UNITED REPUBLIC OF TANZANIA

DAR ES SALAAM INSTITUTE OF TECHNOLOGY (DIT)

DAR ES SALAAM INSTITUTE OF TECHNOLOGY

RISK MANAGEMENT FRAMEWORK

DOCUMENT DATA:

Document Type: Risk Management Framework

Administering Department:

Approved By: .....

Date of Approval: .....

Date Prepared: June, 2025

Responsibility for Review: Management

FOREWORD

Risk management continues to be a critical component of public sector governance and a tool for innovation and achieving public sector objectives. It supports and provides assurance on the achievement of Entity's objectives through proactive and risk conscious decision making process. The implementation of formal risk management structures (system) is therefore a necessity which should never be ignored. Before the year 2012, the risk management process in public sector has been on ad-hoc basis and without any formal implementation guidelines. In recognition of this reality the Government of Tanzania developed and issued a Guideline for Developing and Implementing Risk Management Framework for all Public sector organizations (2012) which offers a systematic approach towards this end.

In December, 2012, Government issued the first Guidelines for Developing and Implementing Institutional Risk Management Framework in the Public sector followed by the amendments issued in July 2023. The guidelines aimed at providing practical guidance to Public Sector Organizations in developing and implementing Institutional risk management frameworks. This has placed greater need for the Public Sector Organizations (PSOs) to develop and implement their own risk management frameworks as part of their governance processes.

In recognition of the above, Dar es salaam Institute of Technology has developed this Framework to guide the implementation of Risk management Process. The Framework is expected to instill a culture that will enable the Institute to embed risk management process in every aspect of governance and at all levels. It is expected that the Institute's management will effectively implement the risk management framework.

The legal requirements on risk management structures place a greater emphasis for DIT and other Public Sector entities to develop and execute a tailored 'Risk Management Framework' that is compliant to the ISO 31000:2018 which is the International Standard that provides guidelines for risk management . The implementation of this Framework is the evidence of Institute's commitment to establish and implement control and governance mechanisms which are necessary for improved service delivery and enhanced stakeholders' confidence and trust.

CHAIRMAN OF THE COUNCIL, DAR ES SALAAM INSTITUTE OF TECHNOLOGY

PREFACE

The preparation of this Risk Management Framework formulates a critical path in developing and implementing a proactive and systematic approach in risk management at DIT. This is crucial in helping the Institute to achieve its strategic objectives in more efficient and effective manner. It must be considered that preparation and subsequent implementation of this Framework is a necessity backed up by legal requirement in Tanzania and that we should abide with as stipulated thereon. It is expected that we make decisions and implement programs in our areas of jurisdiction in consideration of the Institute's risk tolerance levels defined in this Framework document.

The Framework outlines the Risk Management Policy, Risk Governance Structure and Risk Protocols to be followed by the Institute in implementing the risk management process. The Risk management policy sets out the strategy, the appetite, attitudes and philosophy adopted by DIT in managing risks. The Risk Management Governance specifies roles and responsibilities and set outs lines of communications for reporting on risk management issues and events. The Risk protocols specify risk management methodologies, rules and procedures, tools and techniques to be used.

The framework has been designed in a manner that allow an alignment of the framework with the existing structures of Dar es salaam Institute of Technology in order for Risk Management not to be seen as "external" component but rather a complement and improvement in the decision-making process of the Institute.

I wish to accord my acknowledgements to all members of the Management, individuals and stakeholders who were involved in the process of preparation and finalization of this Framework for their valuable contribution and commitment. It is my sincere hope that every one of us will comply with the requirements of this Framework and make it an integral part of the Institute's governance to improve service delivery to our esteemed customers

RECTOR, DAR ES SALAAM INSTITUTE OF TECHNOLOGY

SCOPE AND RESPONSIBILITY

Scope

Risk Management Framework (Risk Policy, Structure and Procedures) is an official document embodying directive of the Institute's Governing Council for effective implementation of risk management practice. The Framework is designed to provide consistent directives; define objectives and requirements for achieving sound risk governance, control and effective usage of resources. It ensures that the Rector, Deputy Rectors, Directors, Heads of Units, Managers, Head of Departments and Officers make consistent risk-based decisions and make risk management an integral part of the Institute's operations and other management practices.

The framework applies across all Directorates, Units, Departments, Sections and projects initiated and implemented by the Institute. The Risk Management Framework shall apply to management, staff, students and relevant stakeholders.

Responsibility

It is the responsibility of the Rector to implement, maintain and ensure compliance with requirements of the approved Risk Management Framework. The Risk Management coordinator (RMC) shall be the custodian of risk management documents. Further, it is the responsibility of all staffs transacting business and executing activities on behalf of the Institute to adhere to the requirements of the Risk Management Framework and ensure risk tolerance limits stated thereon are not exceeded.

CONTENTS

LIST OF ABBREVIATIONS

CRSA	Control Risk Self Assessment
ISO	International Organization for Standardizations
PSOs	Public Sector Organizations
RMC	Risk Management Coordinator
DIT	Dar es salaam Institute of Technology
TBS	Tanzania Bureau of Standards

LIST OF TABLES

LIST OF FIGURES

DEFINITIONS OF KEY TERMS

The following key terms and definitions will be applied by Dar es salaam Institute of Technology (DIT)

Term	Definition/Meaning
Compliance Risk	Is the possibility of an event or condition occurring that will influences DIT failure to adhere to Policies, Plans, Procedures, Laws, Regulations, Contracts or other requirements etc
Consequence	Outcome of an event and has an effect on the Institute's Strategic objectives.
Context	The DIT's internal and external operating environment
Control	Is any action taken by management, the Governing Council, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. It includes any policy, procedures, guideline, practice, process, technology.
Institute	Means Dar es salaam Institute of Technology
Framework	Means DIT Risk Management Framework
Enterprise-wide Risk Management	is a systematic, integrated and continuous approach applied across the entire Organization for identifying, assessing, managing and controlling potential events or situations to provide reasonable assurance regarding the achievement of organizational goals
Heat Map	Graphical representation of data where the value taken by a variable in a two-dimensional map are represented in colour. It highlights risk universe based upon several criteria using impact/consequences of the risk and their likelihood/Probability of occurrence.
Inherent Risks	The risk level before considering any control or action taken by management
Likelihood	The chance of something happening.
Operational Risk	Those risks that arise in day to day operations resulting from inadequate or failed internal processes, people and systems or from external events.
Residual Risk	Risks remaining after considering the existing control.

Risk	The chance of an event happening that will have an impact on the achievement of the Institute's objectives. Risk is measured in terms of consequences and likelihood, and covers threats and opportunities.
Risk Analysis	The systematic process applied to understand the effect of the uncertainty of the risk on Institute's objectives.
Risk Appetite	Is an amount of risk on broad level that the Institute's is willing to accept in pursuit of value or while striving to accomplish its objectives.
Risk Evaluation	The process used to determine risk management priorities by comparing the level of risk against pre-determined standards, target risk levels or other criteria.
Risk Identification	The process of finding, documenting, recognizing and describing risks.
Risk Rating	The rating resulting from the application of the Institute's risk assessment matrix on the likelihood and consequence of a risk occurring.
Risk Register	A system or file that holds all information on identifying and managing a risk.
Risk Treatment	Selection and implementation of appropriate options for dealing with risk.
Risk Management Framework	The DITs policies, procedures, systems and processes that are used for managing risks
Risk Management Process	Systematic application of management policies, procedures and practices to a set of activities intended to establish the context, communicate and consult with stakeholders and identify, analyse, evaluate, treat, record and review risk
Risk Profile	The documented and prioritized overall assessment of a range of specific risks faced by the Institute.
Risk Owner	The Head of Department or Units responsible for the area that the risk will arise and impact the objectives. Each risk has a primary owner who has authority, competence and resources to manage that risk. The risk owner will be responsible for preparing action-plans for mitigating the risk as identified in the detailed risk identification and analysis sheet.
Risk transfer	Shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means.

SECTION ONE

1.0 INTRODUCTION

1.1 Background

Dar es Salaam Institute of Technology (DIT) was established in 1997 through Parliamentary Act Number 6 of 1997. The major functions of DIT are to provide facilities for study, training and conduct applied research and consultancy activities in the disciplines approved by the DIT Act. The Institute has a vision of becoming a leading technical education Institution in addressing the needs of the society

DIT strategic objectives are stipulated in its five year straetegic plan (FYSP) 2021/2022 – 2025/2026 through its Institute Transformation Program (ITP) which articulates its capacity in terms of legal and institutional framework, facilities, teaching and learning, research, knowledge exchange, human resource management (HRM) and quality assurance and control.

In achieving the abovementioned mandatory activities, DIT may be exposed to a number of risks that are related to its mandate, and if not effectively mitigated have the potential to derail the Institute from achieving its objectives. Therefore, risk management is a fundamental function for Dar es salaam Institute of Technology.

It is therefore imperative to integrate risk management into Institute's management and operational processes. This will promote good governance, improve service delivery and increase stakeholder's confidence.

1.2 Vision, Mission and Societal Vision of Dar es salaam Institute of Technology

1.2.1 Societal Vision Statement

The society is provided with affordable, relevant and practical technical education to facilitate development and application of technologies to foster socio-economic development in a sustainable manner

1.2.2 Vision Statement

DIT has a vision of becoming a leading Technical Education Institution in Africa

1.2.3 Mission Statement

To provide competence based technical education through training, research, consultancy and development of appropriate innovative technologies and entrepreneurship

1.2.4 Core Values

DIT Core Values is covered in the word **RESPECT** that means:

Table 1: DAR ES SALAAM INSTITUTE OF TECHNOLOGY CORE VALUES

Na	Core Values	Explanations
1	**Responsive**	DIT is quick to react in the way that is needed suitable or right for a particular situation.
2	**Exceptional Service**	The Institute creates and improves relationships through positive interactions with others
3	**Student Centeredness**	The institution values and respects all students as unique individuals
4	**Professionalism**	The Institute takes pride in what it does and value to learn to perform to the best of its ability
5	**Excellence**	The Institute recognizes the fact that good working working environment is needed including short and long-term planning, exploration of new ideas, support for innovation, enrichment & professional development programs, accountability, and attention to health and well-being of faculty and all staff members
6	**Commitment**	The Institute is dedicated to the community it serves
7	**Transparency**	The Institute believes that success is achieved through open exchange

		of information. Cognizant is built on a foundation of open and honest communication.

1.3 Objectives of the Risk Management Framework

The Institute intends to embed risk management practices into its operations and planning and budgeting process. The Risk Management Framework provides a standardized guidance and direction to management, staff and stakeholders on how to conduct risk management process and on mitigation of events likely to impact Institute's strategic and operational plans and objectives. The Framework ensures that risks are identified, analysed, managed, reviewed and monitored at acceptable levels. Specifically, the framework is designed to ensure that:

i. Appropriate systems are in place to identify types of risks facing the Institute in each Directorate, Unit, and Department

ii. Appropriate controls and strategies are adopted to manage exposure to those risks,

iii. Appropriate responsibilities are delegated to control identified risks effectively,

iv. Any material changes to the Institute's risk profile are disclosed,

v. Better cost control and utilization of resources,

vi. Enhancing shareholder value by minimizing losses and maximizing opportunities,

vii. Increased knowledge and understanding of exposure to risk,

viii. A systematic, well informed and thorough method of decision making.

1.4 Scope of the Risk Management Framework

Risk management practice requires consideration of specific organizational context and setting, such that, the principle of one fit all does not apply in risk management. This framework is

confined to guiding risk management practices in line with the requirements of the ISO 31000:2018 Risk Management – Guidelines, and the operating laws governing DIT functions.

The Framework is devised in the context of the present Institute profile, new opportunities, future growth objectives and new business endeavors/services that may be necessary to achieve the strategic objectives, goals, emerging global standards and best practices amongst the comparable organizations in the education sector. It covers all the events within and outside the Institute which have a bearing impact on the its existence.

This framework presents the commitment and approach in managing risks that endanger the achievement of the Institute strategic and operational objectives. In this case its scope extends to as follows:

i. It cuts across all levels of Institute's organizational structures.

ii. Applies to all projects/programs and activities.

iii. This framework, it cuts across all organisation structures, therefore all the Institute's business processes shall be integrated to the Risk Management Framework

iv. There shall be risk based audit conducted within the Financial Year as stipulated in the Internal Auditor's Guidelines

v. There shall be risk assessment conducted before commencement of any project across all Institutional levels to establish the Project Risk Register and from time to time it shall be updated to reflect the current state of affairs

vi. There shall be risk based budget across all levels of the Institutional undertakings

vii. Risk reporting shall be mandatory and it will encompasses all levels of administration from department/section to Institutional levels

viii. All employees, students and stakeholders in all areas and activities of DIT are responsible for applying risk management principles and practices in their work areas.

1.5 Standards, Legislative and Regulatory Context

In establishing the Risk Management Framework, a number of Standards and Laws/Regulations both within and outside the country need to be considered. These are explained below:

i. The framework is built in line with the International Standards: "*ISO 31000:2018 - Risk Management – Principles and Guideline on Implementations*".

ii. The adoption of risk management is a response to the current requirements of the Public Finance Act, 2001 (as amended in 2010) and the need to adapt to emerging best practices in public sector governance.

iii. The National Guidelines for Developing and Implementing Institutional Risk Management Framework in Public Sector Organizations (2012) and its amendment of July 2023 by the Ministry of Finance.

iv. Treasury Circular No. 12 of 2012/2013 on Implementing Risk Management in Public Sector Organizations.

v. Controller and Internal Auditor's General Recommendations for FY 2023/2024 where it was established that the Institute has outdated Risk Management Framework and Risk Register

vi. The Treasury Registrar Business Continuity Management Guideline for Public and Statutory Corporations issued in May 2025

1.6 Rationale and Benefits of Risk Management Framework

DIT like any other public sector organisation operates in highly dynamic service delivery environment. The Institute is vulnerable and exposed to different risk exposures such as operational, strategic, financial, and legal & compliance risks. Both risks have potential of derailing the Institute from achieving its objectives. DIT, therefore, needs to develop and implement a formalised and institutionalised risks management approach which is increasingly becoming a critical aspect of public sector governance. In support of this need, the Ministry of Finance and Planning issued a Guideline for Developing and Implementing Risk Management

Frameworks (2022) (The Guidelines), and instructed all public sector entities vide Treasury Circular No. 12 (2013) to implement Risk Management Framework.

It has to be taken into account that, the office of Treasury Registrar issued a guideline in May 2025 to all Public entities on Business Continuity Management which provides a minimum compliance requirement for all public Organisation to have a contingency plan that can be enacted during the time of emergency to ensure there is minimal disruption of critical operations.

This Framework has been developed in compliance with these Guidelines to ensure there is an effective risk management process to successfully achieve the Institute's strategic and operational objectives. The system allows the Institute to consistently identify and manage risks to acceptable levels or seize opportunities through practical and uniform guidance

1.6.1 Rationale of Risk Management Framework

DIT continuously translates its vision and mission statements into long term strategic objectives presented in its Strategic Plan reviewed after every five years. The Institute manages service outputs, programs, projects and activities in an effort to achieve its Corporate Objectives. Such services, programs, projects and activities are normally executed and delivered with different levels of uncertainties. It is the effects of these uncertainties on corporate objectives, which can be referred as risk for which DIT is always striving to, manage to ensure that the opportunities to maximize the probability of achieving the intended objectives are taken while the threats are controlled effectively to reduce its consequences. Risk is inherent in all DIT's functions and therefore should be managed in a way that derives the best outcomes for the Institute and its stakeholders.

Following these uncertainties, the Institute is taking a greater interest risk management. It is increasingly understood that the explicit and structured management of risk brings benefits. By taking a proactive approach to risk and risk management, DIT will be able to achieve the following four areas of improvement:
(i) **Strategy**, because the risks associated with different strategic options will be fully analyzed and better strategic decisions will be reached;

(ii) **Tactics,** because consideration will have been given to selection of the tactics and the risks involved in the alternatives that may be available;

(iii) **Operations,** because events that can cause disruption will be identified in advance and actions taken to reduce the likelihood of these events occurring, limit the damage caused by these events and contain the cost of the events; and

(iv) **Compliance** will be enhanced because the risks associated with failure to achieve compliance with statutory and customer obligations will be recognized as it is stipulated in the following directives and compliance standards:

(a) compliance requirement stipulated in the Finance Act 2001 as amended in 2010, Internal Auditor Guideline of July 2023, Budget circular No. 1 of 2025

(b) Implementation requirement of the Institute Strategic Plan 2021-2026
(c) compliance requirement for ISO 21001:2018 which specifies the management system for education organisation (EOMS) that the Institute is currently implementing in collaboration with TBS

1.6.2 Benefits of Risk Management Framework

Formally established and comprehensively documented risk management practice can be beneficial to the Institute in variety of ways as it is a good management practice and necessary for improved public sector governance. The practice, contributes to effective management, strategic planning, and creates confidence and trust that the Institute can deliver desired outcomes, manage threats, and make informed decisions about available opportunities. Specific benefits include the following:
(a) Establish reliable basis for planning, budgeting and improve quality of decision-making process at all levels.

(b) Safeguard and enable more efficient use of resources.

(c) Reduce the likelihood of costly operational surprises, shocks or unexpected losses.

(d) Increase performance and minimize harm to staff and beneficiaries (students and the public).

(e) Uphold moral principles for service orientation protect value and enhance assets and organizational image.

(f) Comply with applicable legal and regulatory requirements, and enhance sharing of risk information across all levels of the Institute.

(g) Increase stakeholders' trust and confidence in the organisation, that it is proactively managing threats in execution of its legal mandate.

1.7 Structure of the Document

The document termed "Risk Management Framework" is divided into four main sections namely:

i. Risk Management Policy and Strategy;
ii. Risk Management Governance Structure;
iii. Risk Management Procedure and;
iv. Risk Management Templates.

While the risk management policy sets out the Institute strategy and commitment to risk management, the other three parts of the framework (i.e. governance structure, guidelines and templates) are designed to support the policy by providing details of the risk governance architecture and processes/protocols in implementing the Institute's Risk Management Framework

SECTION TWO

2.0 RISK MANAGEMENT POLICY AND STRATEGY

Dar es salaam Institute of Technology recognises that, it is exposed to risks while pursuing her mandated functions of learning environment and teaching, research, consultancy and Innovation, and carrying different operations of the Institute. These risks arise from operational undertakings as well as external interferences and could affect the Institute's service delivery capacity and sustainability. We recognise, however, that, risks can be mitigated through designing and implementing formalised risk management process which is supported by the Governing Council, management, staff and all stakeholders

2.1 PURPOSE

The main purpose of the policy is to communicate the Institute's philosophy, attitude, commitment, direction and guidance in establishing and implementing an Institute-wide risk management practices aimed at providing reasonable assurance to ensure its strategic objectives are achieved, value is created and protected within and across the Institute. In this regard, this

framework document serves both as a tool for communicating DIT's acknowledgement of the presence of risks in its operating environment and its commitment to managing them

This document set a consistent approach in making sure that all significant risks to the Institute are identified, assessed and where necessary treated and reported in a timely manner. Dar es salaam Institute of Technology's Risk Policy is designed to assist DIT's stakeholders in the identification, analysis, evaluation, treatment and reporting of risks in timely and consistent manner.

The Institute's Risk Policy intends to achieve the following key objectives:

(a) Encourage pro-active risk management practices and maintain accepted level of risk appetite pertinent to its goals and objectives;

(b) Encourage risk conscious decision making and optimal use of resources across all levels;

(c) Promote risk management awareness and risk culture amongst Institute's internal and external stakeholders

(d) Ensure consistent use of defined risk management practices to comprehensively identify, assess and mitigate risks based on systematic processes and procedures; and

(e) Provide formal communication of knowledge, skills and attitudes required for effective implementation of the Framework to all DIT staff and stakeholders.

2.2 RISK MANAGEMENT PRINCIPLES

2.3 POLY STATEMENT

DIT recognizes that risks are inherent on its functions and processes and can be detrimental on realization of its vision if there is no proper mitigation measures in place. The Institute is committed to avail required resources for conducting and integrating continuous risk management practice across all operational levels, in order to contain risks to its defined tolerable limits towards providing effective public teaching and learning services to the public for sustainable social and economic development.

The Institute recognizes that the management of risks to be a significant aspect of corporate governance, and an essential contribution towards the achievement of its strategic and operational objectives.

To this respect:

i. DIT is committed to embedding risk management so that it becomes an integral part of its decision making and routine management, and to be incorporated within the strategic and operational planning processes at all levels of its structure.

ii. DIT is committed to ensuring that all staff (Rector, Deputy Rectors, Directors and Heads of Unit) are provided with adequate guidance and training on the principles of risk management and their responsibilities to implement risk management effectively.

iii. DIT will regularly review and monitor the implementation and effectiveness of the risk management process, including the development of an appropriate risk management culture across the Institute.

iv. DIT charges all staff with the responsibility of adhering and implementing the principles stipulated in this framework.

2.4 ADAPTED RISK MANAGEMENT STANDARD

The Institute adapts and implements its risk management practice in accordance to the International Organisation for standardization ISO 31000: 2018 - Risk Management Guidelines. The Standard was selected because it is recommended by the Government Guidelines for Risk Management in Public Sector as issued by the Ministry of Finance (2022).

2.5 GUIDING CONSIDERATION AND RISK MANAGEMENT PRINCIPLES

2.5.1 RISK MANAGEMENT PRINCIPLES

The Policy shall be implemented in consideration of core risk management principles based on clause 6 of ISO 31000:2018. The principles ensure effective integration of risk management function into the Institute's operational and management processes. These are:

- **Risk management is structured and comprehensive**, contributing to consistent and comparable results across geographic locations and functional areas.
- **Risk management is customized and proportionate** to the internal and external context of Dar es salaam Institute of Technology;
- **Risk management is inclusive,** with appropriate and timely involvement of key internal and external stakeholders to enable their knowledge, views and perceptions to be considered;
- **Risk management is dynamic**, recognizing that risks can emerge, change or disappear over time; risk management anticipates, detects, acknowledges and responds to those changes in a timely manner;
- **Risk management is based on the best information available** such as historical data, experience, stakeholder feedback, audit findings, forecasts and future expectations. Risk management aims to base decisions on accurate, timely and clear information but also explicitly considers any limitations and uncertainties associated with such information;
- **Risk management takes human and cultural factors** into account and recognizes that for a multi-cultural organization such as DIT, human behavior and culture influence all aspects of risk management at each level and stage; and
- **Risk management facilitates continual improvement** of the organization through supporting a culture of openness, collaboration and learning that encourages personnel and stakeholders to collaborate and to be risk-aware in delivering our mission.

2.5.2 RISK MANAGEMENT GUIDING CONSIDERATION

In applying this Policy, the Institute adheres to the following guiding considerations:

- **Risk management facilitates action and decision making**: DIT recognizes that objectives can only be achieved by taking calculated, well managed risks and seizing opportunities, including through innovation and exploring new ways of working. The risk management process supports Institute's Management in taking effective decisions in pursuit of objectives through: collecting the best available information; carefully assessing the risks and rewards of different options with due diligence; and considering what can be done to manage these uncertainties.

- **Risk management is everyone's responsibility**: anticipating, identifying and responding to risks and opportunities at different levels is an integral part of everything the Institute

undertakes. All personnel should have a 'risk reflex' and are expected to proactively identify, assess and manage risks when executing their daily responsibilities

- **Risk management embedment:** DIT recognizes that the benefits of risk management can be realized when integrated across all organizational daily activities, actions and throughout the entire operational management cycle guiding both strategic and operational decision-making**.**

2.6 RISK APPETITE STATEMENTS

Risk appetite is the level of acceptable risks that the Institute is willing to take in pursuit of its strategic goals and objectives. The following risk appetite statements forms the foundation on managing risks in DIT's day-to-day activities:

Table 2: DIT RISK APPETITE STATEMENTS

Category	Risk appetite statements
Strategic Risk	The Institute has LOW level appetites for risks and uncertainties that may negatively impact the achievement of strategic objectives or sustainability targets and committed to pursuing initiatives towards attaining affordable, reliable and modern urban mobility for sustainable development.
Operational Risk	The Institute has a low level of tolerance on risks that have direct impact on operations of its core objectives. It includes bus provisional of learning and teaching environment, research, innovation, consultancy and technology transfer. The Institute, therefore, has LOW appetite for this risk category
Financial Risk	DIT is also exposed to some significant financial risks, largely due to procurement activities and financing of its operations. DIT will not accept any risk that will lead to financial mismanagement and wastage. This also aligns with the zero tolerance policy to any type of fraud, corruption, theft and misuse of public resources. .

Compliance Risk	The Institute has zero appetite with compliance risks; this is applicable at all levels and aspects of the organization's activities.
Reputational Risk	The Institute is exposed to reputation risk due to the nature of the services it's provide to the society. Reputation is paramount on the Institute's growth, hence it is very important to maintain a good and sound reputation on its mandate and dealings. The Institute, therefore has zero tolerance to any act that jeopardize its reputation

SECTION THREE

3.0 RISK MANAGEMENT GOVERNANCE STRUCTURE

A full integrated and effective functioning risk management is affected by well-defined risk roles and responsibilities and an appropriate reporting structure. To meet this objective DIT establishes a risk governance structure which shall be integrated into existing management systems for effective implementation.

To work effectively risk management system requires commitment from the Governing Council and top management, allocation of appropriate resources, enhanced risk awareness and formal assignment of risk roles and responsibilities. The Institute hereby establishes the risk management governance structure (the risk governance structure) which is integrated into the existing organisation structure. The risk governance structure articulates risk roles and

responsibilities, and dictates risk management reporting and communication levels across the Institute.

3.1 Purpose

Risk management structure can be described as the risk architecture of the organization. The architecture sets out the lines of communication for reporting on risk management issues and events. It gives clear risk management responsibilities in relation to:

i. Oversight of risk management;

ii. Development of risk policy and procedures;

iii. Implementation of the agreed standards and procedures; and

iv. Auditing and compliance of the policy, standards and procedures.

3.2 Roles and Responsibilities

Risk management is everybody's business at DIT. This section assigns and defines risk role and responsibilities to individuals and organs as described hereunder:

3.2.1 The Council

The Governing Council is ultimately responsible for the oversight on the establishment and operation of the Institute 'Risk Management Framework'. It has the responsibility to provide direction and oversight on Risk Management across the Organization. The key risk management responsibilities shall include:

i. Approve *(accept and endorse)* the Risk Management Framework.
ii. Determine strategic approach to risk and set risk appetite.
iii. Seek regular assurance on the efficacy of control mechanisms, risk management and compliance with the approved Risk Management Framework
iv. To set standards and expectations of the Institute with respect to conduct and behavior, and ensuring that effective risk management is enforced through an effective performance management system.

v. To monitor the management of high and significant risks and the effectiveness of associated controls through the review and discussion of one monthly risk management reports.

vi. To approve major decisions affecting the Institute risk profile or exposure

3.2.2 The Rector

The Rector, who is the Accounting Officer, is responsible for ensuring that a risk management system is established, implemented and maintained in accordance with this risk framework.

Specifically Accounting Officer is responsible for:

i. Setting out an appropriate tone and support the design, implementation and enhancement of an appropriate risk management framework.

ii. Supervise the implementation of approved risk policies, procedures and guidelines throughout the Institute.

iii. Ensuring that the control environment supports the effective functioning of risk management;

iv. Holding top-level management accountable for designing, implementing, monitoring and integrating risk management into their day-today activities;

v. Provide assurance to relevant DIT stakeholders that key risks are properly identified, assessed and mitigated;

vi. Devoting personal attention to overseeing the management of the significant risks;

vii. Serving as the key decision-maker with regard to the specific treatment of critical risks facing the Institute.

3.2.3 Risk and Compliance Committee

The Risk and Compliance Committee , in additional to the existing responsibilities, shall provide an independent and objective view of the risk management effectiveness.

Responsibilities of the Risk and Compliance Committee shall include:

i. review and approves Risk Management Framework and Guidelines;

ii. review and approves the Institute's Risk Register;

iii. set the tone and culture towards effective risk management through strategy setting, and approval of resource allocations;

iv. ensure that risks are adequately considered when setting the Institute Strategy;

v. understand the top risks facing the Institute in pursuit of its objectives;

vi. ensure that top Management has established systems to manage risks and are implemented and operating effectively;

vii. deliberate and note the risk management performance and checks whether the Management is responding appropriately;

viii. makes necessary disclosures on risk management activities in the annual financial statements;

ix. oversee the implementation of mitigation actions for reducing exposure to the top risks within Institute's risk profile;

x. Reviews quarterly reports on the status of top risks, compliance, and other controls.

3.2.4 Risk Management Coordinator (RMC)

3.2.4.1 There shall be a Risk Management Coordinator who will be appointed by the Rector among the existing Officers.

3.2.4.2 The Risk Management Coordinator shall report to the Accounting Officer on all matters relating to Risk Management.

3.2.4.3 Specifically, the Risk Management Coordinator shall:

i. Co-ordinate and monitor the implementation of risk management initiatives within the Institute;

ii. Coordinate the development or updating and review of the Institute's Risk Management Framework and Risk Register;

iii. Work closely with the "risk owners" (i.e. Directors and Head of Units) in overseeing the identification and treatment of risks falling in their respective areas of responsibilities;

iv. Ensure that relevant risk information is reported and escalated or cascaded, as the case may be, in a timely manner that supports the DIT's requirements;
v. Attend at Audit Committee's meetings when Risk Management issues are discussed; and
vi. Provide advice to Accounting Officers and Risk Owners on issues of Risk Management;
vii. Receive and compile implementation reports from other Risk Owners;
viii. Compile, summarize and analyze risk management implementation reports on quarterly basis and submit to the Accounting Officer. The reports will also be presented and discussed in the Risk and Compliance Committee meetings;
ix. Conduct or arrange training or awareness workshops/ seminars in risk management to staff.

3.2.5 Directors and Head of Units (RISK OWNERS)

The Risk Owners are responsible for integrating and implementing risk management processes into their respective areas of responsibilities and operational routines.

Specifically, they are responsible for:

i. Executing their responsibilities as set out in the Risk Management Policy and Procedures;
ii. Empowering officials under their areas of responsibilities to effectively perform their risk management duties through proper guidance, supervision, communication of responsibilities and providing opportunities for skills development;
iii. Aligning the functional risk management methodologies and processes with the Institute's risk management process;
iv. The development of risk management plan (including action plans to implement proposed mitigation measures contained in the Institute's Risk Register)
v. Implementation of risk management action plans
vi. Preparations of risk management quarterly implementation reports and submit them to the Risk Management Coordinator. This will also involve annual reporting on the status of implementation of the risk register during the review process.
vii. Devoting personal attention to overseeing the management of key risks within their area of responsibility;

viii. Maintaining the proper functioning of the control environment within their area of responsibility.

ix. Giving cooperation to auditors (both internal and external) in the course of audit of risk management activities within their respective departments and units. Also, in this regard, they are responsible to respond on the audit issues raised by the auditors and/or audit committee.

x. Maintenance of Risk Register and other documents/ reports relating to risk management within their respective departments and units in a systematic manner.

3.2.6 Risk Champions

Risks champions shall be the representatives of Directorate, Units and Departments. Champions shall collaborate with the RMC to promote risk management culture across the Institute. Their roles and responsibilities are:

i. Be aware of DIT's risk management requirement and liaise with coordinator in embedding risk management practices into other systems and processes;

ii. Work with Directors and Heads of Units within their functional areas to identify, capture the key business risks and regularly review, update and monitor their respective risk registers;

iii. Act as point of contact for risk management enquiries at their respective Sections and Units;

iv. Facilitate dissemination of risk information to their respective Directorate and Head of Sections /Units;

v. Update the risk owners regarding progress in implementing risk management plans regularly;

3.2.6 Internal Audit Unit

3.2.6.1 The Internal Audit Unit will be responsible for providing the Accounting Officer with an objective assurance (and advice) on the effectiveness of the Institute's Risk Management Processes.

3.2.6.2 In fulfilling the responsibility, the Internal Audit Unit must:

i. Develop Risk-based Internal Audit Plans consistent with the DIT's risk profile;
ii. Evaluate the DIT Risk Management Framework (i.e. Policy, Governance Structure, and Procedures) to ascertain if they support and align with the Institute mission and strategic objective;
iii. Ascertain whether significant risks on the DIT's strategic objectives, targets and functions are identified and appropriately assessed, and that appropriate risk responses are selected and implemented, so as to align risks treatments with the Institute's risk appetite;
iv. Ascertain if relevant risk information is captured and communicated in a timely manner across the Institute and enabling the Accounting Officers, the Management and staff to carry out their responsibilities; and
v. Provide the Accounting Officer and the Risk and Compliance Committee with reports on the effectiveness of the Institute's risk management framework

3.2.7 All Staff

All staff are responsible for integrating and implementing risk management into their day-today activities. With this respect, they must:

i. Comply with all rules, regulations and instructions relating to Risk Management;
ii. Implement the risk treatment action plans that address specific risks falling in their areas of responsibilities;
iii. Inform their supervisors and/or the Risk champion of new risks and significant changes on known risks; and
iv. Co-operate with other role players in the risk management process and providing information as required.

3.2.8 All Students and External stakeholders

All students and relevant stakeholders are required to comply with requirements of the Institute's Risk Management Framework

SECTION FOUR

4.0 RISK MANAGEMENT PROCEDURES

The Government Risk Management Guidelines (2022) require risk management process to be conducted in a systematic manner and consistent with sequence of tasks underlined by a specified International Risk Management Standard. In view of that, DIT, adopts the risk management process consistent with ISO 31000:2018. The procedures, rules, methodologies, tools and techniques for carrying out the risk management process are detailed in this section of the manual

4.1 The Risk Management Process

DIT risk management process is consistent with seven elements identified in figure 1 with two elements; *communicate and consult*; *monitor and review*, occur continually throughout the process. The remaining elements shall be undertaken sequentially. The Figure 1 summarizes risk management procedures that shall be followed

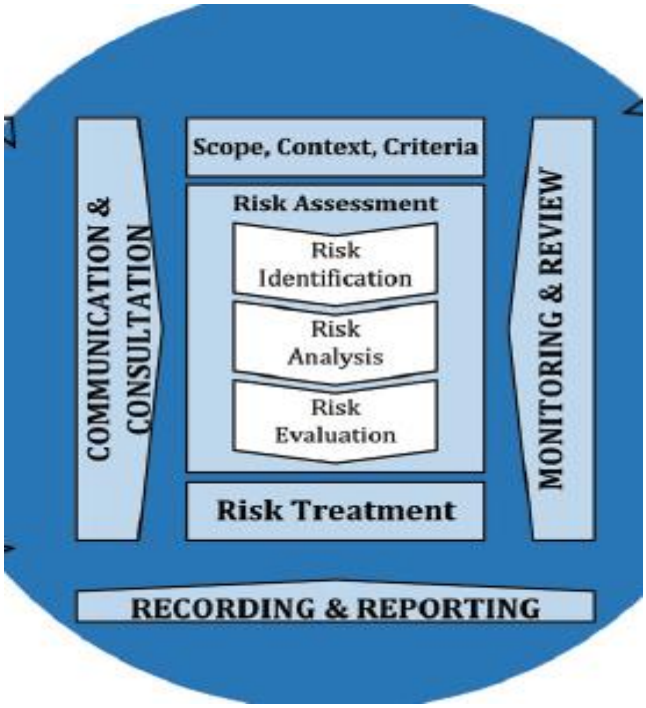

Figure 1: Risk Management Process (Clause 6 – ISO 31000:2018)

4.2 Establish Scope, Context and Criteria

Establishing the context involves defining and understanding external and internal environment that the Institute has to consider when managing risks. The process involves setting the scope of risk management and criteria for assessing identified risks. The scope shall be determined within the context of the Institute's strategic and operational objectives.

4.2.1 Establish Scope

Risk Management at DIT covers Strategic Risk, Financial Risk, Operational Risk, Compliance Risk, Reputational Risk and Employee Health and Safety Risk while taking into account the main objectives of the Institute.

4.2.2 Internal and External Context

This refers to the environment in which the organization seeks to define and achieve its strategic and operational objectives. The context established from the understanding of the external and internal environment in which the organization operates and reflect the specific environment of the activities to which risk management process is to be applied

The following inputs should be used when establishing external and internal context:

(a) The Institute Act No. 6 of 1997.

(b) The strategic Plan as revised from time to time; annual business plans and budget documents;

(c) Various policy documents, Directives, Standards, Manuals and Background documents in place at DIT (Finance and Accounting manual, National Anticorruption strategy Phase IV, schemes of service, Client Service Charter, internal audit manual, human resources manual, Performance Contract etc);

(d) Various reports including internal and external auditor's reports; Performance and specific project reports; Researches and consultancy reports and other publications in the high learning industry

(e) Strategic Plan, Annual Plan and Budgets;

(f) MTEF, Action Plans and Planned targets and outcomes;

(g) Capability of people, systems and processes;

(h) Policies and Guidelines established by the Institute.

4.2.3 Establish Criteria

This is basis for evaluating and ranking of Institute risks has to specify the amount of risk that may or may not take relative to its objectives. DIT risk criteria established in terms of risk appetite levels and risk tolerance limit as defined in paragraph **2.6** of this Risk Management Framework.

4.3 Conduct Risk Assessment

Risk assessment refers to overall process of risk identification, analysis, and evaluation. Tasks identified in 4.3.1 – 4.3.3 are performed during different stages of risk assessment process

4.3.1 Risk Identification

Risk Identification refers to the process of finding, recognizing and describing risks that may impact realization of the DIT objectives. This task sets out to search the Institute's exposure to uncertainties to its strategic execution. It involves identifying potential events and incidences that might have positive (opportunity) or negative (threat) in the achievement of strategic objectives and plans of the organization.

The risks shall be identified from the strategic objectives, targets, specific strategic projects and key processes based on the pre-established level of assessment (Institutional, departmental or project).

The following systematic procedure shall be used during risk identification:

- Understand your objective, target, key processes, activities, strategies and resources towards that objective or target.

- Collect information from historical data, checklists, records of prior losses, gap analysis and discussion with key staff from respective directorates/departments/units, then identify risks against each stated objective/target.

- Assign Risk Identification Number (Risk ID) which is a code that is assigned to the identified risk to create unique identification. DIT code will be formulated by combination of alphabet and numbers starting with short form of the responsible department e.g., EE-C001 is the Risk Id for the first risk in the Electrical Engineering Department which may affect Objective C of the Institute.

- Assign risk ownership using the three areas that underpin activities, who is responsible, who is accountable and Who provides budget for risk mitigation.

- Categorize the risk identified against a specific objective or target into one of the principal risk categories presented in paragraph 2.6 of the Policy.

- The risk identification process shall be described and documented in "Risk Identification and Analysis Form' (DIT/RM/RIAF/01) attached as **Template 1**.

DIT will adopt Risk and Control Self-Assessment workshop' (Team-based Brainstorming) to gain consensus risk assessment as it provides group-oriented and encourage everyone to participate with great sense of risk ownership and commitment. The brainstorming sessions facilitates collective understanding of the risk with reference to the organization context and organization knowledge (experiential, documented and lesson learnt).

4.3.2 Risk Analysis

Risk Analysis refers to the process of rating risks in terms of probability/likelihood that a risk will occur, and the impact/consequence of that event should it occur. It includes risk estimation and it provides the basis for risk evaluation and decisions about risk treatment. DIT shall adopt the ***five (5) band level scale*** in determining likelihood and impact and in conducting risk assessment. The criteria below (Table 4.1) and (Table 4.2) will be followed in determining likelihood and impact.

The Institute shall use the following steps in risk analysis:

- Identify and evaluate existing controls (Test existence, Adequacy and Efficacy of controls).

- Determine the Likelihood (Possibility of identified risk event to occur) and Impact (Consequence if the risk event materializes) in context of existing strategies and controls.

The Institute will analyse risks based on reliable data such as 'past records and practical experience; performance reports, relevant published information and history of events in the Organization or similar Institutions. If there is no reliable data available to use qualitative risk analysis' (Experience, judgment and subjective estimates) shall be applied.

Table 4.1. Risk Impact Description and Decision Guidance

Score	Impact Descriptor	Decision Guidance
5	Severe/ Catastrophic (Very High)	• Non-delivery of services/ impact that would result in failure to achieve three or more of our strategic aims, objectives or key performance targets • Significant financial loss (e.g., budget reduction by 20%). • Multiple loss of life and/or loss of reputation or image that may take more than five (5) years to recover or involves litigation. • Event that involves significant management time
4	Major (High)	• Non-delivery of services/ impact that would result in failure to achieve one to two of our strategic aims, objectives or key performance targets • High financial loss (e.g., budget reduction by 10%) • Multiple loss of life and/or loss of reputation or image that may take 2-5 years to recover or involves litigation. • Event that involves relatively higher management time
3	Significant (Moderate)	• Partial delivery of services/ restricted ability to achieve one or more of our strategic aims, objectives or key performance targets. • Moderate financial loss (e.g., budget reduction by 5%)

		• Moderate loss of life and/or loss of reputation or image that may take 1 year to recover
2	Minor (Low)	• Delivery of services with acceptable levels of problems/ some aspects of one or more of our strategic aims, objectives or key performance targets • Minor financial loss (e.g., budget reduction below 5%) • Event that involves little management time.
1	Insignificant (Very Low)	• No impact or insignificant financial Loss.

Table 4.1. Risk Likelihood Description and Decision Guidance

Score	Impact Descriptor	Decision Guidance
5	Almost Certain (Very High)	• Likely to occur/recur. • High level of recorded incidents and strong evidence. • Typical frequency every 5 years or less. • Likelihood over 5 years: >50% (1 in 2 chances). • The adverse event will definitely occur, probably multiple times in a year (80%-100%).
4	Likely (High)	• Likely to occur/recur. The adverse event is expected to occur in most circumstances (e.g., 60%-80% chance of occurring in the next 12 months. • Regular recorded incidents and strong evidence. • Will probably occurs in many circumstances. • Typical frequency once every 5/7 years. • Likelihood over 5 years: >5% (1 in 20 chance)
3	Possible (Moderate)	• May occur at some time. The risk event should occur at some time e.g., between 40%-60% of occurring in the next 12 months. • Few or infrequent recorded incidents or evidence. • Some opportunity, reason or means to occur. • Typical frequency once every 20 years. • Likelihood over 5 years: >0.5% (1 in 200 chance)

2	Unlikely (Low)	• It is not expected to occur. The risk event may occur only in exceptional circumstances e.g. (20%-40% chance of occurring in the next 12 months or once in 10 years). • No recorded incidents or evidence. • Little opportunity, reason or means to occur. • Typical frequency once every 100 years. • Likelihood over 5 years: >0.05% (1 in 2,000 chance)
1	Rare (Very Low)	• Highly unlikely to occur in the next 5 years (Less than 20% chances of occurring). • No history of adverse event in the organization. • May occur only in exceptional circumstances. • Typical frequency once every 500 years or more. • Likelihood over 5 years: >0.005% (1 in 20,000 chances).

4.3.3 Risk Rating and Evaluation

Risk evaluation involves comparing the results of risk analysis (Total Risk) with its criteria to determine whether the risk and its magnitude is acceptable or tolerable. This helps to determine whether additional action is required.

DIT total risk score is based on the *five (5) bands level* and is summarized on table 4.3. The matrix shows risk severity and shall be a decisive indicator on the urgency of action for each identified risk. The total risks score shall be evaluated against the defined risk tolerance limit described in the Institute Risk Management Policy and Strategy Section, Para. 2.4.3 (Table 2.3) in order to decide the appropriate actions on the respective risk (Accept or mitigate)

Table 4.3: Total Risk Scores

Likelihood	**Almost certain**	5	10	15	20	25
	Likely	4	8	12	16	20
	Possible	3	6	9	12	15
	Unlikely	2	4	6	8	10
	Rare	1	2	3	4	5
		Insignificant	**Minor**	**Significant**	**Major**	**Catastrophic**
Legend	**Impact** **KEY: RANKING = Probability x Consequence**					
	score	1-4	LOW		• This score is considered a minor concern and current controls and actions being carried are adequate. • The RMC and Risk Owners shall accept the risks with this score but review them annually.	
	score	5-9	MEDIUM		• DIT shall develop procedures to manage the risk with this score. • RMC and Risk Owners shall review the risk, action and controls bi-annually.	
	score	10-12	HIGH		• The risk with this score shall be considered by the Institute as a serious concern and of high priority. • DIT shall take immediate action and the controls and actions shall be reviewed at least three times a year.	
	score	15-25	EXTREME		• The risk with this score shall be considered very serious and immediate action shall be taken. • The RMC and Risk Owner shall review the risk, action and controls regularly	

4.4 Risk Register

A risk register is defined as the "document used for recording identified risks". The purpose of the risk register is to facilitate ownership and management of each risk. Typically, the risk register will cover the significant risks facing the organization or department or the project. It will record the results of the risk assessment related to the process, operation, location, business unit or project under consideration.

The risk register will be prepared based on the risk assessment process completed in the Risk Identification and Analysis Form (DITT/RM/RIAF/01). The Institute shall use form DIT/RM/RR/02 to document all identified risks as indicated in **Annex 2**.

The Risk Management Coordinator (RMC) shall consolidate and prepare an overall 'Institutional Risk Register **(IRR)**'. This risk register shall reflect the Institute's risk profile and contain strategic and key operational risks aggregated from other risk registers.

Each Risk Owner (Director/ Manager) shall be responsible, where relevant, for preparation of the Departmental Risk Register also known as Operational Risk Register **(ORR)**'. This shall reflect the key operational risks of the directorates, Divisions, Departments, Units or controlled campus.

The Institute shall conduct an intensive risk assessment, develop and maintain Project Risk Register **(PRR)** where it implements a capital-intensive project such as major infrastructure development projects, acquisition of specialised assets or equipment and Information Technology project, strategic initiative or transformation projects. The PRR shall reflect risk related to that project and shall be maintained throughout the lifecycle of individual project (s).

The Institutional and Operational Risk Registers shall be reviewed at least annually and/or when new initiatives are implemented.

4.5 Risk Treatment Action Plan

The risk treatment planning produces responses and specific action plans to address the risks identified. This follows risk evaluation conducted in 4.3.3 which acts as necessary information to make decisions about which risks need treatment and to prioritize treatments. Risk treatment actions are intended to mitigate the risks which are found to exceed risk tolerance level. The following arrangements shall guide risk responses within the Institute:

(a) The risks found to exceed the defined risk limits shall be treated through appropriate response strategy, which should be based on a comprehensive analysis of the manner in which the risks arise such as the underlying causes.

(b) There may be several risk treatment/response options and more than one may be applied to a given risk. The best risk response options shall be selected in view of its feasibility and cost effectiveness

(c) Once risk response options for individual risks have been selected, they shall be consolidated into the Risk Treatment Action Plan **(DIT/RM/RTAP/03)** by the Risk Management Coordinator (RMC).

(d) As one risk response may impact on multiple risks, response actions for different risks need to be combined and compared so as to identify and resolve conflicts between plans and to reduce duplication of effort

(e) Treatment Action Plan shall be linked and connected to annual planning and budgeting process and integrated into daily operational functions in order to maximize the chances for curbing risks identified

4.6 Communication and Consultation

The Institute shall ensure continuous communication and consultation with all relevant internal and external stakeholders to ensure iterative exchange of information and opinion about nature of risk, and seek to promote awareness and common understanding. Communication and consultation assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required, hence facilitating the sense of ownership of inclusiveness among those affected by the risks.

DIT should establish internal communication mechanisms in order to support and encourage accountability and ownership of risk management. The Institute shall apply the following techniques to communicate with internal stakeholders:

(i) Risk and control assessments workshops

(ii) Management and staff meetings

(iii) Internal emails and intranet

(iv) Internal staff newsletters and magazines

(v) Blogs and other internal information exchanges

(vi) Notice boards/posters/brochures and other printed materials, and

(vii) one on one discussion.

Communication on risk management issues with external stakeholders shall be made through the well established channels as stipulated in the Government communication guideline of the Standing Order, version 2009

4.7 Monitoring, Review and Continuous Improvement

It is necessary to monitor and review effectiveness of the entire risk management practice for continuous improvement. The framework shall be subjected to a continuous monitoring, evaluation and reviews in order to test and enhance its relevance and usefulness. The risk monitoring, shall be executed through reports by the Head of Quality Assurance and Internal Audit Unit (IAU) through quarterly planned risk-based audits.

The Risk Management Implementation Plan **(RMIP)** DIT/RM/RMIP/05**,** Risk Registers and related Risk treatment Action Plans, Quarterly Risk Performance Reports and Quarterly Physical Progress Reports will be used to facilitate risk monitoring and review**.**

4.8 Risk Reporting

Risk reporting is of paramount importance and need to happen at various intervals during the year. The Institute shall comply to the existing reporting structure to report risk issues such that risk reporting becomes an integral part of the formal DIT reporting structure. The quarterly institutional risk reporting shall be done by the RMC through Quarterly Implementation Reports (DIT/RM/RQIR/04.

4.9 Framework Update

The risk management framework shall be subject to review after every three years, or whenever it is deemed necessary. The Risk Register shall be updated annually to capture emerging issues and delete obsolete issues

SECTION FIVE

5 RISK MANAGEMENT TEMPLATES

The following section presents some of the key template or forms to be filled in the risk assessment process. These include the risk identification and analysis sheet, risk register, risk treatment schedule and action plan and format of the risk management quarterly implementation report**.**

5.3 Risk Identification and Analysis Sheet

The risk identification and analysis sheet is a major tool in risk identification process. The form becomes the basis for preparing the Risk Register. This form can be completed by conducting a formal risk identification workshop and/or on daily basis when a new risk is identified.

Template 1: Risk Identification and Analysis Form

	RISK IDENTIFICATION AND ANALYSIS FORM	**DIT/RM/RIAF/01**
Risk title: Provide a brief title of the risk		**Risk ID:** provide a unique identity

Overview	
Risk	*Provide a brief description of the risk*
Principal risk owner	*Include title of the person managing the risk and the area where the risk falls*
Supporting owner(s)	*Provide title of other persons affected by the risk*
Risk Category	*Is it a financial, technical etc (see template 2)*
Objective/plan	*List the objective impacted by the risk*

Details	
Causes:	***Consequence(s):***
Provide the causes that may lead to the risk materializing	*Provide description of what will happen if the risk will materialize*

Inherent risk analysis (tick the appropriate ratings basing on the scenario that current controls do not exist or completely fails)						
Inherent risk	**Impact:**	*VERY HIGH*	*HIGH*	*MODERATE*	*LOW*	*VERY LOW*
	Likelihood:	*VERY HIGH*	*HIGH*	*MODERATE*	*LOW*	*VERY LOW*
Risk rating	**Impact x**	• *Multiply the ratings from impact and likelihood.*				

	likelihood	• *Shade this area with appropriate color (see Table 7 in section 3.3.6)*

Key risk mitigation/controls <u>currently in place</u>: *-briefly describe the current controls existing to reduce the inherent risk,.*	***<u>and their weaknesses</u>*** *also point out the main weaknesses for the current controls*

Residual risk analysis (tick the appropriate ratings basing remaining risk levels after the above existing controls)						
Residual risk	**Impact:**	*VERY HIGH*	*HIGH*	*MODERATE*	*LOW*	*VERY LOW*
	Likelihood:	*VERY HIGH*	*HIGH*	*MODERATE*	*LOW*	*VERY LOW*
Risk rating	**I X L:**	• *Multiply the ratings from impact and likelihood.* • *Shade this area with appropriate color (see Table 7 in section 3.3.6)*				

Actions/mitigating controls to be taken: *(propose feasible treatment actions to be put in place to reduce the risk at tolerable levels, including resources required for each treatment action –financial, physical assets, or human)*	
Treatment: 1. 2.	**Resource required** 1. 2.

5.4 The Risk Register

The Risk Register is the main document that summarizes the Institute risks at corporate or departmental or Department and Units. The register could be prepared at any decided level (i.e. strategic or departmental, project). The main source of its data is the Risk Identification and Analysis Sheet, which also become its attachments.

Template 2: Extract of Risk Register

	RISK REGISTER	**DIT/RM/RR/02**

OBJECTIVE	FUNCTIONAL OBJECTIVE/ SP-TARGET NO.	RISK TITLE	TYPE OF RISK	RISK ID	RISK ASSESSMENT AS PER CRSA[1]		RISK RATING (I X L)	RISK STATUS	PRINCIPAL RISK OWNER	PAGE
					IMPACT (I)	LIKELIHOOD (L)				

[1] High=3; Medium = 2; Low = 1;

5.5 Risk Treatment Schedule and Action Plan

This follows after the risk register has been prepared. The risk owners should use this form to prepare practical action for implementing the mitigating measures or controls as proposed in the risk identification and analysis sheet**.** Each risk owner shall submit the duly completed Risk Treatment Schedule and Action Plan to the Risk Management Coordinator.

Template 3: Extract of Risk Treatment Schedule and Action Plan

	RISK TREATMENT ACTION PLAN	**DIT/RM/RTAP/03**

Department/Department and Unit: .....
Date of review: ..... Compiled by: ..... Date: .....
Reviewed by: ..... Date: .....

Risk title & ID (From Risk Register in priority order)	**Proposed Treatment/Control Options** (From Risk Identification Sheet)	**Results of Cost-benefit analysis** (A = accept, B = reject)	**Person Responsible for Implementation of Treatment Options**	**Time-table for Implementation** (Give specific start and end dates)	**How will this risk and treatment options be monitored**

5.6 Quarterly Implementation Report

This form shall be used to prepare the Risk Management Quarterly Implementation Report by all risk owners. Each risk owner shall submit the Risk Management Quarterly Implementation Report to the Risk Management Coordinator within two weeks after the end of quarter.

Template 4: Format of the Risk Management Quarterly Implementation Report

	QUARTELY IMPLEMENTATION REPORT	**DIT/RM/RQIR/04**

Department/Department and Unit:
.....
Risk Management Quarterly Implementation Report for the Quarter Ending.....
Prepared by: ..... Date: .....

Risk title & ID (From Risk Register in priority order)	**Proposed Treatment/Control Options** (From Risk Identification Sheet)	**Person Responsible for Implementation of Treatment Options**	**Time-table for Implementation** (Give specific start and end dates)	**How will this risk and treatment options be monitored**	**Status of Implementation**	**Remarks and/or Comments**

5.7 REFERENCES

1. Guidelines for Developing and Implementing Institutional Risk Management Framework in the Public Sector Organizations in Tanzania (2022).

2. International Organization for Standardization (ISO) for implementing Risk Management System (ISO 31000:2018).

5.8 AUTHENTICATION

This document, termed RISK MANAGEMENT FRAMEWORK was adopted by the Institute and becomes effective on this day of: .....,……. 2025.

Approved by:

Chairperson of the Council

Name:

Signature: _____

Date: _____