# INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

# RISK MANAGEMENT MANUAL

***(Policy, Framework & Guidelines)***

## Risk Management Office

## TABLE OF CONTENTS

## 1.0 INTRODUCTION

1.1. On 26th November 2020, International Islamic University Malaysia (IIUM) has approved on the separation of the risk and audit oversight functions. Pursuant to this, the Board of Governors (BOG) Meeting No. 60 held on 25th May 2021 has endorsed the establishment of the **Risk Management Office (RMO)** as well as the appointment of the **University Risk Management Committee (URMC)** members.

1.2. Risk is inherent in all academic, administrative and business activities, and every member of the University community continuously manages risk. IIUM recognizes that the aim of Enterprise Risk Management (ERM) is not to eliminate risk totally, but rather to provide the structural means **to identify, prioritize and manage** the risk involved in all University activities.

1.3. IIUM ERM is an integral part of best management practices and an essential element of **good governance**, as it **improves quality decision making** and **enhances outcomes and accountability**. The intent is to embed risk management in a very practical way into **business processes and functions** via key approval processes, review processes and controls, not to impose risk management as an extra requirement.

1.4. This manual consists of three sections in which:
- i) SECTION A: Policy
- ii) SECTION B: Framework
- iii) SECTION C: Guidelines

## 2.0 INTERPRETATION

In this manual unless the context otherwise requires: -

- i) "Centre of Studies" or "COS" means the centres that are named as Kulliyyah, Institutes or Centre that represent a branch or branches of unified concept of knowledge based on the basis concept of Islamic principles and philosophy of knowledge and education as prescribe in IIUM constitution.
- ii) "Division and Office" or "D&O" means the registered offices and divisions for the time being of the University.
- iii) "IIUM" means the International Islamic University Malaysia.
- iv) "ISO31000" means the ISO31000 latest version Risk Management – Principles and Guidelines.
- v) "BOG" means Board of Governors and it is a management and policy making authority of the University.
- vi) "University" refers to the International Islamic University Malaysia.
- vii) "Manual" means the IIUM Enterprise Risk Management Policy, Framework and Guidelines.
- viii) "Policy" means the IIUM Risk Management Policy, and
- ix) "SBU" means the Strategic Business Units.
- x) "Staff" means any person employed under a contract of service with the University

xi) "University Community" means all staff (permanent, contract and part-time), students, business operators, cleaning workers under IIUM Holdings subsidiaries, assigned contractors who study and work in the respective campuses.

xii) "Controlled Entities" means all legal business entities under the purview of IIUM BOG such as IIUM Holdings Sdn. Bhd. and its subsidiaries.

## 3.0 OBJECTIVES

3.1 The objective of this Manual is to ensure that the University makes informed decisions with respect to the activities that it undertakes by appropriately considering both risks and opportunities.

3.2 The Manual is therefore to detail the IIUM Risk Management Policy, Framework and Guidelines to all individuals within the University to enable staff at all levels to understand the policies and structure adopted within the University to ensure the management of risk on an organization-wide basis.

3.3 The Manual is thus intended as a reference manual for all staff in IIUM including its business entities on an ongoing basis. The Office in-charge of risk management is the custodian of this manual and is responsible for ensuring all staff are aware of the IIUM Risk Management Policy.

## 4.0 SCOPE

4.1 Risk management must be effective at all levels of the University. Staff should understand what acceptable risk within the University is and what their individual roles are in relation to the management of risk.

4.2 This Manual amongst others covers:

i) Purpose and Objectives of the Manual
ii) IIUM Enterprise Risk Management Framework
iv) IIUM Risk Management Policy
v) Definition of Risk Management (RM) and Enterprise Risk Management (ERM)
vi) Risk Management Governance and Organisation
    a) Ownership and accountability
    b) Structure and Administration of Risk Management
vii) ERM Guideline (Methodology and Process)
viii) Training and Awareness
ix) Communication and Reporting

4.3 The ISO31000 (Risk Management: Principles and Guidelines) provides principles and generic guidelines on risk management. This International Standard can be applied throughout IIUM and to a wider range of activities, including strategy design and decision making, operations, processes, functions, projects, products, services and assets.

## 5.0 PRINCIPLES

5.1 The risk management is a process that is supported by a set of principles adopted from ISO31000 latest version for the risk management implementation to be effective, IIUM shall, at all levels, comply with the principles below:

| No. | Principles (ISO31000:2018) | Application |
|---|---|---|
| 1. | Risk management **creates and protects value** | Risk management contributes to the demonstrable achievement of objectives and improvement of University performance. |
| 2. | Risk management is an **integral part** of all activities of the University | Risk management is not a stand-alone activity that is separate from the main activities and processes of IIUM. Risk management is part of the responsibilities of management and an integral part of all University processes, including strategic planning and all project and change management processes. |
| 3. | Risk management is **structured and comprehensive** | Risk management is a structured and comprehensive approach to contribute for consistent and comparable results. |
| 4. | Risk management is **customised** | Risk management framework and process are customized and proportionate to the University's external and internal context related to its objectives. |
| 5. | Risk management is **inclusive** | Appropriate and timely involvement of stakeholders and decision makers at all levels of the University ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views considered in determining risk criteria. |
| 6. | Risk management is **dynamic** | Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risk emerge, some change and others disappear. |
| 7. | Risk management is based on the **best available information** | The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholders' feedback, observation, forecasts and expert judgements. |

| | | |
|---|---|---|
| 8. | Risk management takes **human and cultural factors** into account | Risk management recognized the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the University's objectives. |
| 9. | Risk management facilitates **continual improvement** of the University | Strategies should be developed to improve the risk management maturity and effectiveness. |

## SECTION A: IIUM RISK MANAGEMENT POLICY

## 6.0 OBJECTIVES

6.1 The IIUM Risk Management Policy is established to:

i) Protect the University from those risks of significant likelihood and consequence in the pursuit of the University's goals and objectives.
ii) Ensure the integration of risk management in decision making process throughout the University.
iii) Complement other University's internal controls in ensuring its objectives and goals are met; and
iv) Refers as a standard to safeguard the University's assets consisting amongst others of, people, finance, property, information and reputation of the University as well as in meeting all legal and statutory requirements.

6.2 Related Procedures and Guidelines

The related procedures and guidelines can be referred amongst the latest:

i) ISO37001 – Anti-Bribery Management System (ABMS)
ii) ISO31000 – Risk Management – Guidelines
iii) ISO27001 – Information Security Management System (ISMS)
iv) ISO9001 – Quality Management System (QMS)
v) ISO45001 – Occupational Health & Safety Management Systems
vi) IEC31010 – Risk Management – Risk assessment Techniques
vii) ISO31022 – Risk Management – Guidelines for the Management of legal Risk
viii) Other ISO standard that relevant to the risk management practices.

## 7.0 THE POLICY

7.1 Policy Scope

7.1.1 This Policy is applicable to all staff of the following:

i) Centre of studies.

ii) Divisions and offices.
iii) Strategic business units; and
iv) Controlled entities, and entities that are incorporated from the University's legal status.

7.1.2 The Policy encapsulates the component of IIUM Risk Management Framework which details the approach to risk management, all roles and responsibilities, key aspects of the process and terms of reference.

7.1.3 The University Risk Management process involves all levels of the University in the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context (external and internal) and assessing, treating, monitoring, reviewing, recording and reporting risks.

7.2 Policy Statement

7.2.1 IIUM adopts the risk management approach and general methodology specified in the latest version of ISO31000 – Risk Management – Guidelines on implementation.

7.2.2 All IIUM business processes and functions will adopt a risk management approach consistent with the latest version of ISO31000 – Risk Management Process in their approval, review and control processes. The IIUM risk management approach and methodology for this purpose is as set out in the risk framework and guidelines.

7.2.3 The risk management committee of each office shall develop a proper risk management process and associated documentation appropriate to their domain.

## SECTION B: FRAMEWORK

## 8.0 RISK MANAGEMENT FRAMEWORK

8.1 The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout IIUM at all levels. The framework assists the management of risks effectively through the application of the risk management process at varying levels and within specific contexts of IIUM. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant University levels.

8.2 Figure 1 below illustrates the relationship between the components of the framework for managing risk as described in the ISO31000:2018 Standard. It includes the essential steps in the implementation and ongoing support of the risk management process. The components of this framework are:

i) Leadership and commitment
ii) Integration
ii) Design
iii) Implementation
iv) Evaluation
v) Continual improvement of the framework

Figure 1: Relationship between the components of the framework for managing risk


### 8.2.1 Leadership and Commitment

8.2.1.1 Top management and oversight bodies should ensure that risk management is integrated into all University activities and should demonstrate leadership and commitment by:

i) customizing and implementing all components of the framework;
ii) issuing a statement or policy that establishes a risk management approach, plan or course of action;
iii) ensuring that the necessary resources are allocated to managing risk;
iv) assigning authority, responsibility and accountability at appropriate levels within the University.

This will help the University to:

a) Align risk management with its objectives, strategies and cultures.
b) Recognize and address all obligations, as well as its voluntary commitment.

c) Establish the amount and type of risk that may or may not be taken to guide the development of risk criteria, ensuring that they are communicated to the University and its stakeholders.
d) Communicate the value of risk management to the University and its stakeholders.
e) Promote systematic monitoring of risks.
f) Ensure that the risk management framework remains appropriate to the context of University.

8.2.1.2 Top management is accountable for managing risk while the oversight bodies are accountable for overseeing risk management. Their expectation is to:

i) Ensure that risks are adequately considering when setting the University's objectives.
ii) Understand the risks facing the University in pursuit of its objectives.
iii) Ensure that systems to manage such risks are implemented and operating effectively.
iv) Ensure that such risks are appropriate in the context of the University's objectives.
v) Ensure that information about such risks and their management is properly communicated.

Management shall:

a) Define and endorse the risk management policy

The Board of Governors (BOG) shall approve the risk management policy. The policy should be used as the basis for all centre of studies, divisions and offices, strategic business units and other related controlled entities in designing and implementing the risk management process.

b) Ensure that the culture and risk management policies are aligned

Embedding risk management involves an environment that can demonstrate a change in mindset and culture to be more risk-aware from management and staff at all levels. University's effective leadership can shape culture by encouraging the application of risk management through organisational recognition and reward systems.

This risk-aware culture is to be institutionalized into daily operational and business activities for effective risk management at the University, operational, project or team levels.

c) Align risk management objectives with the objectives and strategies of the University

The management should align their risk management objectives with the University's strategies in order to mitigate the risk elements and reduce the adverse consequences to the objective's achievement. The alignment may be conducted during the annual strategic planning process,

d) Determine risk management performance indicators that align with the University performance indicators

The management may align its risk management performance indicators (PI) with the University's performance indicators by:

i) Considering the range of key organisational/business drivers.
ii) Incorporating the risk management into the University's scorecards; and
iii) Integrating the risk management performance assessment into the overall organisational performance management system.

e) Ensure legal and regulatory compliance

IIUM shall ensure legal and regulatory compliance within all jurisdictions in which it operates to effectively mitigate legal and regulatory risks.

f) Assign accountabilities and responsibilities at appropriate levels

The management shall assign appropriate levels of authority, accountability and responsibility for managing risks at all levels as defined in this Manual and the University's approving authority.

g) Ensure that the necessary resources are allocated to risk management

The management shall provide and facilitate sufficient resources and infrastructure to implement the risk management framework, consisting of:

i) People and skills.
ii) Documented processes and procedures.
iii) Information system and databases, and
iv) Financial and any other resources for specific risk treatment activities.

h) Communication the benefits of risk management to all stakeholders

As part of good governance, an effective risk management enables management to improve outcomes by identifying and

analysing the issues and providing a systematic way to make informed decisions. The risk management provides a reasonable assurance to the stakeholders that the objectives are achievable with its tolerable risk appetite.

i) Ensure that the framework for managing risk continues to remain appropriate

The management shall ensure that the framework is reviewed on a regular basis to ensure its relevancy to changes in the external and internal context.

### 8.2.2 Integration

8.2.2.1 Integrating risk management relies on an understanding of University organisational structure and context. Structures differ depending on the University's purpose, goals and complexity. Risk is managed in every part of the University's structure. All staff have responsibility for managing risk.

8.2.2.2 Governance guides the course of the University, its external and internal relationship, and the rules, processes and practices needed to achieve its purpose. Management structures translate governance direction into the strategy and associated objectives required to achieve desired levels of sustainable performance and long-term viability. Determining risk management accountability and oversight roles within the University are integral parts of the University's governance.

8.2.2.3 Integrating risk management into an organization is a dynamic and iterative process and should be customized to the University's needs and culture. Risk management should be a part of, and not separate from the University purpose, governance, leadership and commitment, strategy, objectives and operations.

### 8.2.3 Design

8.2.3.1 Understanding the University and its context. Examining the University's context may include, but is not limited to:

a) The social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local.
b) Key drivers and trends affecting the objectives of the University.
c) External stakeholders' relationship, perceptions, values, needs and expectations.
d) Contractual relationship and commitment.

e) The complexity of Information and Communication Technology (ICT), digital environments, printed media, social media, networks and dependencies.

8.2.3.2 Examining the University's internal context may include, but is not limited to:

a) Vision, mission and values.
b) Governance, University organisational structure, roles and accountability.
c) Strategy, objectives and policies.
d) The University culture.
e) Standards, guidelines and models adopted by the University,
f) Capabilities, understood in terms of resources and knowledge such as capital, time, intellectual property, process systems and technologies.
g) Data, information systems and information flows.
h) Relationship with internal stakeholders.
i) Contractual relationships and commitments.
j) Interdependencies and interconnections.

8.2.3.3 Top management and oversight bodies should demonstrate and articulate their continual commitment to risk management through a policy, a statement or other forms that clearly convey the University's objectives and commitment to risk management. The commitment should include, but is not limited to:

i) The University's purpose for managing risk and links to its objectives and other policies.
ii) reinforcing the need to integrate risk management into the overall culture of the University.
iii) Leading the integration of risk management into core business activities and decision making.
iv) Authorities, responsibilities and accountabilities.
v) Making the necessary resources available.
vi) The way in which conflicting objectives are dealt with.
vii) Measurement and reporting within the University's performance indicators.
viii) Review and improvement.

8.2.3.4 Top management should emphasis that risk management is a core responsibility of all staff and risk owners.

8.2.3.5 The management shall provide and facilitate sufficient resources and infrastructure to implement the risk management framework, consisting of:

i) People and skills.
ii) University's processes, methods and tools to be used for managing risk.
iii) Documented processes and procedures.
iv) Information system and databases, and
v) Professional development and training needs.

8.2.3.6 The University should establish an approved approach to communication and consultation to support the framework and facilitate the effective application of risk management. Communication involves sharing information with targeted audiences. Consultation also involves participants providing feedback with the expectation that it will contribute to and shape decisions or other activities. Communication and consultation methods and contents should reflect those expectations of stakeholders, where relevant. Communication and consultation should be timely and ensure that relevant information is collected, collated, synthesized and shared as appropriate, and that feedback is provided and improvements are made.

### 8.2.4 Implementation

8.2.4.1 The University should implement the risk management framework by:

a) Developing an appropriate plan including time and resources.
b) Identifying where, when and how different types of decisions are made across the University, and by whom.
c) Modifying the applicable decision-making processes where necessary.
d) Ensuring that the University's arrangements for managing risk are clearly understood and practiced.

8.2.4.2 Successful implementation of the framework requires the engagement and awareness of stakeholders. This enables University to explicitly address uncertainty in decision-making, while also ensuring that any new or subsequent uncertainty can be considered as it arises.

8.2.4.3 Properly designed and implemented, the risk management framework will ensure that the risk management process is a part of all activities throughout the University, including decision-making and that changes in external and internal contexts will be adequately captured.

### 8.2.5 Evaluation

8.2.5.1 In order to evaluate the effectiveness of the risk management framework, the University should:

i) Periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviour.
ii) Determine whether it remain suitable to support achieving the objectives of the University.

### 8.2.6 Improvement

8.2.6.1 The University should continually monitor and adapt the risk management framework to address external and internal changes. In doing so, the University can improve its value.

8.2.6.2 The University should continually improve the suitability. Adequacy and effectiveness of the risk management framework and the way the risk management process is integrated.

8.2.6.3 As relevant gaps or improvement opportunities are identified, the University should develop plans and task and assign them to those accountable for implementation. Once implemented, these improvements should contribute to the enhancement of risk.

8.3 The IIUM Risk Management Framework involves three key steps:

i) Setting the corporate strategy on an annual basis, aligning risk management to business objectives.
ii) Adopting a formal and standardized process methodology for risk management across the business; and
iii) Maintaining a structure that assigns ownership and responsibility for monitoring and updating risk management.

8.4 The Framework should be used for the following:

i) Communicate policies and procedures for managing risk on an enterprise-wide basis.
ii) Provide guidelines for responsibilities and duties in managing risk.
iii) Create an understanding of the undertaken processes in which contributing to the success of the risk management implementation from the University wide perspective.
iv) Demonstrate how risk relates to the achievement of corporate objectives; and
vi) Emphasis the importance of risk management towards IIUM vision and mission as well as IIUM strategic direction.

## 9.0 OWNERSHIP AND ACCOUNTABILITY

9.1 All IIUM staff are responsible for the effective identification and management of risks.

9.2 The ownership of the IIUM Risk Management Policy rests with the Risk Management Office (RMO).

9.3 The University Risk Management Committee (URMC) or any designated committee assumes overall responsibility for measuring and monitoring the risk management performances across IIUM.

9.4 The Risk Management Office (RMO) shall be the Secretariat of URMC or any designated committee and Risk Management Working Committee (RMWC) or any designated committee with a responsibility to plan, develop, coordinate and

communicate risk management programmes and monitor adherence to the Policy.

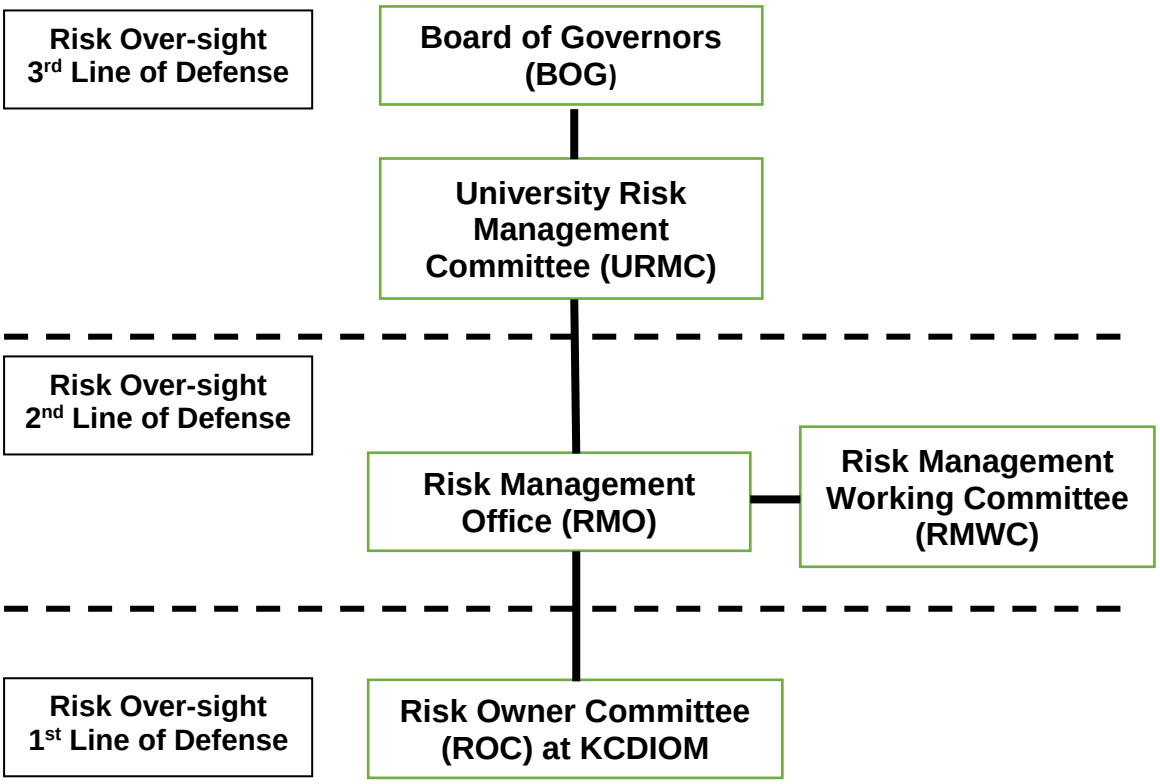
9.5 The Policy does not diminish nor supersede the important role that the IIUM line management plays in the overall management of risk.

## 10.0 THE STRUCTURE AND ADMINISTRATION OF RISK MANAGEMENT

### 10.1 IIUM Risk Management Oversight Structure

10.1.1 IIUM risk reporting structure is depicted in Figure 2 as follows:

**Figure 2: IIUM Risk Management Oversight Structure**




### 10.2 Critical Success Factors

10.2.1 The critical success factors to must be considered in ensuring successful implementation of IIUM Risk Management are as follows:

i) Strong and visible support from Board of Governors and top management.

ii) Dedicated group of cross functional staff to drive IIUM Risk Management implementation at operational level.

iii) Closely link IIUM Risk Management to key strategic and financial objectives of the University and to the business process.

iv) Promoting the IIUM Risk Management is a framework to improve the existing processes within the University.
v) Adopting any suitable external ideas or benchmarking any best practice approaches for improving the existing risk management framework, and
vi) Continuously make improvement and leveraging on “early wins” initiatives.

## 10.3 Management Commitment

10.3.1 Commitment from IIUM top management is shared with all line managers at all levels by embedding the IIUM Risk Management methodology into the business planning processes via any performance measurement tools as determined by the University. Identified risks are managed by applying the Risk Management processes. Vertical and horizontal communications are essential in ensuring pro-active responses to mitigate probable impact and losses.

## 10.4 Roles and Responsibilities

10.4.1 All staff members including appointed members of the respective board and committee have a role in the University’s risk management. However, their specific roles differ based on their capacity and functions in the University. The roles of the various entities within the University are identified as follows:

### 10.4.1.1 Role of the Board of Governors (“BOG”)

The BOG as the highest authority of management and policy making of the university is to ensure that the risk management and internal control processes are in place within the University and the process is effective and ongoing.

### 10.4.1.2 Role of the University Risk Management Committee (“URMC”)

The URMC oversees the effective implementation of the University’s Risk Management Policy.

### 10.4.1.3 Role of the Risk Management Working Committee (“RMWC”)

The RMWC which acts as a “think tank” group is to be chaired by the Director of Risk Management Office (RMO). The members shall be determined by the chairperson in order to facilitate the process of implementing the university risk management programme. The members may be represented from the offices that could assist in risk assessment and responsible for

embedding risk management within the operational management processes of the University. This includes,

i) identification of risks impacting the University;
ii) determining priorities;
iii) assessing risk tolerance;
iv) developing risk management plans; and
v) monitoring progress and implementation of plans.

#### 10.4.1.4 Role of the Centre of Studies/ Divisions/ Offices/ Strategic Business Units (COS/D&O/SBU) Risk Owner Committee ("ROC")

The roles and responsibilities of the COS/D&O/SBU Risk Owner Committee (ROC) are to:

i) Instil awareness of risk management as a cultural approach into the COS/D&O/SBU working environment, and
ii) Report any risks that need attention and action from the University top management through the office that is responsible for risk management of the University.

#### 10.4.1.5 Role of Staff

All staff have a responsibility in ensuring that effective management of risks is implemented within the context of their area of responsibilities, including the identification and disclosure of potential or emerging risks.

## 10.5 Resources and Implementation

10.5.1 The resources required to implement the University's risk management policy should be clearly established at each level of management and within each business unit. Those involved in risk management should have their roles in coordinating risk management policy/strategy clearly defined. The same clear definition is also required for those involved in the audit and review of internal controls and facilitating the risk management process.

## 10.6 Effective Date

10.6.1 The commencement date for this Manual shall be decided and approved by the University Risk Management Committee (URMC).

## 10.7 Ownership, Accountability and Maintenance of Manual

10.7.1 The ownership, formulation and maintenance of the IIUM Risk Management Manual rests with the Risk Management Office (RMO);

and should be assisted by the Risk Management Working Committee (RMWC) or equivalent committee established by the University's authority.

## SECTION C: GUIDELINES

## 11.0 THE RISK MANAGEMENT PROCESS

11.1 The University shall adopt the ISO31000 latest version of Risk Management Process at all levels of the University – strategic, operational and tactical as per Figure 3 below:

**Figure 3: ISO31000:2018 Risk Management Process**


### 11.1.1 Communication and Consultation

11.1.1.1 The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required.

Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making. Close coordination between the two should facilitate factual, timely, relevant, accurate and understandable exchange of information, taking into account the confidentiality and integrity of information as well as the privacy rights of individuals.
Communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process.

11.1.1.2 Communication and consultation aims to:

i) Bring different areas of expertise together for each step of the risk management process;
ii) Ensure that different views are appropriately considered when defining risk criteria and when evaluating risks;
iii) Provide sufficient information to facilitate risk oversight and decision-making; and
iv) Build a sense of inclusiveness and ownership among those affected by risk.

### 11.1.2 Scope, Context and Criteria

#### 11.1.2.1 General

The purpose of establishing the scope, the context and criteria is to customize the risk management process, enabling effective risk assessment and appropriate risk treatment. Scope, context and criteria involve defining the scope of the process and understanding the external and internal context.

#### 11.1.2.2 Defining the Scope

11.1.2.2.1 The University should define the scope of its risk management activities.

11.1.2.2.2 As the risk management process may be applied at different levels (e,g, strategic, operational, programme, project or other activities), it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with University objectives.

11.1.2.2.3 When planning the approach, considerations include:

i) Objectives and decisions that need to be made;
ii) Outcomes expected from the steps to be taken in the process;
iii) Time, location, specific inclusions and exclusions;
iv) Appropriate risk assessment tools and techniques;

v) Resources required, responsibilities and records to be kept;
vi) Relationships with other projects, processes and activities.

### 11.1.2.3 External and Internal Context

11.1.2.3.1 The external and internal context is the environment in which the organization seeks to define and achieve its objectives.

11.1.2.3.2 The context of the risk management process should be established from the understanding of the external and internal environment in which the organization operates and should reflect the specific environment of the activity to which the risk management process is to be applied.

11.1.2.3.3 Understanding the context is important because:
i) Risk management takes place in the context of the objectives and activities of the University;
ii) Organizational factors can be a source of risk; and
iii) The purpose and scope of the risk management process may be interrelated with the objectives of the organisation.

### 11.1.2.4 Defining Risk Criteria

11.1.2.4.1 The University should specify the amount and type of risk that it may or may not take, relative to objectives. It should also define criteria to evaluate the significance of risk and to support decision-making processes. Risk criteria should be aligned with the risk management framework and customised to the specific purpose and scope of the activity under consideration. Risk criteria should reflect the University's values, objectives and resources and be consistent with policies and statements about risk management. The criteria should be defined taking into consideration the University's obligations and the views of stakeholders.

11.1.2.4.2 While risk criteria should be established at the beginning of the risk assessment process, they are dynamic and should be continually reviewed and amended, if necessary.

11.1.2.4.3 To set risk criteria, the following should be considered:

i) The nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible);
ii) How consequences (both positive and negative) and likelihood will be defined and measured;
iii) Time-related factors;
iv) Consistency in the use of measurements;
v) How the level of risk is to be determined;
vi) How combinations and sequences of multiple risks will be considered; and
vii) The University's capacity.

### 11.1.3 Risk Assessment

11.1.3.1 General

11.1.3.1.1 Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

11.1.3.1.2 Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary.

### 11.1.3.2 Risk Identification

11.1.3.2.1 The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks.

11.1.3.2.2 The organisation can use a range of techniques for identifying uncertainties that may affect one or more objectives. The following factors, and the relationship between these factors, should be considered:
a) Tangible and intangible sources of risk;
b) Causes and events;
c) Threats and opportunities;
d) Vulnerabilities and capabilities;
e) Changes in the external and internal context;
f) Indicators of emerging risks;
g) The nature and value of assets and resources;
h) Consequences and their impact on objectives;
i) Limitations of knowledge and reliability of information;
j) Time-related factors; and
k) Biases, assumptions and beliefs of those involved.

11.1.3.2.3 The organisation should identify risks, whether their sources are under its control or not. Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences.

11.1.3.2.4 The risk identification process will enable the risk owner to create a cause-and-effect diagram and identification of risk responses.

11.1.3.2.5 Key questions in risk identification process:

a) What might happen?
b) How might it happen?
c) What are the current risk response mechanisms in place to mitigate this risk?
d) What are the consequences of each risk?
e) What are the stakeholder expectations of the University's performance?
f) What is the potential cost in time, money and disruption to customers of each risk?

11.1.3.2.6 Thus, the risk identification process will allow the University to generate a comprehensive list of possible loss scenario or opportunities and its potential impacts emanating within the possible **sources of risk**.

11.1.3.2.7 Possible methods of identifying risks are:

i) Brainstorming
ii) Surveys and questionnaires
iii) Expert judgement
iv) Structured interviews
v) Focus group discussions
vi) Strategic and business plans including Strength, Weakness, Opportunity and Threat (SWOT) analysis
vii) Results and reports from audits, inspections and site visits
viii) Historical records, incident databases and analysis of failures
ix) Review selected performance indicators

11.1.3.2.8 The risk statement or description should consider the following characteristics:

a) Always 'negative' in description and 'relevant' to the University
b) Should be clear, concise, specific and easily understood
c) Based on causes of risks not consequences

11.1.3.2.9 A Risk Owner (RO) must be assigned to the risk identified. The RO is the person with the accountability and authority to manage the risk identified.

11.1.3.2.10 The identified risks are then summarised into risk categories. The risk categories are a classification system or an approach to summarise the identified risks. **The risk categories are not exhaustive and can be reviewed** during brainstorming workshops and actual risk evaluation. Changing business conditions and decisions made in the course of running the business, each time we look at them. As such, it is important to have frequent and explicit discussion about risk, in order to maintain continuous awareness of which risks are significant.

**Table 1: Sample of Risk Categories**

| No. | Categories | Description |
|---|---|---|
| 1. | Strategic | Losses due to error or misjudgement in the selection of strategy or the execution of the strategy or exposure to loss resulting from a strategy that turns out to be defective or inappropriate. |
| 2. | Financial | Risk associated with the finances of the University, including loan interest charges, exchange rates, taxation, borrowings and credit, government grant. Error in asset valuation (over or undervaluation), liabilities, spending beyond limit, negative cash flows or any other direct and indirect losses affecting other elements of the University's finances. |
| 3. | Operational | Risk arising from execution of a company's business function which focuses on the risks arising from the people, assets, systems and processes through which the University operates. |
| 4. | Governance | Unclarity of direction and control of an organisation. |

| | | |
|---|---|---|
| 5. | Reputational | Risk of impact to the business attributable or related to the trustworthiness of the business and/ar the education industry. |
| 6. | Compliance | Risk due to non-compliance or failure to adhere to sets of rules and regulations as set out by the University, government or regulatory bodies. |

### 11.1.3.3 Risk Analysis

11.1.3.3.1 The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

11.1.3.3.2 Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available. Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use.

11.1.3.3.3 Risk analysis should consider factors such as:

i) the likelihood of events and consequences;
ii) the nature and magnitude of consequences;
iii) complexity and connectivity;
iv) time-related factors and volatility;
v) the effectiveness of existing controls;
vi) sensitivity and confidence levels.

11.1.3.3.4 The risk analysis may be influenced by any divergence of opinions, biases, perceptions of risk and judgements. Additional influences are the quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed. These influences should be considered, documented and communicated to decision makers.

11.1.3.3.5 Highly uncertain events can be difficult to quantify. This can be an issue when analysing events with severe consequences. In such cases, using a combination of techniques generally provides greater insight.

11.1.3.3.6 Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide insight for decisions, where choices are being made, and the options involve different types and levels of risk.

11.1.3.3.7 The processes involved in the analysis are as follows:

a) Determine the level of likelihood of the risk event happening from each risk source – whether rare, unlikely, possible, likely and almost certain.
b) Evaluate the level of impact or the consequence of the risks to the business objectives – whether insignificant, minor, moderate, high and extremely high.
c) Establish the risk rating that is acceptable or otherwise which then provides the basis in the assessment and responses to risks in line with the existing internal controls mechanism. On other words, it shall be confirmed whether the controls are in place and are being used to manage those risks.

11.1.3.3.8 The risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis and the information, data and resources available. The analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances. In detail, the types of analysis are:

**a) Qualitative Analysis**

The qualitative analysis uses words to describe the magnitude of potential consequences and the likelihood that those consequences will occur. It defines impact and likelihood and the level of risk by significance level, such as “low”, ‘medium”, “significant”, “high” and “extremely high”. Generally, qualitative analysis may be used:

i) As an initial screening activity to identify risks which required more detailed analysis.
ii) Where this kind of analysis is appropriate for decisions; or
iii) Where the numerical data or resources are inadequate for a quantitative analysis.

**b) Semi-Quantitative Analysis**

The semi-quantitative analysis uses numerical rating scales for likelihood and impact and combines them to produce a level of risk by way of

formula. The objective is to produce a more expanded rating scale than is usually achieved in qualitative analysis.

It is important to note that since the value allocated to each description may not bear an accurate relationship to the actual magnitude or likelihood and impact, the numbers should only be combined using a formula that recognizes the limitations aof the scales used.

**c) Quantitative Analysis**

The qualitative analysis uses numerical values for both likelihood and impact using data from a variety of reliable sources. The quality of the analysis depends on the accuracy and completeness of the numerical values and the validity of the model used.

Some examples of quantitative methods of risk analysis include:

- Consequence analysis
- Statistical analysis of historical data
- Fault tree and event tree analysis
- Statistical and numerical analysis; or
- Probability analysis

The qualitative and semi-quantitative methods are used primarily to rank risks in order to decide on a priority for action or budget allocation.

11.1.3.3.9 Questions to ask during risk analysis:

- What is the potential likelihood of the risks happening?
- What are the potential consequences of the risk happening?
- What are the current risk responses, which may prevent, detect or lower the consequences of potential or undesirable risks or events?

**11.1.3.3.10 Risk Parameters**

Table 2 and Table 3 are some examples of the levels to be used for likelihood and impact.

**Table 2: Level of Likelihood**

| Level | Descriptor | Probability | Example of Likelihood Description |
|---|---|---|---|
| 1. | Rare | ‹ 1% | The event may occur only in exceptional circumstances – will occur once in every 50 years |
| 2. | Unlikely | 1% - 15% | The event could occur at some time – will occur once in every 20 years |
| 3. | Possible | 16% - 30% | The event might occur at some time – will occur once in every 10 years |
| 4. | Likely | 31% - 50% | The event will probably occur in most circumstances – will occur once in every 3 years |
| 5. | Almost Certain | ›50% | The event is expected to occur in most circumstances – will occur on an annual basis |

**Table 3: Level of Impact**

| Level | Descriptor | Impact Description | | |
|---|---|---|---|---|
| | | Financial | Operational | Compliance |
| 1 | Insignificant | • Unlikely to impact on budget or funded activities<br>• 100% allocation of budget utilisation | • No disruption of critical operation and services<br>• Affects ‹5% of total employees<br>• No effect on leadership effectiveness | • Unlikely to result in adverse regulatory responses or action |

| | | | | |
|---|---|---|---|---|
| | | | • No incidents that lead to injury or death<br>• No disruption of a KCDIOM | |
| 2 | Minor | • Some financial loss<br>• Less than 2% of net profit before tax<br>• Requires monitoring and possible corrective action within existing resources<br>• ±2% variance of utilisation from allocated budget | • 1 to 2 days disruption of several KCDIOMs or one critical service<br>• Affects 5 – 10% of employees<br>• Minor effect on leadership effectiveness<br>• Incidents that lead to minor injury (i.e. staff unavailability between 3 to 5 days) | • Minor non-compliance or breaches of contract, act, regulations or consent conditions<br>• May result in infringement notice |
| 3 | Moderate | • Significant financial loss<br>• 2% - 10% of net profit before tax<br>• Impact may be reduced by reallocation resources<br>• ±5% variance of utilisation from allocated budget | • 3 – 5 days disruption of KCDIOM or several critical services<br>• Affects 11 – 30% of employees<br>• Substantial impact on leadership effectiveness<br>• Incidents that lead to moderate injury (i.e. staff unavailability between 6 to 7 days) | • Significant breach of contract, act, regulation or consent conditions<br>• Potential for regulatory action |
| 4 | High | • Major financial loss<br>• 11% - 30% of net profit before tax | • 6 – 14 days disruption of two or more critical services | • Major breach of contract, act, regulation or |

| | | | | |
|---|---|---|---|---|
| | | • Requires significant adjustment to approved, funded projects or programmes<br>• ±10% variance of utilisation from allocated budget | • Affects 31 – 74% of employees<br>• Major effect on leadership effectiveness<br>• Incidents that lead to major injury (i.e. staff unavailability more than 7 days) | consent conditions<br>• Expected to attract regulatory attention<br>• Investigation, prosecution and/or major fine possible |
| 5 | Extremely High | • Huge financial loss<br>• More than 30% of net profit before tax<br>• Significant budget overrun with no capacity to adjust within existing budget or resources<br>• More than 10% variance of utilisation from allocated budget | • 14 days and more days of disruption of two KCDIOM or most critical services<br>• Affects ›75% of employees<br>• Severe effect on leadership effectiveness<br>• Incidents that lead to severe injury, permanent disability or death | • Serious breach of contract or legislation<br>• Significant prosecution and fines likely<br>• Potential for litigation including class actions<br>• Future funding, approvals, registration in jeopardy |

***Note**: IIUM recognises that many institutions of higher education use 'Strategic Risk Impact' as one category of the risk impact levels, In IIUM's view, however, a significant event in any of the above risk impact has the potential to give impact to the University's strategic plans and outcomes.*

### 11.1.4 Risk Assessment

11.1.4.1 The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to:

i) do nothing further;
ii) consider risk treatment options;
iii) undertake further analysis to better understand the risk;
iv) maintain existing controls; and
v) reconsider objectives.

11.1.4.2 Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders.

11.1.4.3 The outcome of risk evaluation should be recorded, communicated and then validated at appropriate levels of the organization.

11.1.4.4 The likelihood and impact could be estimated using statistical analysis and calculation. If there is lack of reliability or relevant past data, subjective estimation could be made which reflect an individual's or group's degree of belief that a particular risk will occur. Consideration should be made on the existing risk mitigations in place when assessing the likelihood and impact of the risk.

11.1.4.5 The source of information and techniques used to assess likelihood and impact may include

a) Past records
b) Practice and relevant experience
c) Relevant published literature
d) Market research
e) Experiments and prototypes
f) Economic, engineering or other modes
g) Specialist and expert judgements

11.1.4.6 The techniques of assessing may include:

i) Structured interviews with subject matter experts in the area of interest
ii) Use of multi-disciplinary groups or experts
iii) Individual evaluations using questionnaires. and
iv) Use of models and simulations

11.1.4.7 The common factors that could influence the risk assessment:

a) Level of impact on the revenue, Opex, Capex performance etc.
b) The likelihood that the risk will occur.
c) Expected date of occurrence (if can be predicted).
d) Availability, complexity and cost of preventive and corrective actions.
e) Potential risks associated with the preventive and corrective actions.
f) Date the preventive or corrective action needs to be taken.

11.1.4.8 Calculate Gross Potential Loss

The calculation of potential loss is a basis for undertaking risk assessment. It is defined as the losses an organization could possibly incur due to one or several risks transpiring less recoverable amount/

***Potential Loss (PL) ≤ Exposure Less Recoverable Amount (ELRA)***

***Exposure:*** is defined as the asset and source value of the organization that is affected by risks. It is the maximum amount of potential losses that can occur at a specified time due to a risk transpiring.

***Recoverable Amount:*** Is the recoverable loss amount through recovery mitigation e.g. insurance, compensation clause.

Values of potential loss can be calculated for any financial items and proxies can be used a s replacement for non-quantifiable areas.

11.1.4.9 Establish Gross Risk Rating – Risk Likelihood and Impact

Gross Rating of an identified risk should take into consideration the effectiveness of existing mitigations. The gross rating will benefit the organization by:

i) Encourage discussion as to whether existing mitigation strategies are correct and optimal.
ii) Providing a focus to management for prioritization of resources on which risks focusing on.

11.1.4.10 Evaluate effectiveness of existing mitigations

The existing mitigations (i.e. any process, policy, device, practice, or other actions) which modify risk and their effectiveness should be taken into account. The existing mitigation shall include activities such as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties. When examining existing controls, the management should consider its adequacy, method of implementation and level of effectiveness.

**Table 4: Mitigation Effectiveness rating**

| Rating | Effectiveness Rating Description |
|---|---|
| Very Good | Management aware and manages risks well. Mitigation are strong and sufficiently roust to manage risk adequately. Compliance in place. |
| Good | No major issues with mitigations and compliance. Mitigations are adequate and sufficiently robust. |
| Satisfactory | Mitigation and compliance are generally in place. Minimum mitigation issues. |
| Unsatisfactory | Mitigations are inadequate and not sufficiently robust to manage risks. A large number of mitigation lapses and/or non-compliance issues. |
| Poor | Absence of mitigations. Non-compliance to policies and procedures. General lack of compliance culture. |

11.1.4.11 Estimate Level of Risks

The level of risk is a combination of likelihood rating and impact rating. The risk rating is determined by selecting the appropriate level of consequences from the Impact Axis and the likelihood that those consequences will occur from the Likelihood Axis.

The risk rating identified during the analysis process is compared with previously established risk criteria, deciding which risks are more significant and assess whether the current risk levels are acceptable. The risk ratings are determined from the relationship between impact and likelihood as shown in Table 5. The risks levels are Extremely High, High, Significant, Medium, and Low.

**Table 5: Risk Matrix**

| Level of Likelihood | Level of Impact | | | | |
|---|---|---|---|---|---|
| | **Insignificant** | **Minor** | **Moderate** | **Major** | **Extremely High** |
| **Almost Certain** | Medium (5) | Significant (10) | High (15) | High (20) | Extremely High (25) |
| **Likely** | Low (4) | Medium (8) | Significant (12) | High (16) | High (20) |
| **Possible** | Low (3) | Medium (6) | Medium (9) | Significant (12) | High (15) |
| **Unlikely** | Low (2) | Low (4) | Medium (6) | Medium (8) | Significant (10) |
| **Rare** | Low (1) | Low (2) | Low (3) | Low (4) | Medium (5) |

### 11.1.5 Risk Evaluation

11.1.5.1 The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to:

i) do nothing further;
ii) consider risk treatment options;
iii) undertake further analysis to better understand the risk;
iv) maintain existing controls; and
v) reconsider objectives.

11.1.5.2 Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders.

11.1.5.3 The outcome of risk evaluation should be recorded, communicated and then validated at appropriate levels of the organization.

11.1.5.4 The risk evaluation involves comparing estimated levels of risk with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

11.1.5.5 The risk evaluation uses the understanding of risk obtained during risk analysis to make decisions about future actions. Decisions may include:

a) Whether a risk requires treatment.
b) Whether an activity should be undertaken to mitigate risk, and
c) Priorities for treatment.

11.1.5.6 A common approach to decide on the appropriate decisions may be to divide risks into three bands:

a) An upper band where the level of risk is regarded as intolerable whatever benefits the activity may bring, and risk treatment is essential whatever its cost;
b) A middle band (or 'grey' area) where costs and benefits, are taken into account and opportunities balanced against potential consequences;
c) A lower band where the level of risk is regarded as negligible, or so small that no risk treatment measures are needed.

**Table 6: Mitigation Options**

| Mitigation Options | |
|---|---|
| **Extreme** | Immediately initiate action plan to reduce exposure |
| **High** | |
| **Significant** | Develop action plan to reduce exposure |
| **Medium** | Consider if any action plan needs to be developed |
| **Low** | No action required |

### 11.1.6 Risk Treatment

11.1.6.1 General

The purpose of risk treatment is to select and implement options for addressing risk.

11.1.6.2 Risk treatment involves an iterative process of:

i) formulating and selecting risk treatment options;
ii) planning and implementing risk treatment;
iii) assessing the effectiveness of that treatment;
iv) deciding whether the remaining risk is acceptable; and
v) if not acceptable, taking further treatment.

11.1.6.3 Selection of Risk Treatment Options

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Options for treating risk may involve one or more of the following:

i) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
ii) taking or increasing the risk in order to pursue an opportunity;
iii) removing the risk source;
iv) changing the likelihood;
v) changing the consequences;
vi) sharing the risk (e.g. through contracts, buying insurance); and
vii) retaining the risk by informed decision.

11.1.6.4 Justification for risk treatment is broader than solely economic considerations and should take into account all of the organization's obligations, voluntary commitments and stakeholder views. The selection of risk treatment options should be made in accordance with the organization's objectives, risk criteria and available resources.

11.1.6.5 When selecting risk treatment options, the organization should consider the values, perceptions and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

11.1.6.7 Risk treatments, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences. Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective. Risk treatment can also introduce new risks that need to be managed.

11.1.6.7 The following six (6) step process is for general treatment design.

***Step 1: Identify ownership***

The ownership should be identified for all risk treatments for accountability and responsibility.

***Step 2: Review causes and controls***

A risk treatment design should be based on a comprehensive understanding of how risks arise. This includes understanding not only the immediate causes of an event but also the underlying factors ("root causes") that influence whether the treatments will be effective. The

University can carry out a gap analysis to assess how well the risks and the factors which influence them are addressed by existing treatments. This gap analysis then leads to the specification of the treatment objectives for any additional treatment measures as part of a complete control plan.

***Step 3: Treatment Objectives***

The broad intent of risk treatment is to change the risk to a level where the benefit exceeds the total cost of the treatment. Cost Benefit Analysis (CBA) can be used to compare the costs and benefits. It is important to determine the objective of the risk treatment as later it can be used to measure the effectives of risk treatment plan.

***Step 4: Detailed design of treatment measures***

The treatment plans should be practical. To justify its practicality and maintainability, measures should be designed to be "embedded" in normal business processes, activities and systems.

***Step 5: Design Review***

The risk treatments shall be subject to some degree of design review and this includes checking, as a minimum that:

a) The treatment objectives will be achieved;
b) The design is fit for purpose – it is realistically capable of achieving levels of effectiveness, reliability and availability consistent with the importance of the associated activity;
c) It takes into account realistic and reasonable anticipated operational conditions;
d) It is easily capable of being checked and monitored, or is self-checking;
e) The treatment will last and endure and can be maintained easily; and
f) The risk treatments do not introduce new risks, or if they do the new risks are at a lower level of concern.

***Step 6: Communication and implementation***

One of the pre-requisites for an effective treatment plan is the development of an effective communication plan. No treatment can be expected to work effectively unless those who are involved in or affected by the treatment plan understand what it is designed to achieve.

11.1.6.9 If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be recorded and kept under ongoing review.

Decision makers and other stakeholders should be aware of the nature and extent of the remaining risk after risk treatment. The remaining risk

should be documented and subjected to monitoring, review and, where appropriate, further treatment.

11.1.6.10 Preparing and Implementing Risk treatment Plans

The purpose of risk treatment plans is to specify how the chosen treatment options will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored. The treatment plan should clearly identify the order in which risk treatment should be implemented.

The treatment options can include the following:

**a) Accept the risk**

The management may make informed decision to accept the risk without any further actions. The net risk may be deemed acceptable based on factors such as business environment, the cost-benefit analysis of implementing further mitigations and the status of likelihood / impact of the risks on the University.

**b) Reduce or Mitigate the risk**

The management may reduce risk by taking steps to minimise its impact and/or likelihood of occurrence.

**c) Transfer the risk**

The management may decide to transfer or share the risk by transferring the risk to another party or parties to shift the loss or liability. Transfer of risk does not result in transfer of accountability; the risk owner will remain accountable. Therefore, the transfer of risk may require controlling the quality of outsource providers. Transfer of risk can be in full or partial.

**d) Avoid the risk**

If the risk is considered unacceptable, management may avoid the risk by deciding not to start or continue with the activity to prevent the occurrence of risks.

11.1.6.11 Treatment plans should be integrated into the management plans and processes of the organization, in consultation with appropriate stakeholders.

The information provided in the treatment plan should include:

i) the rationale for selection of the treatment options, including the expected benefits to be gained;

ii) those who are accountable and responsible for approving and implementing the plan;
iii) the proposed actions;
iv) the resources required, including contingencies;
v) the performance measures;
vi) the constraints;
vii) the required reporting and monitoring;
viii) when actions are expected to be undertaken and completed.

11.1.6.12 Once the risk treatment options are selected, they should be assembled into risk treatment plans. The purpose of risk treatment plans is to document how the chosen treatment options will be implemented. Risks can be dealt with in the following ways through some of the sample actions highlighted below:

**Table 7: Risk Treatment Options**

| No. | Risk treatment Option | Sample of Action |
|---|---|---|
| 1. | Accept Risk | No further action needed |
| 2. | Reduce Risk | • Improve processes<br>• Ensure adequate skill sets<br>• Determine new policy<br>• Review of business plan |
| 3. | Transfer Risk | • Insure<br>• Outsource<br>• Diversification of investments<br>• Hedge<br>• Put/Call options |
| 4. | Avoid Risk | • Cease activity<br>• Divestment of operations<br>• Change objective, scale of operations or scope of coverage<br>• Prohibit<br>• Pull out of market |

### 11.1.7 Monitoring and Review

11.1.7.1 The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined.

11.1.7.2 Monitoring and review should take place in all stages of the process. Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback.

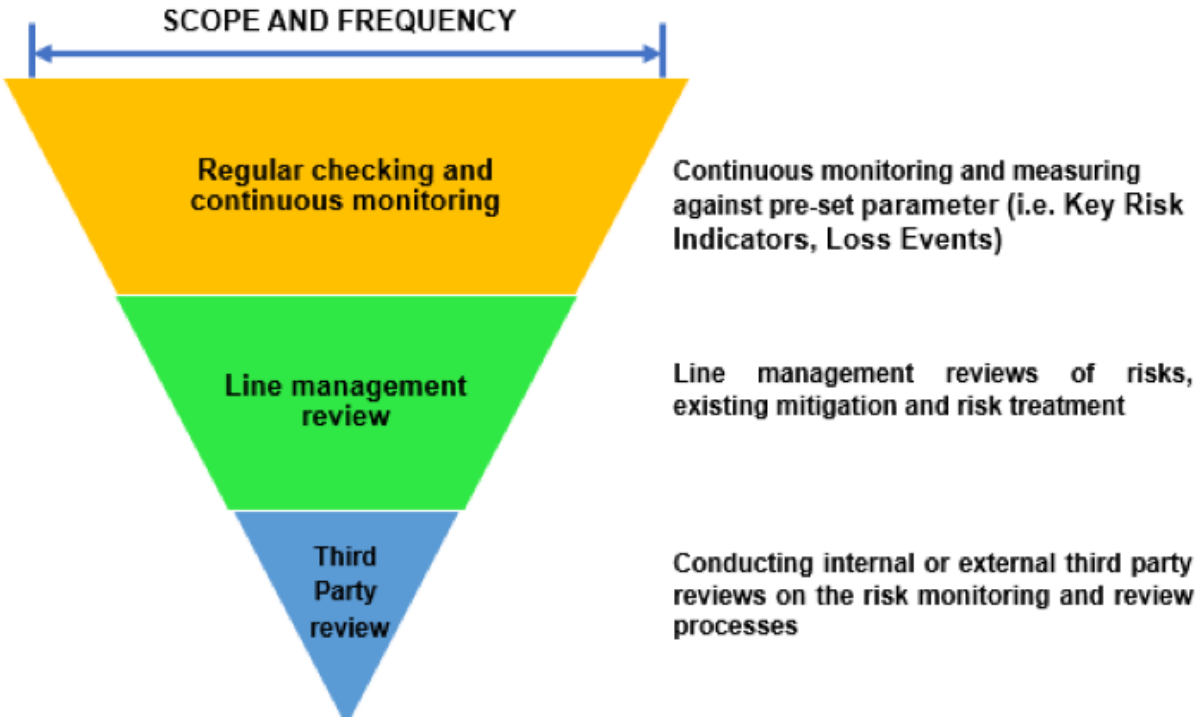
11.1.7.3 The results of monitoring and review should be incorporated throughout the organization's performance management, measurement and reporting activities.

11.1.7.4 The University's monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

a) ensuring that controls are effective and efficient in booth design and operation.
b) obtaining further information to improve risk assessment.
c) analysing and learning lessons from events (including near-misses), changes, trends, successes and failures.
d) detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities, and
e) identifying emerging risks.

11.1.7.5 Monitoring and review practices are illustrated as a hierarchy of assurance activities in Figure 4:

**Figure 4: Hierarchy of Risk Assurance Activities**




11.1.7.6 During the monitor and review stage.

a) Follow-up on results achieved by the action implemented,
b) Re-valuate risks if necessary, and
c) Adjust priorities if required.

11.1.7.7 Establish Nett Risk Rating

The nett risk rating refers to the risk remaining (residual risk) after considering the effectiveness of all mitigations. It is the targeted position in the future state.

The nett rating will provide management with:

a) A view on whether the remaining risk is within tolerance level
b) It will act as an indication of whether the correct mitigations have been selected and whether further mitigations are required.

11.1.7.8 Calculation Nett Potential Loss

Nett Potential Loss = Gross Potential Loss Less Additional Recoverable Amount from New / Enhance Mitigations.

11.1.7.9 Develop Key Risk Indicators

a) Key Risk Indicators act as early warning signals by:
   i) Providing the ability to appreciate changes to an organisation's risk profile due to shifts in established patterns and circumstances.
   ii) Informing and keeping management apprised to enable proactive action is implemented, hence preventing or reducing the impact of the risk.

b) Key Risk Indicators (KRI) are divided into two (2) types, which are:
   i) Leading KRI – Measure a risk before it occurs and is forward looking. Leading KRI provides valuable insight in order to take timely action and improve results.
   ii) Lagging KRI – Measures a risk after event occurred. Lagging KRI provides a backward-looking perspective and is less likely to prevent risk from occurring.

c) Critical KRI Attributes:
   i) KRIs should be agreed upon

      KRIs must be agreed upon by the Risk Owners and Risk Owner Committee (ROC) as an effective measure of risks.

   ii) They must be measurable

      KRIs must be linked to risks clearly. There can be a many to one (i.e. many KRIs linked to one risk) or one too many (i.e. many risks linked to the same KRI). However, the correlation must be fairly clear and not too distant.

d) Documented well

The KRI details must be clearly documented so there is no ambiguity on the purpose of the KRI, what it measures and implication should be “triggered”.

e) Cost effectiveness and practicality

The cost effectiveness of the KRI and its practicality to extract is vital in the selection of KRIs. There is no point selecting a nice-to-have KRI such as customer satisfaction if there is no economically feasible or practical manner to extract such KRIs on a regular basis. In situations like these, replacement KRI which may not be so direct such as number of customers complains might be a more practical measure. There is therefore a need to be creative in KRI identification & selection.

f) Clearly defined tolerance level

There must be a clear tolerance level setting via a “trigger Point” for each KRI where there is a prompting for investigation and action. The purpose is to initiate action and ensure issues are clearly addressed.

g) Must have point of accountability

There must be clear ownership of the KRI, whereupon the explanation for triggering of KRI, its trend etc must be available.

h) Integrated with risk assessments

The identification of KRI must be conducted continuously prior to the risk assessment workshop, during the workshop and after the workshop. The purpose is to independently validate the key measures that track the business and ensure critical risks are clearly measured.

i) Must be integrated to the business planning or key management measure

KRIs should be aligned to the KPIs used during the business planning process and that used management reporting. This is because KPIs track the critical measure of whether the University is achieving its objectives, and KRIs are intended to actively measure and track risks which could prevent our strategic objectives from being achieved.

11.1.7.10 Setting the plan/target and the KRI trigger/tolerance.

When setting up the KRI, one of the critical factors is to determine the two main measurable values:

i) The Target or Planned Value

This represents the planned value for achievement. Typical the target or planned value will have to be broken into annual value, and dissected into the frequency of reporting (either monthly, quarterly, half yearly or annually).

For example, for system uptime, the target uptime may be set at 99.5% i.e. it is intended that the system be online for 99.5% of the time.

ii) The Risk Trigger or Tolerance Value

For each of the KRI, there is a need to identify the value below/above the planned or target value that the KRI is considered triggered.

For example, for the same KRI (System uptime), the risk trigger/ tolerance level may be set at 97%, i.e., if the system is online for anything less than 97% of the time, the risk of system failure is considered “triggered".

Where there is no tolerance value determined, a default threshold of 20% below the planned / target may be used as guidance. However, this needs to be aligned to management requirements.

### 11.1.8 Recording and Reporting

11.1.8.1 The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting aims to:

i) communicate risk management activities and outcomes across the organization;
ii) provide information for decision-making;
iii) improve risk management activities;
iv) assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

11.1.8.2 Decisions concerning the creation, retention and handling of documented information should deliberate, but not be limited to their use, information sensitivity and the external and internal context.

11.1.8.3 Reporting is an integral part of the organization’s governance and should enhance the quality of dialogue with stakeholders and support top

management and oversight bodies in meeting their responsibilities. Factors to consider for reporting include, but are not limited to:

i) differing stakeholders and their specific information need and requirements;
ii) cost, frequency and timeliness of reporting;
iii) method of reporting;
iv) relevance of information to organizational objectives and decision-making.

11.1.8.4 The risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods and tools, as well as in the overall process. Each stage of the risk management process should be recorded appropriately. Assumptions, methods, data sources, analyses, results and reasons for decisions should all be recorded. The records of such processes are an important aspect of good corporate governance.

11.1.8.5 The enterprise risk management information system shall be developed and to be used to:

i) record details of risk, controls and priorities and show any changes in them.
ii) record risk treatments and associated resource requirements.
iii) record details of incidents and loss events and the lessons learned.
iv) track accountability for risks, controls and treatments.
v) track progress and record the completion of risk treatment actions.
vi) allow progress against the risk management plan to be measured, and
vii) trigger monitoring and assurance activities.

As a minimal requirement, these are the records that need to be kept:

i) Periodical and ad hoc risk reports,
ii) Risk Profile/Register
iii) Minutes on Meetings, and
iv) URMC reports

11.1.8.6 Risk reporting

A consolidation risk management report to the BOG and URMC is to highlight the following:

i) The list of significant or key risk of the University.
ii) The internal or existing control measures put in place to manage identified risk exposures.
iii) The outcome of risk awareness training programme conducted for all employees, and
iv) The outcome of skill building training to selected key staff.

The periodical report will enable the BOG to be informed that the risk management and internal control processes are in place within the University and the process is ongoing. Following the review, responses and independent appraisal of the programme, the BOG would be in the possible to make an appropriate disclosure statement on risk management and internal control in the University report.

### 11.1.9 RISK AWARENESS TRAINING

11.1.9.1 The risk management process can only be effectively implemented if staff is convinced that identifying and controlling risks are essential to the success of their work that contribute towards achieving the University's objectives. Therefore, periodical risk-awareness training and workshops need to be planned and executed at all level of operations.

**-THE END-**

***Approved By:***

***University Risk Management Committee***
***Meeting No. 2/2023 (11th April 2023)***

***Next Review:***
***March 2026***

## GLOSSARY OF RISK TERMS AND DEFINITIONS

| TERMS | DESCRIPTION |
|---|---|
| Corporate Governance | Is the process and structure used to direct and manage the business and affairs of the company towards enhancing business prosperity and corporate accountability with the ultimate objective of realizing long term shareholder value, whilst considering the interest of other stakeholders.<br>(Source: Malaysian Code on Corporate Governance) |
| Enterprise Risk Management | Is a process, affected 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. (Source: The Committee of Sponsoring Organisations of the Treadway Commission or COSO) |
| Gross Risk | Gross risk is the product of the impact of the risk on the objective(s) and the likelihood of the risk occurring should no management actions or controls be in place to mitigate the risk. Also known as "Inherent Risk" |
| Impact | The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event. Commonly, they are expressed in the categories of insignificant, minor, moderate, significant and extremely high. Also known as "consequences" |
| Inherent Risk | Please see "Gross Risk" |
| Internal Control | A process effected by an entity's board of directors, management and other personnel, designed to provide "reasonable assurance" regarding the achievement of objectives in the following categories:<br>-Effectiveness and efficiency of operations<br>-Reliability of financial reporting<br>-Compliance with applicable laws and regulations.<br>*(Source: COSO)* |
| Key Risk Indicators (KRI) | A management information indicator that provides continuous insight into the level of risk in group or business. KRIs enable management to manage and monitor risk proactively on an ongoing basis. It is preferable to focus on leading indicators proactively to prevent a risk from materializing. |
| Key Risk Indicators (KRI) | A management information indicator that provides continuous insight into the level of risk in the group/business. KRIs enable management to manage and monitor risk proactively on an ongoing basis. |

| | |
|---|---|
| | KRIs may be leading or lagging indicators. (Note: It is preferable to focus on leading indicators proactively to prevent a risk from materializing). |
| Level of Risk | The relationship between impact and likelihood applicable to the area of risk or program under review. |
| Likelihood | • A qualitative description or synonym for probability or frequency.<br>• The probability of a specific outcome happening. It assigned in accordance with its severity of happenings.<br>• They are expressed in the categories of Rare, Unlikely, Possible, Likely or Almost Certain. |
| Monitor | To check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change. |
| Nett Risk | *Please see residual risk.* |
| Probability | *Please see likelihood.* |
| Residual Risk | • Residual risk is the product of the impact of the risk on the objective(s) and the likelihood of the risk occurring taking into consideration current management actions/controls in place to mitigate the risk.<br>• Also known as nett risk. |
| Risk | • Effect of uncertainty on objectives. *(Source - ISO31000)*<br>• The chance of something happening that will have an impact on objectives. It is measured in terms of consequences and likelihood. *(Source - ANZS4360)* |
| Risk Acceptance | Risk acceptance is used in risk management to describe an informed decision to accept the consequences and likelihood of a particular risk. In terms of best practice, risk can only be accepted if it can be illustrated that the risk is within set risk appetite limits. |
| Risk Analysis | A systematic use of available information to determine how often specified events may occur and the magnitude of their likely consequences. |
| Risk Avoidance | Risk avoidance is used in risk management to describe an informed decision not to become involved in activities that lead to the possibility of the risk being realized. |
| Risk Appetite | The quantum of risk the group is willing to accept in pursuit of its business strategy. |
| Risk Assessment | A process used to determine risk management priorities by evaluating and comparing the level of risk against predetermined standards, target risk levels or other criteria. |
| Risk Identification | The process of determining what can happen, why and how. |
| Risk Management | • The systematic, proactive identification of threats to resources and the development of appropriate |

| | |
|---|---|
| | strategies which will minimize risks. *(Source - ANZS:4360)*<br>• The process whereby organization is methodically addressing the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities. *(Source - Institute of Risk Management)* |
| Risk Management Process | The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk. |
| Risk Management Framework | A model that outlines the processes, steps, and interrelationships in risk management. |
| Risk Matrix | A table of Likelihood and Impact used during Risk Assessment to derived at the risk rating. |
| Risk Mitigation | *Please see risk treatment.* |
| Risk Rating | • The level of risk calculated as a function of likelihood and impact.<br>• The outcome of the likelihood and impact are expressed as low, medium, significant, high or extreme. |
| Risk Response | *Please see risk treatment.* |
| Risk Transfer | • Shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means.<br>• Risk transfer also refers to shifting a physical risk or part there of elsewhere. |
| Risk Treatment | • Risk treatment is used in risk management to describe steps taken to control or prevent an issue or event hazard from causing harm and to reduce risk to a tolerable or acceptable level and within risk appetite levels.<br>• A choice or decision regarding how to react to a risk (which may be active or passive).<br>• Also known as risk mitigation or risk response. |
| Risk Treatment Options | • Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies;<br>o Accept/Retain the risk<br>o Reduce the likelihood of occurrence<br>o Reduce the consequences of occurrence<br>o Share or Transfer the risk<br>o Avoid the risk. |
| Risk Treatment Plan | • Outline of the various decisions including reviews, audits, appraisals and internal controls which will take place over time to provide assurance over the effectiveness of the risk-based internal control system.<br>• Also known as risk response. |

**REFERENCES:**

- ISO 9001:2015 - Quality Management System
- ISO 31000:2018 – Risk Management Guidelines
- Australian/New Zealand Standard on Risk Management (AS/NZS 4360:2004)
- The Turnbull Report
- The Committee of Sponsoring Organizations (COSO) Internal Control Framework
- The Committee of Sponsoring Organizations (COSO) Enterprise Risk Management Integrated Framework
- The Institute of Risk Management (IRM)
- Institute of Enterprise Risk Practitioners (IERP)
- Organisation of Certified Risk Managers (OCRM)

**ACKNOWLEDGEMENT:**

- Members of University Risk Management Committee (URMC)
- Members of University Management Committee (UMC)
- Assoc. Prof. Dr. Sherliza Puat Nelson (Risk Management Office)
- Ts. Dr. Siti Aliyyah Masjuki (Risk Management Office)
- En. Muhamad Asri Bin Basil, *ERA* (Risk Management Office)
- Mdm. Norita Hj. Nanyan (Risk Management Office)
- Mdm. Norhana Bt. Mohd. Yunos (Finance Division)
- Mdm. Razsera Binti Hassan Basri (Development Division)
- En. Faisal Razul Bin Razali (Sultan Ahmad Shah Medical Centre@IIUM)
- En. Ilmyzat Bin Ismail (Office of the Deputy Rector, Academic and Internationalisation)
- Mdm. Rusnani Binti Din@Yaakob (Office of Knowledge for Change and Advancement)
- Mdm. Saidah Zawanah Binti Sulaiman (Information Technology Division)
- Mdm. Rahaidah Bt Ramli (Residential Services Department)
- Mdm. Zahirah Binti Mohd. Zokri (Office of the Legal Adviser)
- En. Shahrulnizam Bin Jaafar (Occupational Safety, Health and Built Environment Department)
- Sr. Salina Bt Sa-idul Haj (Office of the Deputy Rector, Responsible Research and innovation)
- Mdm. Adilah Huda Binti Baharudin (Office of Internal Audit)
- En. Ahmad 'Izzuddin Bin Yunus (Office of the Deputy Rector, Student Development and Community Engagement)
- Others who are directly and indirectly contributing to the completion of this manual.