NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Risk Management Framework



Risk Management Framework

Internal Audit and Risk Management Department

Policy Number	***13/P/6/COUN/ARM***	
Policy Custodian	*Office of Vice-Chancellor*	
Contact Person and Contact Details	*Internal Audit and Risk Management*	
Status	*New Framework*	
Legal Scrutiny	*Chief Legal Advisor*	
Date of Approval by Senate	*13 April 2026*	
Date of Approval by Council	*13 May 2026*	
Effective Date	*13 May 2026*	
Date of Review	*Every five years, or earlier if required*	
Related Policies and Other Documents (Internal and External)	***External***	***Internal***
	Namibia Corporate Governance Code for Namibia (NamCode)	*NUST Draft Risk Management Policy 2024*
	Namibia University of Science and Technology Act (Act No.7 of 2015)	*NUST Statutes, Rules, and Regulations, 2016*
	International Standard ISO 31000:2018 Risk Management – Guidelines	
	International Standard IEC 31010:2019 Risk Management Techniques	

Version Control and Change History			
Version	***Date Approved/ Recommended***	***Approved/ Recommended by***	***Amendment***
1	13 April 2026	Audit and Risk Committee	New Framework
1	13 May 2026	Council	New Framework

AUTHENTICATION

Vice-Chancellor's Signature: _____ Date: 25/06/2026

Registrar's Signature: _____ Date: 09/06/2026

University Seal:

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS 4

DEFINITIONS 5

1. INTRODUCTION 8

2. PURPOSE 8

3. SCOPE OF APPLICATION 9

4. RISK MANAGEMENT PHILOSOPHY 9

5. APPROACH TO RISK MANAGEMENT 11

6. PRINCIPLES OF RISK MANAGEMENT 11

7. LEADERSHIP AND COMMITMENT 14

8. RISK MANAGEMENT PROCESS 14

8.1 COMMUNICATION AND CONSULTATION 15

8.2 SCOPE, CONTEXT AND CRITERIA 17

8.3 RISK ASSESSMENT 19

8.4. RISK TREATMENT 27

8.5. RISK MONITORING AND REVIEW 28

8.6. RECORDING AND REPORTING 30

9. RISK MANAGEMENT STRUCTURE 31

10. ROLES AND RESPONSIBILITIES 32

11. DOCUMENTATION 32

12. REVIEW AND UPDATE OF THE FRAMEWORK 32

Annexure A: Roles and Responsibilities 33

Annexure B: Risk Categories 36

Annexure C: Broad Risk Appetite 40

Annexure D: Risk Action Plan/guide 42

Annexure E: Risk Register 43

Annexure F: Risk Response Plan 44

ABBREVIATIONS AND ACRONYMS

Abbreviations	Meaning
IT	Information Technology
VC	Vice-Chancellor

Acronym	Meaning
ARC	Audit and Risk Committee
EXCO	Executive Management Committee
IRMC	Internal Risk Management Committee
NUST	Namibia University of Science and Technology
PESTEL	Political, Economic, Social, Technological, Environmental, Legal
SWOT	Strengths, Weaknesses, Opportunities, Threats

DEFINITIONS

Term	Definition
Audit and Risk Committee	The three members of the Council, Vice-Chancellor, Deputy Vice-Chancellor, Finance and Administration, Registrar and Internal Auditor.
Control effectiveness assessment	An assessment of the control activities' effectiveness in achieving the desired risk treatment. The assessment can be completed by management or assurance providers.
Executive Management Committee	The Vice-Chancellor, Deputy Vice-Chancellors, and the Registrar.
Impact	The consequence (positive or negative) of the occurrence of a given event (risk).
Inherent Risk	The exposure inherent to the potential risk event in the absence of interventions aimed at decreasing exposure; in short, the risk before actions to reduce it
Internal Risk Management Committee	A Committee established to support the implementation and embedding of risk management within the university. The committee provides oversight, guidance, and coordination in identifying, assessing, and managing risks across university operations.
Likelihood	An estimate of the potential probability that a given uncertain event or condition (risk) may occur.
Operational risks	Exposure to an event resulting from unsuccessful operational controls, operational activities, or incidents that could lead to loss, damage, or injury
Probability	The chance that an event will take place. In the context of inherent risk, it refers to and is influenced by factors such as the macro-economic environment and geographic representation. In the context of residual risk, it is influenced by the efficiency of controls such as human resources, processes, and systems.
Residual Risk	The measurement of risk in terms of its likelihood and impact (consequence) after considering any measures to mitigate the risk.

Risk	The effect of uncertainty on the objectives of the University which may result in both positive and negative outcomes. It encompasses the potential for loss or harm as well as the opportunity for gain or benefit.
Risk analysis	The process is used to understand the nature, sources, and causes of identified risks and determine the risk level. It is also used to evaluate the impact, consequences, and controls currently in existence.
Risk appetite	The types and level of risks that the University is willing to accept in pursuit of its strategic objectives.
Risk assessment	A process to identify, analyse, and evaluate risks and determine risk priorities in terms of predetermined acceptance levels of risk.
Risk evaluation	Application of techniques to evaluate the exposure of one risk against another to prioritise risks
Risk identification	Application of various methods to find, recognise, and describe, inclusive of the main causes and risks that may influence the attainment of goals
Risk management	Coordinated activities to direct and control the University's processes of identifying, assessing, and treating risks.
Risk management framework	The fundamental and organisational components that support and maintain risk management in the university. The fundamental component includes the risk-management policy, goals, mandates, and commitment to these. The organisational component includes the plans, relationships, accountabilities, resources, processes, and activities used to manage the university's risks.
Risk-management policy	A declaration of the targets, direction, and tempo at which an institution strives in risk management
Risk Management Process	A systematic approach used to identify, assess, manage, and monitor potential risks that could impact the achievement of the university's objectives. This process aims to minimize negative outcomes and maximize opportunities through structured methods of handling uncertainties.

Risk Matrix	A tool used to assess and visualize risks by combining two key factors: the likelihood (probability) of a risk occurring and the impact (consequences) if it occurs.
Risk owner	A person, incumbent, or entity with risk management responsibility in a particular operational or strategic area.
Risk Register	A document or tool used to record and track identified risks.
Risk treatment	The selection and implementation of measures to mitigate risks. It may include avoiding, accepting, transferring, or managing the risk.
Risk tolerance	The level of risk the university is willing to accept to achieve its objectives. It sets the limits for different types of risks, indicating how much uncertainty or potential negative impact the university is prepared to bear without taking additional mitigation actions.
Senior management	Senior management means executive deans, executive directors, directors, and heads of university departments.
Strategy	The overall approach to achieving the university's long-term goals and objectives.

1. INTRODUCTION

The Risk Management Framework (RMF) provides NUST with a structured and systematic approach to identifying, assessing, managing, and monitoring risks that may impede the achievement of the university's strategic and operational objectives. This framework outlines the university's risk management processes, methodologies, risk appetite, and reporting mechanisms, while establishing implementation responsibilities. It aligns with NUST's commitment to maintaining high standards in teaching, learning, research, innovation, and entrepreneurship, ensuring the safety and well-being of students, staff, and stakeholders.

In addition, the RMF promotes a proactive risk culture that encourages all members of the university community to engage in risk management practices, fostering an environment where risks are viewed as opportunities for growth and improvement. This framework is designed to align with international best practices, ensuring that NUST remains resilient, responsive, and committed to excellence in all its endeavors.

2. PURPOSE

The purpose of the RMF is to establish a comprehensive and coherent approach to risk management that aligns with NUST's strategic objectives and operational priorities. This framework aims to:

2.1 Enhance Decision-Making: By providing a structured process for identifying, assessing, and managing risks, the RMF empowers decision-makers at all levels to make informed choices that balance risk and opportunity.

2.2 Safeguard Resources: The framework ensures that the university's resources financial, human, and physical are effectively protected against potential threats, thereby promoting sustainability and resilience.

2.3 Promote a Risk-Awareness Culture: The RMF fosters a culture of risk awareness among all stakeholders, encouraging proactive engagement in risk management practices and reinforcing the importance of shared responsibility in safeguarding the university's mission.

2.4 Support Strategic Objectives: By aligning risk management with strategic planning, the RMF facilitates the achievement of NUST's goals, ensuring that risks are understood and managed to support innovation and growth.

2.5 Ensure Compliance and Accountability: The framework establishes clear accountability for risk management activities, ensuring compliance with relevant laws, regulations, and ethical standards, thereby enhancing the university's reputation and integrity.

2.6 Drive Continuous Improvement: The RMF promotes an iterative process of learning and adaptation, enabling the university to refine its risk management practices in response to emerging challenges and opportunities.

Through these objectives, the RMF serves as a vital tool for NUST to navigate the complexities of the educational landscape, ensuring that the university remains resilient, responsive, and committed to excellence in all its endeavours.

3. SCOPE OF APPLICATION

This Framework applies to all staff members (permanent, fixed-term, and part-time) in faculties, departments, students, stakeholders, and entities within the structure and/or under the control of the University. It encompasses all activities, programmes, and projects undertaken by the University, ensuring that risk management is a fundamental aspect of its operations.

The Council holds ultimate accountability for decisions made at NUST and thus must be assured that key issues are effectively managed, ensuring that the University remains on track to meet its objectives. The Council receives NUST's risk management information through reports submitted to the Audit and Risk Committee. Furthermore, the framework applies to all affiliated entities and partnerships to ensure a comprehensive approach to risk management across all university-related activities, fostering collaboration and shared responsibility in risk mitigation.

This philosophy encourages a mindset that views risk as an integral part of decision-making, fostering innovation and resilience within the university while ensuring that all stakeholders are equipped to navigate uncertainties effectively.

4. RISK MANAGEMENT PHILOSOPHY

The philosophy of the University recognises that risk management is a vital element of good corporate governance and is, therefore, fundamental to sound business principles and practices. The focus on

risk management extends beyond merely addressing threats and challenges; it also encompasses the opportunities that arise from effective risk management strategies and procedures. NUST's risk management philosophy is rooted in the understanding that effective risk management safeguards the institution's assets and reputation and enhances decision-making processes across all levels of the organisation.

The following core elements are embedded in the NUST Management Philosophy:

4.1 Holistic Approach: NUST adopts a comprehensive approach to risk management that encompasses identifying, assessing, and mitigating risks while also capitalising on opportunities. This philosophy acknowledges that risks are inherent in all activities and that a proactive stance can transform potential threats into avenues for growth and innovation.

4.2 Integration into Culture: Risk management is integrated into the University's culture, encouraging all stakeholders—faculty, staff, and students—to recognise their role in identifying and managing risks. By fostering a shared responsibility for risk management, the university empowers individuals to contribute to a safer and more resilient environment.

4.3 Continuous Improvement: NUST's commitment to risk management is dynamic and evolves with changing circumstances. The university will regularly review and update its risk management strategies and procedures to reflect emerging trends, regulatory changes, and best practices. This commitment to continuous improvement ensures that the university remains responsive to internal and external challenges.

4.4 Informed Decision-Making: Effective risk management informs strategic management and operational decisions. By understanding the risks associated with various initiatives, the University can make informed choices that align with its mission and objectives, enhancing its ability to achieve long-term success.

4.5 Opportunity Recognition: Risk management focuses beyond merely addressing threats and challenges. NUST recognises that effective risk management strategies can uncover opportunities for innovation, collaboration, and enhanced service delivery. By leveraging these opportunities, the University can strengthen its position as a leader in education and research.

4.6 Stakeholder Engagement: NUST believes in the importance of engaging stakeholders in the risk management process. Open communication and collaboration with internal and external partners foster a shared understanding of risks and promote collective ownership of risk management efforts.

4.7 Commitment to Transparency: The University is committed to transparency in its risk management practices. The University will communicate openly about risks and the measures taken to manage them, thereby building stakeholder trust and confidence.

5. APPROACH TO RISK MANAGEMENT

The University's approach to risk management is embedded in its philosophy that risk management is a vital aspect of good corporate governance. An effective approach ensures that risk management is proactive, structured, and aligned with the university's mission to foster excellence and a progressive educational environment.

The university aligns its risk management practices with internationally recognised frameworks, drawing guidance from the principles and methodologies of ISO 31000 and IEC 31010. This approach supports the university community in effectively managing risks through a structured methodology. The NUST risk management approach is also informed by best practices from leading institutions worldwide, ensuring that it remains current, effective, and responsive to emerging trends in risk management.

6. PRINCIPLES OF RISK MANAGEMENT

The principles guide the key characteristics of effective and efficient risk management, highlighting its value and clarifying its purpose and intent. These principles form the basis for managing risk and should be considered when developing the University's risk management framework and processes. They are designed to help NUST manage the impact of uncertainty on its strategic objectives.

6.1 Integrated

Risk management is not a stand-alone activity separate from the institution's main activities and processes. Risk management is embedded into all the University's processes, including strategic planning, operational activities, and decision-making, ensuring that risk considerations are part of every significant decision.

Furthermore, risk management practices should be integrated into the university's performance management systems to enhance accountability and transparency, ensuring that risk management is a key consideration in achieving performance targets.

6.2 Structured and Comprehensive

The risk management process is systematic, structured, and timely, ensuring that all relevant risks are identified, assessed, and managed comprehensively and effectively. This structured approach allows for the prioritisation of risks, enabling the university to allocate resources efficiently and focus on the most critical areas of concern.

6.3 Customised

The risk management framework is tailored to the university's external and internal contexts, specific objectives, and risk profile. It is designed to reflect the complexity of the university's environment and its unique challenges. This customisation process should involve regular stakeholder consultations to ensure that the framework remains relevant and effective in addressing the evolving risk landscape.

6.4 Inclusive

Risk management is a transparent and inclusive process that involves stakeholders at all levels. Appropriate and timely involvement of stakeholders enables their knowledge, views, and perceptions to be considered, resulting in improved awareness and informed risk management. Engagement with diverse stakeholder groups will enhance the richness of insights gained during the risk management process, fostering a sense of ownership and accountability across the university community.

6.5 Dynamic

The risk management approach is dynamic, anticipating, detecting, and responding to changes in the internal and external environment. It is designed to be flexible and adaptable, ensuring the university can respond promptly to emerging risks and opportunities. The framework should also incorporate continuous feedback and improvement mechanisms, allowing for adjustments as needed in response to changing circumstances.

6.6 Best available information

Risk management relies on historical and current data and future projections. It also considers the limitations and uncertainties inherent in this information and these projections. To be effective,

information must be timely, clear, and accessible to the appropriate stakeholders. Regular training will be provided to ensure that all stakeholders are equipped to interpret and utilise risk-related information effectively.

6.7 Human and Cultural Factors

Risk management acknowledges the abilities, perceptions, and intentions of internal and external individuals that can either support or obstruct the achievement of the university's goals. The importance people assign to different risks affects decision-making and should be thoroughly examined and clearly articulated whenever possible. Cultivating an environment that values diverse perspectives will enhance the university's ability to identify and manage risks effectively.

6.8 Continual Improvement

Risk management is continually improved through learning and experience. The university is committed to continuously improving its risk management practices. Lessons learned from past experiences, stakeholder feedback, and changes in the operating environment are used to enhance the effectiveness of the risk management process. Regular reviews of the risk management framework will be conducted to incorporate the best practices and innovations in the field, ensuring continuous enhancement of the university's risk management capabilities. Regular training and capacity-building initiatives will also be implemented to foster a culture of continuous improvement in risk management practices across the university.

6.9 Resource allocation

Risk management efforts are proportional to the level of risk. Resources and attention are focused on the most significant risks to ensure that the university’s risk management efforts are efficient and effective. The allocation of resources will be regularly assessed to ensure that they are directed towards areas of highest risk and potential impact.

6.10 Risk Ownership

Clear accountability and risk ownership are established at all university levels. Risk owners are responsible for managing risks within their areas of control with the support of the Audit and Risk Management Department. Risk owners will receive ongoing training and support to ensure they can effectively fulfill their responsibilities.

6.11 Compliance with regulations and standards

The university's risk management practices ensure compliance with all relevant legal, regulatory, and ethical standards. This principle underscores the university's commitment to operating within the bounds of the law and maintaining its ethical standards. Compliance audits will be conducted regularly to ensure adherence to these standards and identify areas for improvement, reinforcing the university's commitment to integrity and accountability.

7. LEADERSHIP AND COMMITMENT

The Council and Executive Management lead NUST's risk management efforts. NUST leadership must ensure that risk management is effectively integrated into all aspects of the university's processes and culture and adequately supported by the necessary resources. Management at all levels must be actively involved in and committed to managing risk.

Leadership and commitment require NUST leadership to:

- Allocate sufficient resources, such as personnel, budget, and technology, to implement risk management processes effectively.
- Clearly define roles and responsibilities for managing risks, ensuring that individuals or teams are accountable for identifying, assessing, treating, and monitoring risks.
- Promote a risk-aware culture where employees understand the importance of managing risks and are encouraged to communicate openly about potential risks.
- Regularly review and improve the risk management framework, ensuring it remains effective and responsive to internal and external changes. This includes setting performance indicators and ensuring risks are continuously monitored.

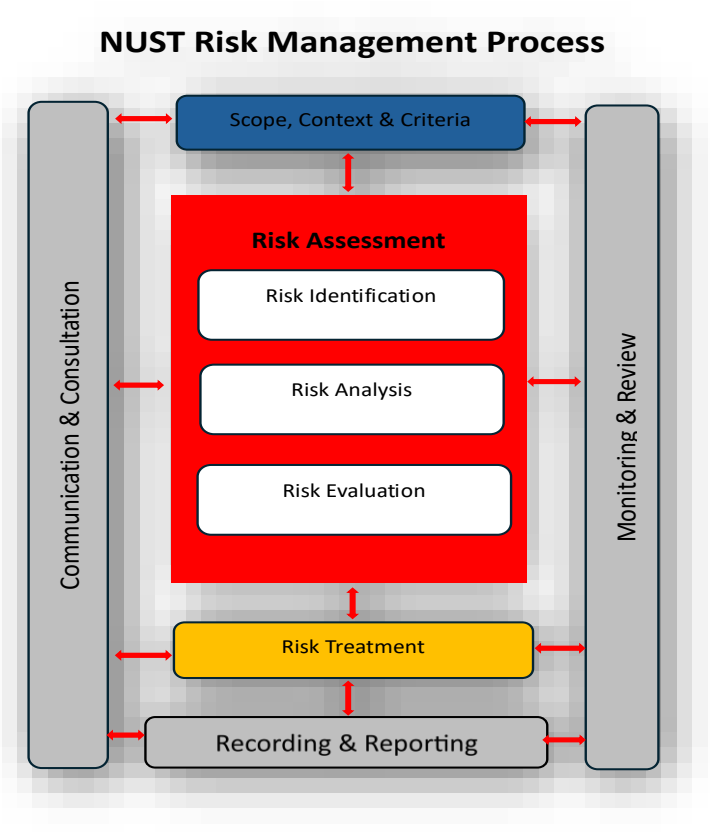
Moreover, leadership will encourage an open dialogue regarding risk management, fostering an environment where staff feel empowered to raise concerns and suggest improvements, reinforcing transparency and trust.

8. RISK MANAGEMENT PROCESS

To align with its risk management policy, NUST embraces a widely recognized risk management process grounded in best practices outlined in the international standards ISO 31000 and IEC 31010. This process provides the university with a structured approach to identifying, assessing, and

managing risks, offering deeper insights into potential threats and their impact on achieving its strategic objectives.

The university's risk management process includes the activities described in 8.1 to 8.6 and shown in **Figure 1** below.



8.1 COMMUNICATION AND CONSULTATION

A risk communication and consultation strategy should be established at the outset of the risk management process. Effective communication and consultation with relevant internal and external stakeholders should occur during all stages of the risk management process. Communication should be honest, relevant, accurate, and easy to understand while respecting confidentiality and personal integrity.

Communication and consultation aim to:

- Bring together various areas of expertise for each stage of the risk management process.

- Ensure diverse perspectives are adequately considered when establishing risk criteria and assessing risks.
- Provide the necessary information to support risk oversight and informed decision-making; and
- Foster a sense of inclusiveness and ownership among those impacted by risk.

This involves the following actions:

8.1.1 Stakeholder Involvement: Engaging with stakeholders at all levels to ensure understanding and buy-in for the risk management process.

8.1.2 Reporting: Keeping senior management informed on key risks, changes, and mitigation measures.

The following are examples of the University's internal and external stakeholders to be considered in this process:

Internal

- NUST Council and sub-committees.
- Vice-Chancellor.
- Executive Committee.
- Heads of Departments, Faculties, Centres, and Units.
- Internal Audit.
- NUST managerial employees.
- Risk Owners and Risk Champions.
- Students.

External

- Government.
- Regulatory Bodies.
- NUST Suppliers.
- External Auditors.
- Relevant Ministries; and
- Third-party service providers.

8.2 SCOPE, CONTEXT AND CRITERIA

In risk management, establishing the scope, context, and criteria is a critical step that ensures clarity on the boundaries, environment, and parameters within which risks will be managed. This step lays the foundation for a focused and effective risk management approach. At NUST, it is imperative to comprehensively understand both the internal and external environments, aligning risk management with strategic objectives while defining clear risk evaluation criteria.

8.2.1 Defining the Scope

The scope outlines the range of activities, processes, and areas the risk management process will cover. The scope of a university can be broad and include various academic, administrative, operational, and compliance activities. It is essential to clarify the extent to which risk management will apply within the institution.

Key Aspects of Scope

- **Departments and Faculties** – Identify which academic and administrative units are directly involved in risk management (e.g., Faculty of Engineering and the Built Environment, Faculty of Health, Natural Resources, and Applied Sciences, Finance).
- **Activities and Processes** – Specify the unique activities (teaching, research, administration, student services, etc.) that are subjects that fall under the risk management umbrella.
- **Period** – Clarify whether the focus is on short-term (current academic year) or long-term (strategic planning over several years).
- **Stakeholders** - Identify the key stakeholders affected by the risks (students, staff, faculty, alumni, regulators) to ensure their input and perspectives are considered.

8.2.2 Establishing Context

The context of the risk management process is defined based on an understanding of the internal and external environments in which NUST operates and is tailored to the specific environment of the activity to which the process will be applied. This process also involves a thorough analysis of the university's institutional landscape, including governance structures, regulatory requirements, and stakeholder expectations. Evaluating the University's strengths, weaknesses, opportunities, and

threats (SWOT) alongside identifying key external stakeholders is crucial for a well-rounded risk assessment.

8.2.3 Risk Criteria

NUST recognises that effective risk management is vital to achieving its strategic objectives and preserving its reputation in higher education. The university is committed to a balanced approach to risk-taking, ensuring that opportunities are pursued while safeguarding its core values, mission, and stakeholder interests.

8.2.3.1 Risk Appetite

Risk appetite refers to the level of risk the University is prepared to accept in pursuit of its objectives. It is essential to determine acceptable risk levels, which provide a reference point for strategic planning and objective setting, and manage stakeholder expectations regarding the risks the University is prepared to assume.

The Executive Management develops the university's risk appetite and proposes it to the Council through the ARC for approval. Once approved, it is the responsibility of the Council and the EXCO to communicate the university's risk appetite to NUST staff and key stakeholders, as needed.

The risk appetite statement indicates the level of risk and the risk appetite within each category. Refer to **Annexure C** for the University's risk appetite statements across the various risk categories.

Risk appetite is a critical component of the strategic planning process. Therefore, it must be established and communicated throughout this process. The risk appetite should also be updated to align with ongoing strategic planning efforts.

8.2.3.2 Risk Tolerance

Risk tolerance is defined for each specific risk and reflects the level the University is willing to accept while pursuing its strategic objectives. The risk tolerance level is set when completing the risk assessments and ensures that the University operates within its overall risk appetite. Collectively, these risk tolerances represent the University's appetite for each strategic objective or risk category, providing a framework for decision-making.

8.3 RISK ASSESSMENT

Risk Assessment is a process that helps management understand the likelihood and impact of potential events and associated risks identified during event identification. This process offers a standardised and consistent approach to evaluating risks that affect objectives across the University, providing management with a comprehensive view of the risks (i.e., the "risk profile").

The university should conduct risk assessments systematically, continuously, and collaboratively, incorporating the knowledge and perspectives of stakeholders. It should use the best available information, supplemented by further inquiry when necessary. Risk assessment includes three key phases: Risk Identification, Analysis, and Evaluation.

8.3.1 Risk Identification

Risk identification seeks to discover, recognise, and describe risks that may enhance, hinder, or delay the achievement of the University's objectives. A proactive approach to identifying risks is essential, as it allows the University to anticipate challenges and seize opportunities effectively.

The University's risk categories, outlined in **Annexure B**, ensure that all major areas of risks threatening business objectives are considered during the identification process. This list is for guidance only and should not be deemed to be exhaustive.

Risk identification is crucial at both strategic and operational levels, and all significant sources of risk, including those outside the University's control, should be considered.

8.3.1.1 Approaches to risk identification

Three basic approaches can be adopted in identifying risk:

- Quantitative Method – This approach collects and develops relevant historical or predictive data sets to analyse risks numerically.
- Qualitative Method - This method includes, but is not limited to, techniques such as market research, surveys, questionnaires, and risk workshops to gather subjective data.
- Semi-quantitative Method - This involves using a combination of both quantitative and qualitative techniques for a more rounded view of risks.

8.3.1.2 Risk sources

To ensure consistency and standardisation in risk identification, the following sources can be used:

- External (using models such as SWOT and PESTEL analysis)
- Operations (business process level risks, business continuity plans)
  information Technology (trends in technology)
- Strategic Information (strategic risk registers, competitor analysis, market trend analysis)
- Operational Information (audits, internal questionnaires, performance reports)
- Financial Information (financial reports, budgets)

8.3.1.3 Risk identification techniques

Various tools can be employed to identify risks at different levels within the university. These tools include, but are not limited to, the following:

- SWOT and PESTLE analysis
- Scenario planning
- Peer organisation benchmarking
- Workshops
- Interview and focus organisation discussion
- Brainstorming
- Incidence analyses
- Questionnaires and surveys
- Flowcharting and system analysis
- Decision trees
- Audit reports (internal, quality, compliance, external, etc.)

8.3.1.4 Questions to consider

- What could prevent the achievement of objectives?
- When, where, why, and how are the risks likely to occur, and who might be involved?
- What is the source/category of each risk?
- What resources are needed?
- What are the stakeholders' expectations?

8.3.1.5 Procedures of risk identification

- Confirm the unit, department, process, or project's objectives.
- Determine the most appropriate method of identifying risks; more than one technique can be used.
- Identify all the root causes/sources of those situations, trends, events, or circumstances (risks) that may impact on the objectives.
- Identifying areas of opportunities.
- Capture all the information on a risk register.

The Audit and Risk Management Department coordinate the risk identification workshops for each department and faculty within NUST. Risks will be identified and recorded during these sessions in the risk register. The format of NUST's Risk Register is provided in **Annexure E**.

8.3.2 Risk Analysis

Risk analysis aims to comprehend the nature of risk and its characteristics, including the level of risk. It thoroughly examines uncertainties, risk sources, potential consequences, likelihood, events, scenarios, controls, and their effectiveness. An event may have various causes and consequences, potentially impacting multiple objectives.

Risk analysis may be conducted with different levels of detail and complexity, depending on the analysis's purpose, the quality and availability of information, and the resources at hand.

The following factors should be considered:

- The likelihood of events and consequences.
- The nature and magnitude of consequences.
- The complexity and connectivity.
- Time-related factors and volatility.
- Effectiveness of existing controls.
- Sensitivity and confidence level.

Risk analysis informs risk evaluation and guides decisions on whether and how risks should be addressed. It also helps determine the most suitable strategies and methods for risk management.

8.3.2.1 Likelihood Rating

The likelihood rating indicates the probability that an identified risk may materialise. It reflects how likely and how often an event is expected to occur, ranging from almost certain to rare.

There are several methods to estimate the probability (quantitative) or likelihood (qualitative) of an event. Expert judgment is crucial in ensuring that the outcomes of any modelling or extrapolation process are accurate and reliable.

The tools and techniques used for estimation can be categorised as follows:

- Extrapolation of historical data - This method identifies the root causes of past events or situations if similar circumstances will lead to recurring events, making predictions reliable in operational contexts.
- Probability modelling - When specific information about a risk or situation is limited or unavailable, a model based on the theoretical behaviour of the system is developed to forecast future events. This model can be calibrated using data from similar systems, organisations, technologies, operational experiences, or externally available data.
- Expert judgment **-** The insights of industry experts and specialists are highly valuable and should be considered when estimating the likelihood of an event.

Table 1 indicates the established likelihood levels, description, probability, and the appropriate ratings that may be used.

Table1: Likelihood rating

Likelihood Rating	Description	Frequency of Occurrence	Probability	Rating
Almost Certain	Highly likely to happen/occur, possibly frequently in most circumstances	Expected to happen multiple times a year.	91-100%	5
Likely	Will probably happen/occur but not persistent in nature.	Could occur once or more per year.	66-90%	4
Possible	May happen/occur occasionally	May happen once every 1-3 years.	36-65%	3
Unlikely	Not expected to happen but it is a possibility	May occur once every 3-5 years.	11-35%	2
Rare	Very unlikely to occur; will never happen	Unlikely to happen more than once every 5-10	0-10%	1

8.3.2.2 Impact Rating

The impact rating indicates the possible magnitude of the effect of the risk should it manifest. The impact or consequence of a risk materialising can range from immaterial to catastrophic.

When a risk or opportunity materialises, its impact can vary across several areas. It may result in financial losses, affect human resources through injuries or fatalities, disrupt business continuity, lead to legal or compliance issues, or have environmental or community consequences. The Impact Rating Table below indicates the established impact levels and ratings that should be used.

Table 2: Impact Rating

Level	Description	Rating
Catastrophic	A disaster or event that will prevent the University from achieving its strategic objectives and may lead to lasting negative consequences.	5
Major	A serious event that can be endured but will have extensive negative consequences over the long term.	4
Moderate	An event that can be managed but will have extensive negative consequences in the short term.	3
Significant	An event that can be sustained under normal operating conditions.	2
Insignificant	An event that will have no or a limited impact on the University.	1

8.3.2.3 Inherent Risk Rating

The inherent **risk rating** is the level of risk present before any measures, controls, or mitigation strategies are applied to reduce it. It represents the natural level of risk associated with an activity, process, or situation, assuming no preventive actions are in place. Inherent risk is determined by **Likelihood (Probability) x Impact (Consequence).** The purpose of assessing the inherent risk rating is to understand the baseline level of risk, allowing the University to evaluate what mitigation efforts are necessary to reduce the risk to an acceptable level.

The risk rating is important to:

- **Prioritise Risks:** Risk rating helps the University to focus on the most critical risks that need immediate action or in-depth mitigation efforts.
- **Efficient Resource Allocation:** By identifying high-risk areas, resources (e.g., time, budget,

personnel) can be allocated more effectively to manage or reduce those risks.

- **Informed Decision-Making:** Risk ratings provide decision-makers with a clear view of which risks have the greatest potential to disrupt operations or harm the University, guiding better strategic planning.
- **Risk Communication:** Standardised risk ratings offer a common language for stakeholders to understand the significance of risks and agree on risk management strategies.

All identified risks must be categorised into four risk levels, which determine the significance of the risk to the University. These risks are classified as shown in Table 3 below.

Table 3: Risk Rating

Risk Rating	Risk Description	Reporting requirements
Critical 20 -25	Severe risks that can lead to collapse of the University's and fundamental to the achievement of objectives (result in catastrophic outcomes for the university, such as financial crisis, severe reputational damage, legal issues, or operational shutdowns).	EXCO, ARC, Council
High 10 - 19	Risks that could cause significant disruptions or harm. These risks can affect multiple areas of the university, including academic programs, financial health, and institutional reputation, and will require a strategic response.	EXCO, ARC, Council
Medium 5 - 9	Risks that could lead to noticeable disruptions. These risks may require additional management attention and resources to prevent moderate impacts on students, staff, finances, or reputation.	EXCO
Low 1 - 4	Risk that can be easily managed through routine procedures. These risks may cause small, localised disruptions, with minimal consequences to the university's functioning.	Monitored at Department level

8.3.2.4 Risk Matrix

A risk matrix is a tool used to assess and visualize risks by combining two key factors: the likelihood (probability) of a risk occurring and the impact (consequences) if it occurs. It provides a clear framework for determining the severity of risks and helps prioritize them for effective management. Applying the risk matrix ensures consistency and a standard rating approach across the University. The University's Risk Matrix is depicted in Table 4 below.

Table 4: Risk Matrix

LIKELIHOOD						
	Almost Certain 5	5	10	15	20	25
	Likely 4	4	8	12	16	20
	Possible 3	3	6	9	12	15

	Unlikely 2	2	4	6	8	10
	Rare 1	1	2	3	4	5
		Insignificant 1	**Significant 2**	**Moderate 3**	**Major 4**	**Catastrophic 5**
		IMPACT				

8.3.2.5 Risk Register

All fully described risks must be recorded in the risk register or an equivalent system. This register should also detail the risk responses undertaken and the relevant controls implemented to manage the risks. NUST utilises the Risk Register template as shown in **Annexure E**.

8.3.3 Risk Evaluation

The last step in the risk assessment process is the risk evaluation. This step requires the University to evaluate the adequacy of existing controls to prevent or mitigate the identified risks. After assessing the controls, they are applied to the inherent risk rating to determine the residual risk rating. The residual risk rating is then compared to the University's risk tolerance or risk appetite, and an appropriate risk treatment strategy is chosen for any risks exceeding this threshold.

8.3.3.1 Controls Assessment Rating

When determining whether a control effectively addresses a risk, the following questions should be considered:

- Does the nature of the controls adequately address the risk?
- Are the controls properly documented and communicated to all relevant parties?
- Are the controls functioning effectively and applied consistently?

Controls are categorised as preventative controls (those controls that reduce the likelihood of a risk materialising) or corrective controls (those controls that mitigate the impact of a risk when it does materialise).

When assessing the control effectiveness and/or the need to implement additional controls or mitigating measures, it is important to consider the benefits of maintaining or implementing controls. If the cost of implementing a control exceeds the benefits, it would not be cost-effective to implement

such a control. Table 5 below provides the description and the rating to be used when assessing the adequacy of controls.

Table 5: Control Assessment Rating

Level	Description	Rating
Excellent	All measures and controls have been implemented to mitigate the risk fully.	1
Good	Measures and controls are in place to mitigate the risk, but there is room for improvement.	2
Average	Measures and controls are in place, but only partially mitigate the risk and require improvement.	3
Inadequate	The controls and measures in place do not adequately mitigate the risk and require significant improvement.	4
Unacceptable	Few or no measures and controls are in place to mitigate the risk. Immediate action is needed to implement or significantly improve these controls.	5

8.3.3.2 Residual Risk Rating

After assessing the controls, the assessment is applied to the inherent risk rating to determine the residual risk rating. This rating reflects the level of risk that remains after considering the measures or controls implemented to reduce or mitigate it. The residual risk rating will reveal the severity of the risk and guide the selection of suitable risk treatment options.

The following process is followed in assessing the residual risk:

1. **Identify Inherent Risk**: Assess the level of risk before applying any controls or mitigation strategies. This is based on the potential impact and likelihood of the risk occurring.
2. **Evaluate Existing Controls**: Review the current controls to mitigate the risk. This includes assessing how well these controls reduce the likelihood or impact of the risk.
3. **Assess Control Effectiveness**: Determine whether the existing controls are adequate and effective. Consider if they are properly designed, implemented, and functioning as intended.
4. **Calculate Residual Risk**: After evaluating the controls, reassess the risk by considering the reduced likelihood or impact. Residual risk = Inherent Risk – Control Effectiveness.
5. **Use Risk Rating Matrix**: Apply a risk rating matrix (impact vs. likelihood) to classify the residual risk as Critical, high, medium, or low based on the reduced likelihood and/or impact.

6. **Document the Outcome**: Record the residual risk, considering the current controls and the potential for further mitigation if necessary.

8.3.3.3 Opportunity Assessment

The methodology used for identifying and evaluating risks should also be applied to gathering commercial insights on opportunities. This assessment process should go beyond simply recognising the positive side of threats. Evolving business environments present risks and opportunities for innovation or adapting the University to new challenges.

Opportunities identified by management should be shared, validated, and addressed by employees throughout the university in a top-down approach. At the same time, employees should be encouraged to communicate their own ideas for improvement, adaptation, and innovation through the institution's management structure in a bottom-up manner.

8.4. RISK TREATMENT

Risk treatment aims to select and implement options to address risk. After the residual risk rating for all assessed risks has been determined, a risk treatment strategy must be determined for risks that fall outside acceptable levels.

8.4.1 Risk Treatment Options

Choosing the most suitable risk treatment option(s) requires weighing the potential benefits of achieving objectives against the associated costs, efforts, or implementation drawbacks. Risk treatment options may not always be mutually exclusive nor universally applicable in all situations.

Even with careful planning and execution, risk treatments may not yield the expected results and could lead to unforeseen consequences, including the creation of new risks. For this reason, ongoing monitoring and review should be essential to the risk treatment process to ensure that the chosen methods remain effective over time.

If treatment options for a specific risk are not available or if they do not adequately mitigate the risk, the risk should be documented and continuously monitored.

Risk treatment includes the following options:

- **Avoidance** - Eliminating the risk by not engaging in or terminating the activity that generates it.
- **Tolerate** - Acknowledging the risk and deciding not to take further action where the risk is deemed acceptable or where the cost of mitigation may be higher than the potential impact.
- **Transfer -** Transferring the risk to a third party, for example, through contracts, insurance, or outsourcing.
- **Treat/Mitigate -** Implement controls to reduce the likelihood or impact of the risk occurring.
  Reduce likelihood – This can be done by implementing preventative controls.
  Reduce impact - Implement corrective control to alter the severity of the risk should it materialise (e.g., business continuity, disaster recovery, and incident management plan)
- **Enhance -** Pursuing opportunities by initiating or continuing an activity likely to generate or enhance the positive side of the risk.

8.4.2 Risk Treatment Plan

The risk treatment plan outlines how the selected treatment options will be implemented, ensuring that all parties know the approach and allowing progress to be tracked and monitored against the plan. The treatment plan allocates actions to specific individuals or groups of individuals with clear due dates.

For all risks with a residual rating of Critical, High, and Medium, the University must develop and approve specific risk treatment strategies, establish timelines for implementation, assign appropriate responsibilities, and ensure adequate progress reporting. **Annexure F (Risk Response Plan)** should be used to document the appropriate action.

8.5. RISK MONITORING AND REVIEW

Risk monitoring and review are important in successfully implementing the identified risk strategies. It is important to frequently review and continuously monitor the risk mitigation plan to determine whether there are changes in the risk conditions and whether the risk remains a risk for the University. Risk monitoring also helps identify new risks that might be on the horizon so the University can better prepare to manage them.

While risk management is an ongoing management responsibility, there are specific occasions when the formal risk management process should be conducted. These include:

- Annually, as part of the strategic planning process.
- Before commencing with any major new initiatives by the Faculties, Departments, Centres, or University-controlled entities.
- Before starting any significant new commercial venture or collaboration.
- Before the launch of any major institutional project.
- Before commencing any activity that may pose a risk of injury, significant property damage, or harm to the University's reputation.
- As required by other University's policies, procedures, or legislation.

8.5.1 Procedures for Monitoring and Review

An Institution-wide review process will be conducted systematically. This review aims to assess whether each previously identified risk remains relevant to the University and evaluate the adequacy of:

- the assessments of impact and likelihood for each risk.
- risk ratings.
- the effectiveness of existing systems and risk mitigation controls.
- the residual risk ratings.
- the treatment strategies previously considered.

When performing the annual risk management process review, the following considerations should be made:

- **New Influence** – Are there new external or internal influences to consider?
- **Strategic Alignment** – Does the risk register align with institutional strategy and intent?
- **Controls** – Are existing controls sufficient and effective to keep exposure within limits?
- **Structure** – Are institutional structures sufficient and effective to support internal and external expectations?
- **Adaptability** – Review and organise the ability to act timeously on new internal and external influences.
- **Reporting** – Monitor and review the effectiveness and reporting processes.

8.5.2 Independent Risk Management Evaluations

Independent assurance providers, such as internal and external auditors, offer an objective assessment of the University's internal controls and, by extension, the components of its Risk Management Framework. The Internal Audit/Assurance team will review the risk management process every two years, producing a report for the Audit and Risk Committee. This report will evaluate the effectiveness of the Risk Management Framework and its processes and, where necessary, provide recommendations for improvement.

8.6. RECORDING AND REPORTING

8.6.1 Institutional Reporting

The Audit and Risk Management Department coordinate the enterprise-level risk reporting and will aggregate and develop risks per department or faculty. The ARM department will present the department's and faculty's risks quarterly to the Internal Risk Management Committee, EXCO, and the Audit and Risk Committee. The Risk Report will include:

- Risk Register
- Executive summary of key changes in risk profile and appetite.
- Commentary on critical residual risk (for committee consideration).
- Details of escalating risks and emerging risk issues considered during the reporting period.
- Significant project risk (if applicable).

8.6.2 Appropriate Committees

Internal Risk Management Committee:

The University’s Risk Register will be reviewed quarterly. Each member will report the risks of Units/departments under their authority. The ARM department will consolidate the reports for the EXCO and ARC reporting.

EXCO

EXCO members will review the University’s Risk Register quarterly. Each EXCO member will be accountable for the risks under their departments.

Audit and Risk Committee

The ARM department will report quarterly to the ARC on the University's Risk Register (high and critical risks).

Council

The ARC will report quarterly to the Council on the University's Risk Register (high and critical risks). The ARC will also report to the Council in December each year on the state of the risk management process at the University. This report will inform the annual statement of assurance.

8.6.3 Risk Reporting Indicators

The following indicators will be used for monitoring and reporting purposes.

Description	Indicator
New risk	
Closed out risk	
Risk reduced	
Risk remained same	
Risk increased	

9. RISK MANAGEMENT STRUCTURE

While all line managers are responsible for risk management, specific governance and management structures within the University's stakeholder community are primarily tasked with overseeing and controlling the risk management process, including:

- NUST Council
- Audit and Risk Committee
- Vice-Chancellor
- Executive Management Committee
- Internal Risk Management Committee; and
- Audit and Risk Management Department

10. ROLES AND RESPONSIBILITIES

The roles and responsibilities of each structure are outlined in **Annexure A.**

11. DOCUMENTATION

Proper documentation on the risk management activities must be maintained. Documentation is necessary to enable the following:

- Demonstrate that the risk management process was conducted in alignment with the University's approved risk management policy.
- Serve as a resource for performance management purposes.
- Provide documentation of decision-making processes in case a project falls short of expectations or if legal action against the University arises.
- Offer evidence of any cost/benefit analysis conducted.
- Contribute to the development of the annual internal audit plan.

As a baseline, the following documentation should be compiled:

- Risk Identification and Assessment worksheet.
- Risk Treatment Plan (where applicable).
- Strategic and Departmental Risk Registers.

12. REVIEW AND UPDATE OF THE FRAMEWORK

The Audit and Risk Management department oversees the review and annual update of the risk management framework and adjusts whenever changes to relevant guidelines impact on the framework.

ANNEXURE A: ROLES AND RESPONSIBILITIES

Role player	Responsibility
NUST Council	• Set the tone and influence the risk management culture at the highest level. • Provides oversight and ensures that risk management is effectively integrated into the University's governance framework. • Approves the University's risk appetite. • Considers the critical risk exposures that the university faces. • Ensures that effective risk-based internal audits and reporting occur and reports on the efficiency of the risk management system and internal controls. • As part of the annual report, reports on how the university dealt with institutional risks.
Audit and Risk Committee	• Recommends risk management policy and framework to the Council for approval. • Review the risk management process and the high-to-critical risks facing the University on behalf of the Council. • Reports to the Council on its risk management responsibilities. • Annually reviews the institution's approach to risk management and recommends changes or improvements to key processes and procedures to the Council for approval.
Vice-Chancellor	• Accountable to the Council to ensure that the University fulfils its risk management responsibilities effectively. • Accountable to the Council to ensure that a robust risk management framework for the University is established, implemented, and maintained.

	• Oversees the risk management process's design, implementation, and monitoring, ensuring its integration with the University's business processes. • In consultation with the Executive, determines and recommends the University's risk appetite to the Council for approval.
NUST Executive	• Ensures compliance with the University's Risk Management Policy and Framework across all departments. • Fosters a culture that embraces risk management as a collective responsibility among all university staff within their area of responsibility. • Oversees and manages risks within their domains, including specific risks delegated by the Vice-Chancellor. • Integrates risk assessment into their ongoing decision-making processes. • Conducts a quarterly comprehensive review of the University's Risk Register.
Internal Risk Management Committee	Provide oversight, guidance, and coordination in identifying, assessing, and managing risks across university operations.
Senior Management	• Ensures compliance with the University's Risk Management Policy and Framework within their areas of responsibility. • Appoint the Risk Champions within their departments. • Maintains a Departmental Risk Register for their area of responsibility. • Manages risks within their area of responsibility, including specific risks assigned to them by the respective EXCO Member. • Accountable to their respective EXCO Member to ensure they fulfil their risk management responsibilities.
Risk Management Department	• Develops and maintains a Risk Management Policy and Framework for the University. • Establishes processes and tools to facilitate effective risk management across the University.

	• Coordinates the university's annual risk review and compilation of the institutional risk register. • Provides risk management training and guidance to all staff in managerial and decision-making roles in implementing risk management principles. • Regularly monitors the implementation and effectiveness of the University's risk management processes. • Alert the Vice Chancellor to any significant risks that arise outside the normal risk management process of the University.
NUST Staff	• Actively manages risks within their day-to-day operations to ensure a safe and productive environment. • Identifies potential risks within operational practices and promptly reports to the appropriate management for further action.
NUST Stakeholder	• Are encouraged to proactively raise any risk-related concerns with NUST management to foster a culture of transparency and accountability
Assurance providers	• Provide assurance on the adequacy, efficiency, and effectiveness of the University's risk management processes.

ANNEXURE B: RISK CATEGORIES

Risk Category	Broad definition and examples
Strategic	These risks affect the achievement of the strategic plan and objectives. Examples: •Failure to maintain, grow, and diversify income streams •Failure to deliver strategically high-profile projects Failure to offer new programs in response to the market demands •Inadaptability to provide alternative learning solutions •Inability to adapt programs to equip a graduate of the future •Inadequate implementation and execution of changing strategies
Teaching, Research and Community Engagement	These risks affect the quality of teaching, research, and community engagement. Examples: • Curriculum design flaws and outdated programs • Inadequate assessment processes • Inadequate library services • Plagiarism and other academic fraud • Failure to obtain/maintain academic standards and accreditation requirements • Inadequate research skills of staff • Failure of staff to engage in research and scholarly activities • Insufficient guidance of research students • Improper research ethics
Legal and Compliance	Risks relating to potential liabilities resulting from third-party lawsuits, contract disputes, and non-compliance with Acts, laws, and regulations, including non-compliance with university policies and procedures by staff members. Examples: • Failure to protect intellectual property and personal information

	• Inadequate contract management and liability/damages claims • Litigation resulting from improper research ethics and student disputes • Ineffective internal controls over financial reporting • Non-compliance with Occupational Health and Safety legislation • Non-compliance with Labour Laws
Operations	Risks arising from internal processes, people, systems, or external events that can disrupt the university's operations and ability to achieve its objectives. **Examples**: **Management and Governance** • Inappropriate governance, management, and committee structures • Inadequate/ineffective performance management • Inadequate internal communication • Inadequate succession planning **Human Resources** • Effects of organisational change • Low staff morale • Inappropriate staff discipline • Inadequate staffing capacity and staff retention • Lack of training and development **Health, Safety and Environment** • Inadequate emergency response plans • Inadequate safety and security for staff and students • Mental health issues among staff and students • Workplace accidents or injuries. **Business Continuity** • Inadequate crisis management • Major breakdowns of the IT system

	• Loss of facilities due to fire and natural disasters • Major acts of violence on campus **Students** • Student unrest or protests • Mental and physical health issues • Dropout and low student retention • Poor student experience
Financial	Risks that may have a detrimental effect on the University's financial position. Examples: • Abnormal increase in expenses or an abnormal decrease in subsidy income and other revenue streams • Rising cost of tertiary education and increasing student loan debt • Inadequate cash flow management • Inadequate investment management • Failure to commercialise research effectively
Information Technology	Risks relating to Information Technology Systems. Examples: • Increased cyberattack • Inadequate IT infrastructure • Obsolete software/hardware • Lack of data integrity •Increasing deployment of cloud technology and the management around it •Social media/social networks could lead to inadvertent disclosure of educational records or personally identifiable information •Balancing and rightsizing IT priorities and budget •Emerging technologies such as virtual reality, drone technology, and blockchain technologies

Image, Reputation and Ethics	Risks affecting the image and reputation of the University. Example: • Adverse publicity in local and overseas publications • Insensitive handling of crises • Negative experiences of the University by stakeholders • Declining student performance • Research fraud by academics and students • Inappropriate use of emerging technologies • Failure on academic excellence, academic freedom, alumni relations, constitutional challenges, free speech, and expression. • Increased fraud risk.

ANNEXURE C: BROAD RISK APPETITE

Risk Category	Risk appetite description
Strategic Risk	The university has a **moderate** risk appetite for pursuing innovative academic and research initiatives that enhance the university's standing, recognising that calculated risks are necessary to achieve long-term growth and excellence.
Operational Risk	The university has a **low** appetite for operational risks, such as IT system failures, administrative inefficiencies, and disruptions to academic programs or services.
Financial Risk	The university maintains a **low** appetite for financial risks affecting core operations such as financial reporting but may accept moderate risks related to investments or new funding models to enable diversification and sustainability.
Compliance Risk	NUST is committed to maintaining the highest integrity, compliance, and ethical standards. There is a **low** appetite for non-compliance with laws, regulations, and accreditation standards to protect the institution's integrity and legal standing.
Reputational Risk	The university has a **low** appetite for risks that could damage its reputation, academic standing, or relationships with key stakeholders.
Health, Safety, and Security Risk	The university has a **low** appetite for student and staff health, safety, and well-being, with strict measures to mitigate risks.
Research & Innovation	The university accepts a **high** level of risk in research and innovation, encouraging groundbreaking work that may have uncertain outcomes but could yield high rewards.
Environmental Risk	The university aims to minimize environmental risks and adopt sustainable practices, with a **low** appetite for risks that impact sustainability efforts.
Technology and Cybersecurity Risk	The university has a **moderate** risk appetite for adopting new technologies to enhance learning and operational efficiency but maintains a **low** risk appetite for cybersecurity risks, ensuring the protection of sensitive data and personal information.

Student Experience	University prioritises the student experience and has a **low** appetite for risks that could negatively affect student services, support systems, or learning outcomes.

ANNEXURE D: RISK ACTION PLAN/GUIDE

Residual Risk Level	Action to be taken	Responsible level of management	Level of reporting and oversight
Critical	Urgent and immediate action is required. • Responsible Member of the Executive to recommend risk response and prepare a risk treatment plan. • Recommended risk treatment plan is presented to the Vice-Chancellor for review and approval. • The Vice-Chancellor takes ownership of the risk and decides on further appropriate action.	The Vice-Chancellor	EXCO Audit and Risk Committee NUST Council
High	Immediate action is required. • The Responsible Member of the Executive and Senior management decide on a risk response and prepare a risk treatment plan. • The Executive takes ownership of the risk	EXCO Member and responsible senior management (Risk owners).	EXCO. Audit and Risk Committee
Medium	Action is required. • A responsible member of the Executive appoints a risk owner (member of his/her senior management team). The risk owner decides on the risk response and prepares a risk treatment plan for approval by the member of the Executive. • The risk owner monitors the risk and reports progress to the Member of the Executive.	EXCO Member and responsible senior management (Risk owners).	EXCO. Executive Member
Low	No immediate action is required. • Risk monitored by the Risk Owner for any change in risk events.	The appropriate member of the senior management team (Risk Owner).	Executive Member

ANNEXURE E: RISK REGISTER

Risk Number	Objective	Risk Category	Risk heading	Risk description	Risk owner	Inherent Risk			Current controls	Residual Risk			Acceptable risk level	Controls to be implemented	Task owner	Due date
						Likelihod	Impact	Risk rating		Likelihod	Impact	Risk Rating				

ANNEXURE F: RISK RESPONSE PLAN

Risk	likelihood	impact	Current control	Response chosen	Secondary risk,possible benefits and effects on stakeholders	Responsibility: Implementation Approval	Proposed Actions	Required resources	Contingencies, performance measures and constraints	Reporting and monitoring requirements	Timing and schedule



NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Office of the Vice-Chancellor

Risk Management Framework

Private Bag 13388
Windhoek, NAMIBIA

T: +264 61207 2306
F: +264 61207 9306
E: ovc@nust.na