment deploys precious resources and appropriately adjusts organization's activities to changing circumstances.

Organizations realize value when stakeholders derive recognizable benefits that they in turn value. For public institutions, value is realized when constituents recognize receipt of valued services at an acceptable cost. Risk management facilitates management's ability to both create sustainable value and communicate the value created to stakeholders.

While each organization will find its own way to integrate risk management into existing decision-making structures, the following are factors to be considered;

- i. Aligning risk management with objectives at all levels of the organization;
- ii. Introducing risk management components into existing strategic planning and operational practices;
- iii. Communicating organizational directions on an acceptable level of risk;

- iv. Including risk management as part of employees' performance appraisals; and
- v. Continuously improving control and accountability systems and processes to take into account risk management and its results.

### **2.3 Benefits of Risk Management**

The University will not operate in a risk-free environment, and the risk management process does not create such an environment. Effective risk management will assist the University to achieve its performance and service delivery targets and to reduce the potential loss of resources. This results in effective responsibility and performance as well as compliance with laws and regulations, thus avoiding damage to its reputation and other undesirable consequences. Key specific benefits include;

- i. Greater likelihood of achieving pre-stated objectives;
- ii. Effective and efficient service delivery;
- iii. A rigorous basis for strategic management through consideration of key elements of risk;
- iv. Enhanced risk management strategy decisions through quantification of risk tolerances;
- v. More focus internally on doing the right things in the right way;
- vi. Identification and management of risks affecting different departments and/or different processes;
- vii. Identification and implementation of cost effective, integrated responses to multiple risks;
- viii. Minimizing operational surprises, costly and time consuming litigation and unexpected losses;
- ix. Rationalization of capital and financial resources;
- x. Continuity of service delivery;
- xi. Greater transparency in decision making and ongoing management processes; and
- xii. Enhanced accountability and corporate governance processes.

### **2.4 Activities included in Risk Management**

The University will include the following activities while managing its risks;

- i. Articulating and communicating the objectives of the University;
- ii. Determining the risk appetite of the University;
- iii. Establishing an appropriate internal environment, including a risk management framework;
- iv. Identifying potential threats to the achievement of the objectives;
- v. Assessing the risks i.e. the impact and likelihood of the threat occurring;
- vi. Selecting and implementing responses to the risks;
- vii. Undertaking control and other response activities;

- viii. Communicating information on risks in a consistent manner at all levels within the University;
- ix. Centrally monitoring and coordinating the risk management process and the outcomes; and
- x. Providing assurance on the effectiveness with which risks are managed.

### **3.0 APPROACH TO RISK MANAGEMENT**

The University is committed to the implementation of a comprehensive risk management framework, has an open and receptive approach to solving risk problems and ensures that risk management is integrated into normal business processes and aligned to the strategic goals of the University. The Approach to Risk Management adopted by the University is based on the best practices worldwide which have also been adopted by other organizations.

The two main approaches are based on the Committee for Sponsoring Organizations of the Tread way Commission, (COSO) and COBIT. COSO defines Enterprise Risk Management as; “A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

The Control Objectives for Information and related Technology (COBIT) approach applies significantly in the Information Technology Environment within JOOUST. The COBIT framework was revised and enhanced to support increased management control, introduce performance management and further develop IT governance.

#### **3.1 Risk Management Policy Framework**

A framework provides a comprehensive approach for the University to adopt in identifying and managing risks, which if not realized, could effectively prevent the University from achieving its business goals and strategies. The University operates in a complex environment with ever increasing public expectations, greater accountability and higher quality standards of service delivery which are placing more pressure on resources. The implementation of a robust and transparent risk management program becomes increasingly important in order for the University to adapt and meet these challenges in a structured way so as to continually align its priorities and objectives against a background of changing risk and uncertainty.

Consequently, the framework will be developed to;

- i. Allow the University to proactively manage its risks in a systematic and structured way and to continually refine its processes to reduce the University’s risk profile thereby maintaining a safer environment for all of its stakeholders;
- ii. Ensure that appropriate strategies are in place to mitigate risks and maximize Opportunities

- iii. Embed the risk management process and ensure it is an integral part of the University's planning process both at strategic and operational levels;
- iv. Help create a risk awareness culture from a strategic, operational, individual project and fraud perspective;
- v. Give credibility to the process and engage management's attention to the treatment, monitoring, reporting and review of identified risks as well as considering new and emerging risks on a continuous basis;
- vi. Recognize the need for, and align the holistic University wide "top-down" strategic assessment with the "bottom-up" operational and strategic risk assessment.

### 3.2 University Risk Management Principles

Risk management should:

- i. Create and protect value;
- ii. Be an integral part of all processes;
- iii. Be part of organizations decision making;
- iv. Be used to deal with uncertainty;
- v. Be structured, systematic and timely;
- vi. Be based on the best information;
- vii. Be tailored to the operating environment;
- viii. Deal with human and cultural factors;
- ix. Be transparent, inclusive and relevant;
- x. Be dynamic, responsive and iterative; and
- xi. Facilitate continual improvement.

### 3.3 Generic Sources of Risk

Identifying sources of risk and areas of impact provides a framework for risk identification and analysis. A generic list of sources and impacts will focus risk identification activities and contribute to more effective risk management. The University has identified the following generic sources of risk;

- i. Commercial and legal relationships including but not limited to contractual risk, product liability, professional liability and public liability.
- ii. Economic circumstances. These can include such sources as currency fluctuations, interest rate changes, taxation and changes in fiscal policy.
- iii. Human Behavior such as riots, strikes, sabotages.
- iv. Natural Events. These can include fire, water damage, earthquakes, vermin, disease and contamination.
- v. Political Circumstances such as legislative changes or changes in government policy that may influence other sources of risk.
- vi. Technology and Technical Issues. Examples of this include innovation, obsolescence and reliability.
- vii. Management Activity and Control such as poor safety management, the absence of control and inadequate security.
- viii. Individual Activity including, misappropriation of funds, fraud, vandalism,

illegal entry, information misappropriation and human error. In most instances a risk source will be under the control of the officer conducting or accountable for an activity or function. In some instances (and these are entirely circumstance driven) the risk may be spread across the organization or even outside it. If this is the case then the relevant parties should be consulted during the risk assessment process.

#### 4.0 RISK MANAGEMENT PROCESS

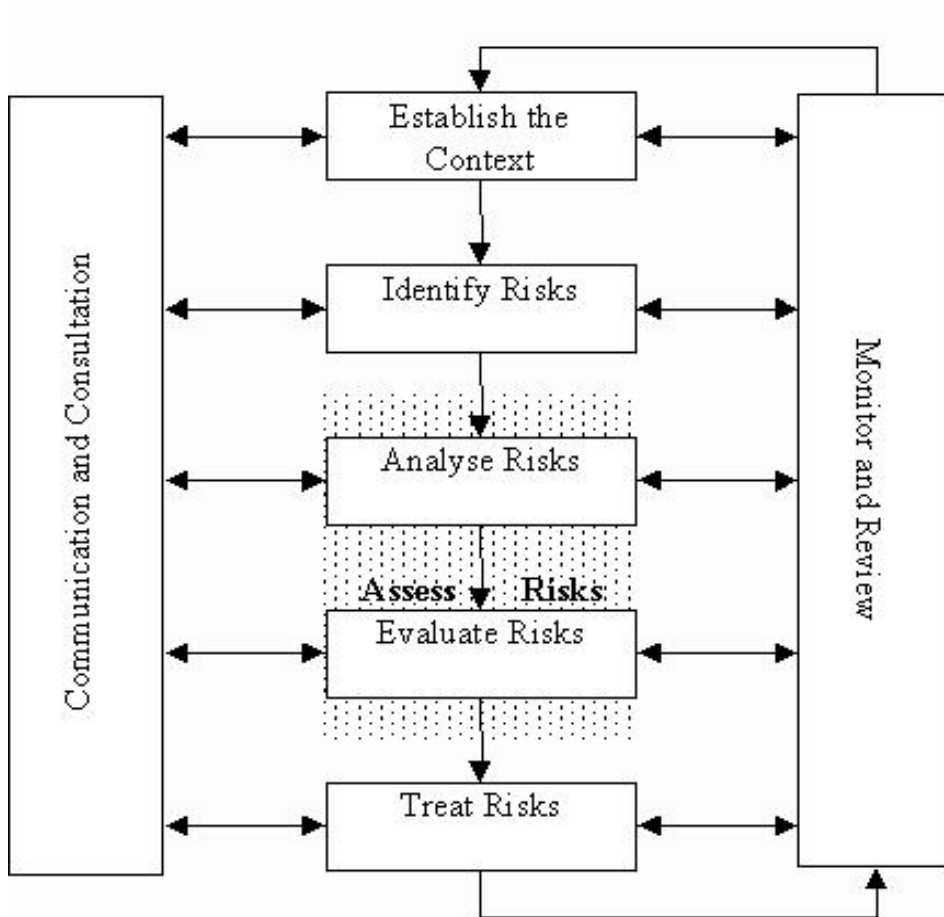
This is a detailed process for establishing risk management practice within the University; the process is as follows;

- i. **Establish a context:** This is the strategic, organizational and risk management context against which the rest of the risk management process in the University will take place. It involves identification of areas susceptible to risks. It also involves organizing the necessary resources and defining duties and responsibilities. Criteria against which risk will be evaluated should be established and the structure of the risk analysis defined.
- ii. **Identify Risks:** The University will carry out the identification of what, why and how events arise as the basis for further analysis.
- iii. **Analyze Risks:** The University will determine the existing controls and the analysis of risks in terms of the consequence and likelihood in the context of those controls. The analysis should consider the range of potential consequences and how likely those consequences are to occur. Consequence and likelihood are combined to produce an estimated level of risk.
- iv. **Evaluate Risks:** The University will compare estimation of risk levels against pre-established criteria. This enables risks to be ranked and prioritized
- v. **Treat Risks:** This is the phase in which the decision making processes become particularly important For higher priority risks, the University is required to develop and implement specific risk management plans including funding considerations. It includes, either alternatively or in combination, one or more of the following conditions:
  - a) Transfer of risk;
  - b) Exclusion of risk;
  - c) Reduction of risk;
  - d) Acceptance of risk or an amount of the risk.
- vi. **Monitor and Review:** The University will oversee and review risk management system and any changes that might affect it. Monitoring and reviewing occurs concurrently throughout the risk management process.

- vii. **Communication and Consultation:** The University will ensure that appropriate communication and consultation with internal and external stakeholders should occur at each stage of the risk management process as well as on the process as a whole.

Schematically, the risk management process is depicted in the following diagram;

**Table 1: Risk Management Process**



### 4.1 Risk Register/Plan

The University defines risk register as a table of risks in each and every department. It covers the risk identity, risk area, title and description of the risk, implication of the risk, its impact, likelihood, score, expected responses/control and the attendant responsibilities. This register will be updated from time to time, depending on the emerging risks affecting each and every school, directorate, departments and the University at large. The following explanations are therefore paramount in this context;

**Risk:** Is the possibility that an event will occur and adversely affect the achievement of set objectives.

**Risk rating:** The risks identified are rated depending on impact and likelihood, where;

**Likelihood (L):** Is the probability that an adverse event, which could cause materialization of the risk, may occur; and

**Impact (I):** Is the potential loss should the risk materialize.

The likelihood and impact are both scored on a graduated scale of between 1 and 10, with the final risk rating arrived at using the formula  $(I \times L)/10$ ,

Where;

I – Impact and  
L – Likelihood

Risks have also been rated as high, low or medium according to the scale as follows:

**High:** Risks with a rating equal to or greater than **7.0**;

**Medium:** Risks with a rating greater than **4.0** and less than **7.0**; and

**Low:** Risks with a rating less than or equal to **4.0**

If a weighing scale for example is described to be not working as expected, the risk is that the supplier will be overcharged or undercharged. Using the above graduated scale, the impact is chosen to be **9** and the likelihood chosen to be **5**, the overall score will then be calculated as follows;

$(I \times L)/10 = (9 \times 5)/10 = 4.5$  Hence the overall risk rating is Medium. An overall risk score is **ideal** when it is low.

A risk register for the University will be developed in consultation with the Deans of schools, Directors, Coordinators, and Heads of departments/sections.

## 4.2 Risk Spectrum

In this policy, Risk Spectrum defines the global risks and University risks. The global risks can be; climate change, population explosion, religious fundamentalism, Nuclear Proliferation, Pandemics, Political Fragmentation among others. These global risks will also affect the achievement of the University's strategic objectives. The global risks will mirror into the organizations' risks and results into legal liability risks, operational risks, financial market risks and political or regulatory risks. For the University to manage and mitigate the resultant risks, controls have to be put in place. The controls will be in form of procedures, standards, policies, rules, regulations etc

## 4.3 Categories of Risk

The University has highlighted general types of risks that may be faced by the University.



They will be utilized as a starting point guide to aid risk discussions. They will also act as a checklist during the development of University risk registers. They include;

- i. Budgeting (relates to availability or allocation of resources);
- ii. Fraud or Theft;
- iii. Unethical dealings;
- iv. Public perception and reputation;
- v. Exploitation of workers and or suppliers (availability and retention of suitable staff);
- vi. Failure to comply with legal and regulatory obligations and or contractual aspect;
- vii. Civil Action;
- viii. Failure of the infrastructure (including utility supplies, computer networks etc);
- ix. Failure to take account of widespread disease or illness among the workforce and students;
- x. Failure to establish effective continuity arrangements in the event of disaster;
- xi. Collapse of contractors;
- xii. Failure of suppliers to meet contractual commitments (this could be in terms of quality, quantity, and timescales on their own exposures to risk);
- xiii. Exchange rate fluctuation;
- xiv. Interest rate instability;
- xv. Inflation;
- xvi. Management incompetence;
- xvii. Inadequate corporate policies;
- xviii. Inadequate adoption of management practices;
- xix. Poor leadership;
- xx. Poor staff selection procedures;
- xxi. Lack of clarity over roles and responsibilities;
- xxii. Vested interest creating conflict and compromising the overall aims;
- xxiii. Indecisions or inaccurate information;
- xxiv. Natural disasters.

#### **4.4 Areas of Impact**

Within the University a source of risk may impact on one area only or on several areas. Areas of impact to the University include;

- i. Asset and resource base including personnel;
- ii. Revenue and entitlements;
- iii. Costs both direct and indirect;
- iv. Human resource;
- v. The community;
- vi. Students;
- vii. Performance;
- viii. Timing and schedule of activities;
- ix. The environment;
- x. Intangibles such as reputation, goodwill and the quality of life; and
- xi. Organizational behaviour.

## 5.0 RESPONSIBILITIES

Every member of the University is responsible for effective management of risk including the identification of potential risks. Management is responsible for the development of risk mitigation plans and the implementation of risk reduction strategies. Risk management processes should be integrated with other planning processes and management activities.

### 5.1 University Council

Further to statute xxiv, the University Council is responsible for;

- i. Oversight of risks within the University;
- ii. Approving the risk management policy, overseeing its implementation and approving changes to policy;
- iii. Satisfying itself that fundamental risks are being managed in an appropriate way by approving risk management policy and procedures and reviewing risk reports from the Audit Committee;
- iv. Determining the University's attitude towards risk; risk appetite and acceptability of risk and acceptable level of exposure;
- v. Setting the tone and influencing the culture of risk management within the University;
- vi. Delegating responsibility for the implementation of risk management policy to the Audit Committee, the University Management Board, the Risk Management Committee and key Management personnel.

### 5.2 Audit, Governance and Risk Management Committee of Council

In accordance with the JOOUST Statutes 2013; schedule vi (3) the role of the Audit Committee is to assure the Council that adequate systems of Risk Management are in place in the University and that fundamental risks are adequately and appropriately managed. It oversees the risk management and business continuity framework. The Audit Committee is responsible for;

- i. Ensuring that risk management and business continuity policies, procedures and framework is established, implemented and maintained;
- ii. Monitoring the management of strategic and significant operational risks;
- iii. Considering the system of internal financial controls and to satisfy itself that the control environment is adequate and that controls are operating effectively;
- iv. Keeping under review, and advise on, the operation and effectiveness of the University's risk management systems;
- v. Considering the Internal Audit Annual Audit Programme, to review reports from the Head of Internal Audit, to consider major findings and Management's response;
- vi. Monitoring the effectiveness of Risk Management in relation to the risks identified as fundamental to the success or failure of the University's objectives.

### 5.3 The Management Board

The Management Board is responsible for;

- i. Implementing the University policy on risk management;
- ii. Formal identification of strategic risks that impact upon the corporations objectives, mission and vision;
- iii. Responsible as individual risk owners for the management of fundamental risks and allocation of priorities;
- iv. Considering all risk matters referred to it by the Risk Management Committee, in particular, risk issues which have emerged from Risk Registers and which may require escalation;
- v. Ensuring, in conjunction with the Risk Management Committee that each Fundamental Risk has a 'Risk Owner' responsible for its management;
- vi. Ensuring that risks associated with significant proposals / projects have been properly considered and can be appropriately managed within the University's Risk Policy.

### 5.4 Risk Management Committee

The Risk Management Committee provides overview and direction to the risk management processes within the University. The Risk Management Committee reports and makes recommendations to the Audit, Governance and Risk Management Committee of Council. The risk management committee also;

- i. Monitors and reviews strategic, significant operational and enterprise-wide risks;
- ii. Receive and consider risk management and business continuity reports to inform the Audit, Governance & Risk Management Committee of Council;
- iii. Review risk management and business continuity management incidents as they occur;
- iv. Establish and administer a University-wide risk register;
- v. Establish and administer University-wide business continuity management system;
- vi. Implement University-wide risk management and business continuity training.

The composition of the Risk Management Committee is as follows;

- i. DVC (Planning, Administration & Finance)-Chairperson
- ii. All Registrars
- iii. Director, ICT
- iv. Dean of Schools (One to be appointed to represent all Schools)
- v. Finance Officer
- vi. Legal Officer
- vii. Librarian
- viii. Procurement Officer
- ix. Security Officer
- x. Internal Auditor-Secretary

## 5.5 Internal Audit

In pursuant to Statute XIX, the role of internal audit is to provide independent and objective assurance to the Vice Chancellor and the Audit, Governance and Risk Management Committee of council on the effectiveness of risk management process put in place by the management and recommend appropriate risk mitigation measures. The internal audit office will also ensure that;

- i. The organization's risk management process address the objectives which generally gauge the adequacy and effectiveness of risk management process
- ii. Risks relating to the organization are categorized into strategic, operational, compliance, environmental, political, financial and are then prioritized.
- iii. Risk mitigation measures are developed and implemented to reduce or otherwise manage risks that are determined to be acceptable to the organization
- iv. Monitoring activities are conducted periodically to re-assess risk and the effectiveness of controls to manage the risks
- v. Provides management and Audit Committee with periodic reports on the effectiveness of the risk management process

## 5.6 Other Employees

All employees are responsible for applying risk management principles and practices in their work areas. Employees in supervisory and managerial positions are responsible for ensuring that risk management principles and practices are applied by those under their supervision;

- i. To report risks with the potential to impact upon their work area or the wider University to the relevant area of the University's Risk Management Structure;
- ii. Employees are to participate in University risk management and business continuity education and training activities relevant to their level of responsibility;

## 6.0 BUSINESS CONTINUITY PLANNING

The University shall conduct business continuity planning on an enterprise-wide basis as one the major components of risk management. In this case the University defines business continuity planning as a process whereby organizations ensure maintenance of critical operations when confronted with adverse events such as natural disasters, technology failures, human errors, or terrorism. The University has an obligation to protect and provide for students, faculty, staff, and visitors in the event of a major interruption of its mission or operations. These obligations extend to a responsibility for each department to be able to meet its individual obligations. This includes the ability to provide the services expected of them and to carry out services critical to the mission of the University should an event occur that interrupts the normal course of operations. The University will therefore have in place an adequate continuity plan that will prevent such effects as financial disaster, interruption of

academic classes, failure of research projects, and delays in completing other mission critical activities.

## **7.0 TRAINING AND DEVELOPMENT**

The University will be committed towards the development and encouragement of enterprise-wide training and exercises with the main aim of achieving successful risk management and business continuity management. As a result key officers from the board level to lower level staff will be identified from time to time to undergo relevant trainings. Such trainings will not only enable participants understand how risk management affects decision making but will also enable them raise basic awareness of risk management concepts and mechanisms that will allow them identify and manage risks in their respective units and strengthen business continuity management through adequate forward planning practices.

## **8.0 REVIEW OF POLICY**

Risk management policy and underlying strategies or procedures will be reviewed regularly by the Council through the Audit Committee to ensure its continued application, effectiveness and relevance.

9.0 INTERNAL AUDIT ORGAN GRAM

