BLANTYRE INTERNATIONAL UNIVERSITY

BIU RISK POLICY

January 2017

Private Bag 98, Blantyre, Malawi
Tel: +265 1 831516 | Fax: +265 1 831514
Email: info@biu.ac.mw
Website: www.biu.ac.mw

Contents

Introduction

This Risk Management Policy is meant to formalize BIUs commitment in incorporating the principles of risk management into all aspects of the University.

Purpose and scope

In accordance with the University's Risk Management Policy, these procedures describe the University's standard process for risk management, including:

- Risk identification
- Risk rating
- Risk controls
- Risk monitoring and reporting

A standard approach to risk management allows risks to be correctly prioritized across all of the University's operations, which in turns means that effective controls can be put in place to ensure the University is able to manage its operations effectively now and into the future.

The procedure applies to all activities undertaken in the course of university business, whether on the university campuses or other locations.

Responsibilities

The Board retains the ultimate responsibility for risk management and for determining the appropriate level of risk that the University is willing to accept.

The Audit and Risk Management Committee is delegated by the Board with responsibility for: overseeing the risk management activities at the University; and approving appropriate risk management procedures and measurement methodologies throughout the organisation.

The Audit and Risk Management Committee will liaise with management in monitoring key risks and where appropriate will report to Board to provide assurances concerning the management of risks within the University.

The **Vice-Chancellor and Chancellor** is responsible for ensuring that risk management activities are carried out effectively within the University. On a quarterly basis, and upon request, the Vice-Chancellor and Chancellor shall present to the Audit and Risk Management Committee an up-to-date register of the key risks for the University, that is, the Risk Register.

The Vice-Chancellor and Chancellor shall appoint the Risk Manager. The Risk Manager shall provide regular reports to the Vice-Chancellor and Chancellor on key risks to the University and the control and monitoring activities in place to manage those risks.

The Risk Manager may be a dedicated role, or may be additional responsibilities to an existing position. The Risk Manager is responsible for ensuring that risk management activities are carried out in the university in accordance with the risk management policy and risk management procedures.

The Risk Manager is responsible for providing information to the Vice-Chancellor and Chancellor to forward to the Audit and Risk Management Committee regarding the status of risk management activities since the previous meeting.

A Risk Owner will be assigned for each risk area within the University. A Risk Owner is the most senior staff member within an organisational unit, which is responsible, or should be responsible, for the management of the particular risk.

Where the situation arises where it is unclear as to who should be the Risk Owner for a particular risk, the Risk Manager shall assign a Risk Owner.

It is the Risk Owner's responsibility to provide the Vice-Chancellor and Chancellor with information to report to the Audit and Risk Management Committee on progress against mitigation plans and the results of risk assessments performed on new initiatives.

All University Staff shall diligently identify risks and report them to their supervisors/Heads. Staff shall comply with all risk treatments.

The assurance providers play a role in monitoring and reporting to the Council and Audit and Risk Management Committee on the University's management of its risks, by assessing the internal controls in place to mitigate risks and recommendations to enhance the University's risk management framework.

Risk management process and BIU Model

A risk to the University is any event or action that could have a negative impact on the University. This includes events that could lead to:

- Death or injury.
- Financial loss to the University.
- Damage to the University's reputation or adverse media coverage.
- Damage to the physical environment, including land, water or air quality.
- Failure to meet regulatory or legislative requirements.

In addition the failure to identify and capitalise on opportunities is also considered a risk.

It is essential that the University is aware of what risks it faces, and takes adequate precaution to avoid significant damage as a result of those risks. The University has therefore developed a risk management model to ensure that management of risks is undertaken in a systematic and standard approach across all of its operations.

Risk Management Model

The Risk Management Model (Figure 1 below) outlines the University's approach to risk management and integrates the Risk Management Principles and Risk Management Process.

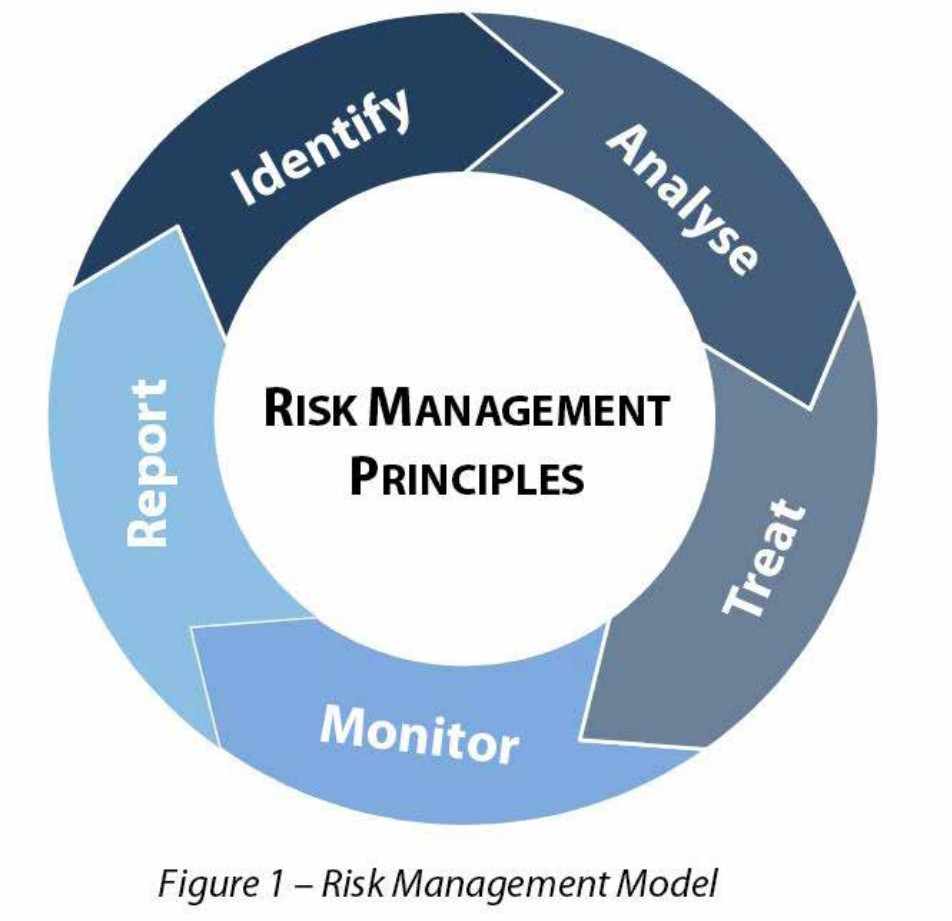

Figure 1 – Risk Management Model

Risk Management Principles support the effective management of risk across the University. The University's risk management must:

- Align with its Mission and Vision;
- Be embedded within its operations, processes and systems;
- Have clear accountability, ownership and governance;
- Be systematic, transparent and consistently applied;
- Include effective consultation and communication;
- Consider the context (both the internal and external environment);
- Support evidence-based decision-making; and
- Facilitate continual improvement.

Risk Management Model:

Risk identification

A structured approach to identifying the events that, if they were to occur, could have a negative impact on the University.

Risk rating

A process to analyse and understand each of the risks, including understanding what causes the risk to occur and what controls are already in place to manage the risk; risk assessment also determines:

- how severe a potential impact could be, and
- what is the likelihood of the University being negatively impacted in this way.

Once the potential impact and likelihood have been assessed, the risk assessment process considers whether the risk is acceptable to the University, or whether further treatments are required to further reduce the level of risk.

Risk controls

Controls represent a whole range of actions, measures and strategies taken by management to eliminate or reduce risks. They include documenting policies and procedures, ensuring separation of duties in certain functions, implementing quality assurance programs, including appropriate clauses in contracts, etc.

The process in determining risk controls includes, assessing the risk, assessing risk appetite and evaluating how to treat the risk through mitigating actions.

In assessing a risk, we firstly must give consideration of our risk appetite by making a risk assessment, this could include:

- avoid the risk
- mitigate the risk
- transfer the risk, and
- accept the risk.

A process should then be followed to identify efficient and effective ways to mitigate against the risk, this can occur by either:

- removing the risk
- reducing the likelihood of the risk impacting on the University
- reducing the consequences if the risk were to occur, or
- a combination of these approaches.

Risk monitoring and reporting

A process of regular review to ensure that:

- new risks are identified and considered as they arise
- existing risks are monitored to identify any changes which may impact on the University

- new risk controls are being implemented according to the planned schedule
- existing risk controls are still in place and working effectively
- that information on risks is adequately communicated to appropriate parties, in particular the Vice-Chancellor and President and the Audit and Risk Management Committee.

Following this process allows the University to:

- Anticipate and respond in advance to events that would otherwise cause damage to the University
- Reduce the costs and other damage associated with failing to respond
- Create a safer environment for everyone within the University
- Focus management attention on developing and expanding the University rather than responding to incidents that could have been avoided
- Negotiate reduced premiums with insurers

The Stages in the BIU Model

Risk identification

Risk identification requires reasonably foreseeable risks that have the potential to have a meaningful impact on the university to be identified. A risk to the University is any event or action that could have a negative impact on the University. This includes events that could:

- Lead to death or injury
- Lead to financial loss to the University
- Damage the University's reputation or lead to adverse media regarding the University
- Lead to damage to the physical environment, including land, water or air quality

Business risks arise as much from the possibility that opportunities will not be realised as they do from the possibility that threats will materialise, errors be made, or damage/injury occur.

Within the University, risk identification occurs in two ways:

Structured risk identification: Time is specifically allocated, and appropriate staff are convened, to identifying risks; this is usually carried out within the operation of the Senior Staff Advisory Committee.

Ad-hoc risk identification: Risks are identified during the normal course of work; these risks are managed at the time and reported by staff to the Senior Staff Advisory Committee.

Structured risk identification:At least once per year, the Vice-Chancellor will convene a risk identification workshop.

The workshop will follow a structured process to identify risks within the University. Newly identified risks will be recorded in the University's risk register.

Ad-hoc risk identification

Clearly, many risks will be identified by staff during the course of their work within the University. When risks are identified in this way staff must determine whether immediate action is necessary to reduce the risk, and if so carry it out; for example there may be a safety risk where immediate action is necessary to prevent injury.

All identified risks must be entered in the University's Risk Register by the Risk Manager. As a minimum the following information must be included:

- The name of the risk: this is a short, meaningful title so that the risk can readily be referred to in the future.
- A full description of the risk, including information on how the risk impacts on the University.
- The causes of the risk.
- Details of the controls that are currently in place to manage the risk, including temporary controls that are being used to manage the risk until further action is taken.
- Details of any other controls that are planned for the risk, including a due date for implementation and a person responsible for putting the control in place.
- The risk rating determined from the assessment of the potential consequences and likelihood for the risk.

Risk rating

All identified risks shall be assessed to determine the overall ranking for the risk. Risks are ranked in the following four categories:

- High
- Significant
- Moderate
- Low

The ranking of a risk determines:

- The nature of further action that is required, and the urgency with which further action should be undertaken.
- The reporting requirements for the risk, including who the risk is reported to.
- How the risk is monitored.

All risks within the University are ranked using a common scale that assesses:

- The potential consequences if the risk were to occur, and
- the likelihood of the University being impacted in that way.

A common approach to risk ranking is necessary to ensure that the largest risks to the University can readily be identified and management of risks can be prioritised in a way that has the greatest overall benefit to the University.

Likelihood rating

The number of times within a specified period which a risk may occur either as a consequence of business operations or through failure of operating systems, policies or procedures.

Assessing likelihood

When assessing likelihood, it is important to note that the likelihood score for a risk needs to reflect the likelihood of the consequence occurring, rather than the likelihood of the risk occurring.

For example: There may be a risk that staff or students are injured as a result of assaults. The consequences of an assault may range from a relatively minor injury to death, depending on the circumstances of the incident.

Whilst assaults are unfortunately not uncommon within the university, the likelihood of staff or students dying as a result of an assault is considered to be unlikely.

Overall it is clear that this risk would be considered to be Significant to High. To highlight the serious nature of the risk, it would therefore be appropriate to give this risk the risk scoring that shows the High risk rating, and therefore score this risk with a consequence of 5 and a likelihood of C.

Risk controls

Assess how risks will be treated

The objective of the step is to identify how the identified risks will be treated. Risk treatment involves identifying the options for treating each risk, evaluating those options, assigning accountability (for High, Serious and Medium risks), preparing risk treatment plans and implementing them. The following options are available for treating risks and may be applied individually or in combination, with due consideration of risk appetite:

- **Avoid the risk:** Not to proceed with the activity or choosing an alternative approach to achieve the same outcome. Aim is risk management, not aversion.
- **Mitigate:** Reduce the likelihood - Improving management controls and procedures. Reduce the consequence - Putting in place strategies to minimise adverse consequences, e.g. contingency planning, Business Continuity Plan, liability cover in contracts.
- **Transfer the risk:** Shifting responsibility for a risk to another party by contract or insurance. Can be transferred as a whole or shared.
- **Accept the risk:** Controls are deemed appropriate. These must be monitored and contingency plans developed where appropriate.

Identifying controls

To recognise existing or required controls to mitigate the identified risks:

Consider ways to remove the risk. Alternative methods of working may be available that mean that the risk no longer represents a threat to the University.

Consider the causes of the risk – information on causes is listed with the information for the risk. Consider what can be done to remove causes, or reduce the likelihood of the causes creating the risk.

Consider the consequences of the risk – if the risk were to occur, what would need to be done to reduce the consequences? This can include controls that reduce the amount of damage that occurs, for example: only having limited amounts of corrosive materials available in order to limit the amount of injury and environmental damage that can result from a spill.

Alternatively, controls for consequences can be recovery and clean-up controls once the damage has occurred, for example: first aid and emergency response procedures to recover from and limit further injury once a safety accident has occurred.

Outsource management of the risk. A common example of a risk control that is outsourced is the use of external security contractors, who may be provided with better training and resources than the University could supply itself. The improved skills and resources of an outsourced provider may reduce the risk of assaults for all staff and students.

Provide insurance. Insurance is a common control for providing post-event recovery from financial losses. Whilst insurance is a very common risk control, it needs to be remembered that insurance will only cover financial losses and will not necessarily provide recovery from other types of damage, for example damage to reputation that may occur following a major incident.

Control implementation

Where controls have been identified for a risk, the Risk Manager must update the University's risk register to show:

- Causes of the risk.
- Implication of the risk with amendment existing controls (if they exist).
- What any existing mitigating controls are.
- What actions are being undertaken to put further controls in place, or maintain existing controls and by when.
- Who is responsible for ensuring the controls are in place.

The action items entered into the risk register shall be followed up and reported on by the Risk Owner at each Senior Staff Advisory Committee Meeting,

Risk Monitoring and Reporting.

It may also be appropriate to include other information such as suppliers who are providing

resources for the control, or the funding process that is being relied on to purchase the control.

All Risks rated as moderate, significant or high, in the risk identification process will be reviewed by the Senior Staff Advisory Committee (SSAC) regularly. This review will be via either:

- The Risk Manager reporting on new risks identified by staff during the course of their work since the last SSAC meeting; and/or
- Risk Owners providing a report on the status of their assigned risk in line with the Risk Owner's Report Format to the SSAC/Senator (see below); and/or
- The Risk Manager reporting on reviews of the Risk Register following a Structured Risk Identification Workshop each year, or any review of the Risk Register by the Executive.

Risk Owner's report format to the SSAC

The Risk Owner's reports to the Senator should outline that the risk controls are to indicate:

- Causes of the risk.
- Implication of the risk with amendment existing controls (if they exist).
- What any existing mitigating controls are.
- What actions are being undertaken to put further controls in place, or maintain existing controls and by when.
- Who is responsible for ensuring the controls are in place.

The above elements for the Risk Owner's reports are in line with those required in the Risk Register.

Role of Senator/Senior Staff Advisory Committee (SSAC) review

The role of the SSAC in their review of Risk Owner's reports is to advise the Vice-Chancellor and Chancellor on acceptability and relevance of the controls detailed in these reports. SSAC members should make recommendations to the Vice-Chancellor and President either at the meeting, or via the Risk Manager at a later date.

Following the presentation of Risk Owner's reports at the SSAC, the next steps will be:

- The Risk Manager will liaise with the Risk Owners and the Vice-Chancellor and President to confirm the recommendations of the SSAC.
- The Risk Manager will prepare a draft Risk Manager's Report for the next Executive meeting.
- The Executive will review and endorse or amend the information contained in the draft Risk Manager's Report.
- This endorsed or amended draft Risk Manager's report should then be

provided as the Risk Manager's Report at the next Audit and Risk Management Committee meeting or at the next Senior Staff Advisory Committee meeting for information and review, whichever meeting falls sooner.

This process should proceed continuously throughout the year, with Risk Owner's supplying an updated Risk Owner's report at least quarterly to the SSAC, or at each meeting, if requested by the Risk Manager.

Risk reporting responsibilities are further detailed in Appendix Two – Risk Reporting Responsibilities.

To ensure proper management of risks at a strategic level, the Executive should review the University's risk register on a quarterly basis to ensure:

- New risks to the University are identified and considered.
- Existing risks are monitored to identify any changes which may impact on the University.
- Risks have been properly assessed and recorded in the University's risk register together with relevant information such as existing risk controls.
- An appropriate person has been nominated for all new risk controls and new risk controls are being implemented according to the planned schedule.
- Existing risk controls are still in place and operating effectively.

Appendices

General definitions

Risk management: For the University refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the University. The process of managing risk is achieved through the systematic application of policies, procedures and practices to establish the context, identify, analyse, evaluate, treat, monitor and communicate risk.

Risk: Within the University, a risk to the business is any threat of an action or event to our industry or activities that has the potential to threaten the achievement of our business objectives. Business risk arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.

Likelihood: Likelihood measures the expected frequency of a risk occurring. Typically, a subjective judgment based on past experience and the insights of persons familiar with the activity.

Consequence: Consequence measures the expected level of impact on the University and its objectives, should the risk occur.

Risk owner: Risk owners are individuals within the University with primary responsibility for managing a particular risk.

Risk reporting responsibilities

The following risk reporting responsibilities exist within the University.

Reporting responsibilities: Audit and Risk Management Committee

The Audit and Risk Management Committee is responsible for receiving risk reports from the Vice-Chancellor and forwarding risk information to Council as appropriate.

Reporting responsibilities: Vice-Chancellor

The Vice-Chancellor will arrange for a Risk Manager's Report to be provided at each Audit and Risk Management Committee meeting. The Vice-Chancellor must, as a minimum, ensure this report contains:

- all changes to Significant and High risks, including any new Significant or High risks, at every meeting; and
- significant changes to risks or risk controls.

The Vice-Chancellor will ensure that the full risk register for the University is provided to the Audit and Risk Management Committee at least once per year, for their information and comment.

Reporting responsibilities: The Executive

The Executive shall review the overall risk management on the basis of recommendations provided by the Risk Manager, Risk Owners and the Senior Staff Advisory Committee and provide the Vice-Chancellor with information on:

- all risks to the University including newly identified risks
- significant changes to risks or risk controls
- changes to the University's operating environment that may impact on risks or risk management activities
- progress reports on the implementation of risk controls

The Executive shall also provide recommendations to the Vice-Chancellor regarding the Risk Manager's Report for the Audit and Risk Management Committee and conduct a quarterly review of the Risk Register.

Reporting responsibilities: Senior Staff Advisory Committee (SSAC)

The SSAC shall receive reports from the Risk Manager and each Risk Owner at each meeting. The SSAC will review these reports and make recommendations via the Risk Manager to the Executive on:

- all risks to the University including newly identified risks
- significant changes to risks or risk controls
- changes to the University's operating environment that may impact on risks or risk management activities

- progress reports on the implementation of risk controls.

Reporting responsibilities: Risk Manager

The Risk Manager shall ensure that information on new risks is reported to the SSAC. The Risk Manager shall also ensure that information on risks is escalated immediately to the appropriate Cost Centre Manager or the Vice-Chancellor if further action to manage a risk within their area of control is required. The Risk Manager shall prepare the Risk Register to be reviewed by the Executive on a quarterly basis.

Reporting responsibilities: Senior staff

Senior Staff must forward information from the Senior Staff Advisory Committee, or from their supervising staff, to staff and students within their area of management. Information may include details of new risks or new risk treatments that staff and students must comply with.

Reporting responsibilities: All staff

All Staff are responsible for reporting information on newly identified risks to their supervisor and the Risk Manager.