Risk Management Policy

Version 1.1

Revision History:

Date of this revision:	19th February 2024
Date of next review:	19th February 2024
Version Number/Revision Number	1.1
Revision Date	19th February 2024
Summary of Changes	• Change to new Policy Format. • Change of Review Period to 2 Years
Changes Marked	Yes
Date of this revision:	13 April 2022
Date of next review:	13 April 2023
Version Number/Revision Number	1.0
Revision Date	N/a
Summary of Changes	New Policy
Changes Marked	N/a

Consultation History:

Number/ Revision Number	1.1
Consultation Date	23 January 2024
Names of Parties in Consultation	UPT
Summary of Changes	Change to two years review period
Number/ Revision Number	1.0
Consultation Date	N/a
Names of Parties in Consultation	N/a
Summary of Changes	N/a

Approval:

This document requires the following approvals:

Version:	1.1
Approved By:	Governing Body
Date:	19th February 2024
Version:	1.1
Approved By:	Audit and Risk Committee
Date:	6th February 2024
Version:	1.0
Approved By:	Governing Body
Date:	13th April 2022

Quality Assurance:

Version:	1.1
Date Approved	19th February 2024
Date Policy to take effect:	19th February 2024
Date Policy to be reviewed:	19th February 2026
Version:	1.0
Date Approved (V1)	13th April 2022
Date Policy to take effect:	13th April 2022
Date Policy to be reviewed:	13th April 2023
Written by:	ATU Corporate Governance and Data Protection PSC
Approved by:	Working Group 4
Approving Authority	Governing Body
Head of Function responsible	VPs for Finance and Corporate Services/ Secretary to the Governing Body
Reference Documents:	Risk Management Policies of IT Sligo, GMIT and LYIT

Document Location:

Website – Policies and Procedures	Yes
Website – Staff Hub	Yes
Website – Student Hub	No
Other: - Internal Use Only	No

This Policy was approved by the Governing Body on 19th February 2024. It shall be reviewed and, as necessary, amended by the University every two years. All amendments shall be recorded on the revision history section above.

Note: Prior to publication and dissemination of policies and procedures, documents must be reviewed for accessibility as part the University's commitment to Equality, Diversity, and Inclusion (EDI). Further advice on accessibility can be obtained from the EDI Team.

Contents

1. Setting the Context

1.1 Background and Context

The Governing Body, its committees, management and employees are committed to the identification and management of risks associated with the delivery of the University's strategic objectives and its responsibilities under the terms of THEA Code of Governance. The Technological Higher Education Institutions (THEIs) have also taken into account the guidelines set out in the following documents:

- ISO 31000 Risk Management Principles and Guidelines; and
- COSO Enterprise Risk Management Integrating with Strategy and Performance (2017).

The Governing Body has approved this risk management policy ('Policy') which sets out the following:

- A common process across the University to identify, analyse and assess risks;
- The process to facilitate the determination of strategies which mitigate or treat the identified risks;
- The process to ensure that risks and mitigating controls are documented in the Schools and Functions Risk Registers (Bottom Up view) and the University's Risk Register (Top Down view) with clear allocation of risk ownership;
- The process to ensure that an on-going risk monitoring and review process is established and embedded, including the regular maintenance and update of all risk registers across the University; and
- Details of the implementation of a robust risk appetite and incident and near miss reporting and management process supported by a formal escalation process.

As part of its oversight responsibilities, the University's Executive Board and the Audit and Risk Committee (A&RC) will keep under review the adequacy and effectiveness of the University's risk management process.

1.2 Scope/Applicability

This policy applies to the entire University including the Governing Body, its committees, schools, departments and functions both academic and support, and includes campus companies and research centres.
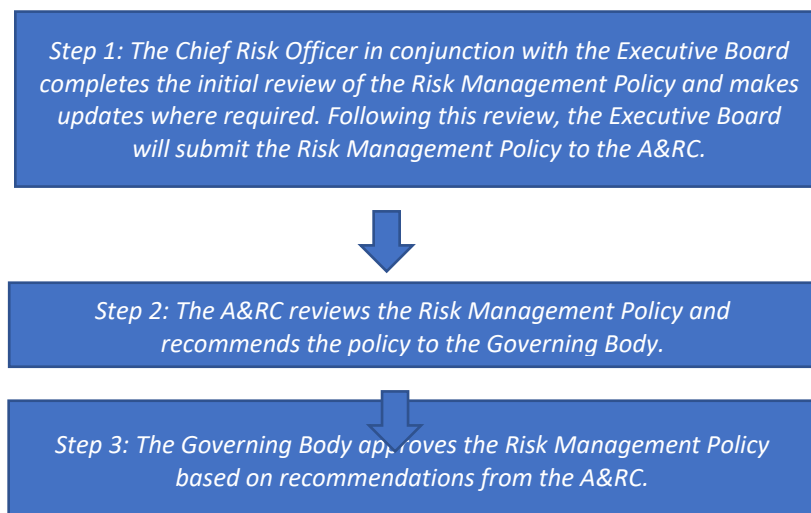
1.3 Implementation

The policy shall be communicated to and available to all employees. All employees are responsible for familiarising themselves with and adhering to the requirements of this policy assisted by an appropriate level of risk training and awareness. Compliance with policy is mandatory.

1.4 Policy Review

This policy is maintained by the Chief Risk Officer (CRO) and is reviewed, at least, on an annual basis, or more frequently, as required following significant change to the University, its business activities or to the external environment. The Chief Risk Officer will review the policy in conjunction with the Executive Board and make updates where required.

Following, the review of the policy by the Executive Board, the policy is submitted to the A&RC for review and challenge. The Governing Body is ultimately responsible for approving the policy.

> **Step 1:** The Chief Risk Officer in conjunction with the Executive Board completes the initial review of the Risk Management Policy and makes updates where required. Following this review, the Executive Board will submit the Risk Management Policy to the A&RC.

> **Step 2:** The A&RC reviews the Risk Management Policy and recommends the policy to the Governing Body.

> **Step 3:** The Governing Body approves the Risk Management Policy based on recommendations from the A&RC.

1.5   Mission and Risk Appetite

The strategic mission adopted in the application to become a technological university is that "Our TU will be known for building capacity and community in our region through excellent, flexible and innovative academic programmes, collaborative and experiential learning, advancing knowledge through research and engagement, provision of lifelong learning and undergraduate, postgraduate, remote and enterprise-based education."

The Atlantic TU Strategic Mission will be based on two overarching pillars:

- Our TU will provide excellent learning opportunities spanning multiple campuses and will contribute to sustainable development across our region and beyond
- We will aim to become a university of choice for learners and for collaborators within and beyond our region through the excellence and foresight demonstrated by our programmes, our student experience, our research and engagement and our international focus.

In pursuing its strategic objectives as set out in our TU application, the University is exposed to a broad range of risks.

The University seeks to ensure high standards of governance and risk management in all engagements with its broad-ranging stakeholder groups and in delivering its mandate in accordance with relevant legal and statutory obligations. Defining a risk appetite contributes to good governance and sound risk management practice which supports the Governing Body, and Executive Board in ensuring their decision-making is informed by risk considerations.

The University must accept an element of risk across its activities in order to work towards achieving its strategic objectives. The risk appetite statement articulates the level and nature of risk that the University is willing to accept to deliver on its strategic objectives. The risk appetite is formally documented through risk appetite statements linked to each key risk area identified for the University (see section 6), which is reviewed annually by the EMT, A&RC and is approved by the Governing Body.

Where Risk Appetite threshold levels are exceeded, they must be escalated. All risks which threaten the achievement of key strategic objectives will be reported to the Governing Body and necessary remedial action taken.

2. Purpose of the Risk Management Policy

2.1 Purpose of the Policy

The purpose of this policy is to provide a framework for management to identify, assess and rate strategic and business risks, and to detail actions required to deal with risks so as to provide reasonable assurance that the University's strategic objectives will be achieved. In effect, this policy will establish a framework to identify potential events that may expose the University to risk, to manage this risk, to keep it within the University's risk appetite and to provide reasonable assurance regarding the achievement of the University's strategic objectives.

2.2 Risk Management Objectives and Principles

The broad objectives of the Risk Management Policy are to:

- Ensure that sound risk management practices and procedures are embedded within the University, providing a consistent approach to risk management;

- Support the University in aligning to the THEA Code of Governance through the adoption of best practice in the identification, assessment and management of risks to support their elimination or reduction to a level acceptable to the Governing Body in the achievement of its objectives;

- To facilitate continuous improvement of the internal control environment and support better decision making through a good understanding of individual risks and the overall risk exposure that exists at a particular time;

- Develop a common understanding of risk across the University, thereby enabling the University to manage risk effectively on an University wide basis;

- Outline the risk related roles and responsibilities across the University;

- Ensure that risks (including new and emerging risks), to which the University is, or may become exposed to, are identified in a timely manner and manage those risks that may significantly affect the pursuit of the stated strategic goals and objectives;

- Ensure that a robust risk assessment is undertaken for all risks identified by the University;

- Ensure that effective risk mitigation strategies are adopted and applied by the University;

- Ensure that the University's risk profile is monitored and reported on an on-going basis; and

- Promote and embed a strong risk culture for the entire University.

The objectives of the Risk Management Policy will be fulfilled through the principles outlined below which have been adopted by the University for effective risk management:

- Documenting those activities required to be performed on an ongoing basis to support the risk management process;
- Establishing clear ownership of risks and mitigating controls;
- Operating in line with the approved Risk Appetite at all times;
- Establishing independent oversight through the Chief Risk Officer and Internal Audit of the risk management processes, to assess the effectiveness of those internal controls that mitigate documented risks; and
- Facilitate the promotion of a risk aware culture through training, which in turn bolsters effective risk management and ensures that risk-taking activities are identified, assessed, mitigated, monitored and reported in a timely manner.

2.3   Benefits of Risk Management

Risk management is not solely about managing risks, it is also about identifying and taking opportunities. Some of the benefits associated with risk management include:

- Transparent processes and embedding a consistent approach to managing risk;
- Support for management decisions;
- Support the achievement of strategic objectives;
- Safeguard staff, students and assets;
- Protect the University's reputation;
- Support financial sustainability
- Provision of competitive advantage by adapting to new circumstances;
- Improved accountability through clearly defined roles and responsibilities;
- Increased quality and efficiency in processes;
- Immediate risk prioritisation; and
- Positive attitude to implementing risk controls.

3.   Risk Management Framework

Risk management is the systematic application of management policies, procedures, and practices to identify, assess and manage risk effectively while reporting to the relevant stakeholders of the College. The Risk Management Framework of Atlantic TU is made up of the following:

- Risk Management Policy;
- Risk Appetite; and
- Risk Management Procedure

ALIGNING RISK MANAGEMENT WITH THE STRATEGIC FRAMEWORK   AND KPIs FRAMEWORK.

Risk management should not be viewed in isolation, but instead viewed as an activity that aids a University in the achievement of its strategic and operational goals. The TU sector must focus on the achievement of the predetermined KPIs, and risk management can provide insight and assurance into the achievement of these measures and objectives.

The process of identifying KPIs should be embedded in the strategic planning process of the University. The diagram below shows risk management is an integral, over-arching element of the Strategic Management Framework. The absence of effective and integrated risk management processes increases the likelihood of non-achievement of strategic objectives and adversely impacts the achievement of agreed KPI outcomes.

Risk management at an Executive Level (Strategic Risk Management) must be used in the context of meeting the strategic objectives of the University. The constant monitoring of risks and the effectiveness of strategies put in place to mitigate these risks, is a function of the Executive Board and should be viewed as an integrated function of executive management.

3.1   Strategic Risk versus Compliance Risk

The THEA Code of Governance places a strong emphasis on Internal Controls and Risk Management:
As outlined in the table below, there is a clear link between Compliance Risk Management (which is covered as part of the Internal Control Framework) and Strategic / Business Risk Management (which is set out in this policy).

The Atlantic TU internal control framework is informed based on the Technological University Act 2018, the THEA Code of Governance, legislation, national and international guidelines and Atlantic TU policies and procedures. The framework is designed to review the controls from the bottom up identifying areas of non-compliance and the associated risk exposure to the University.
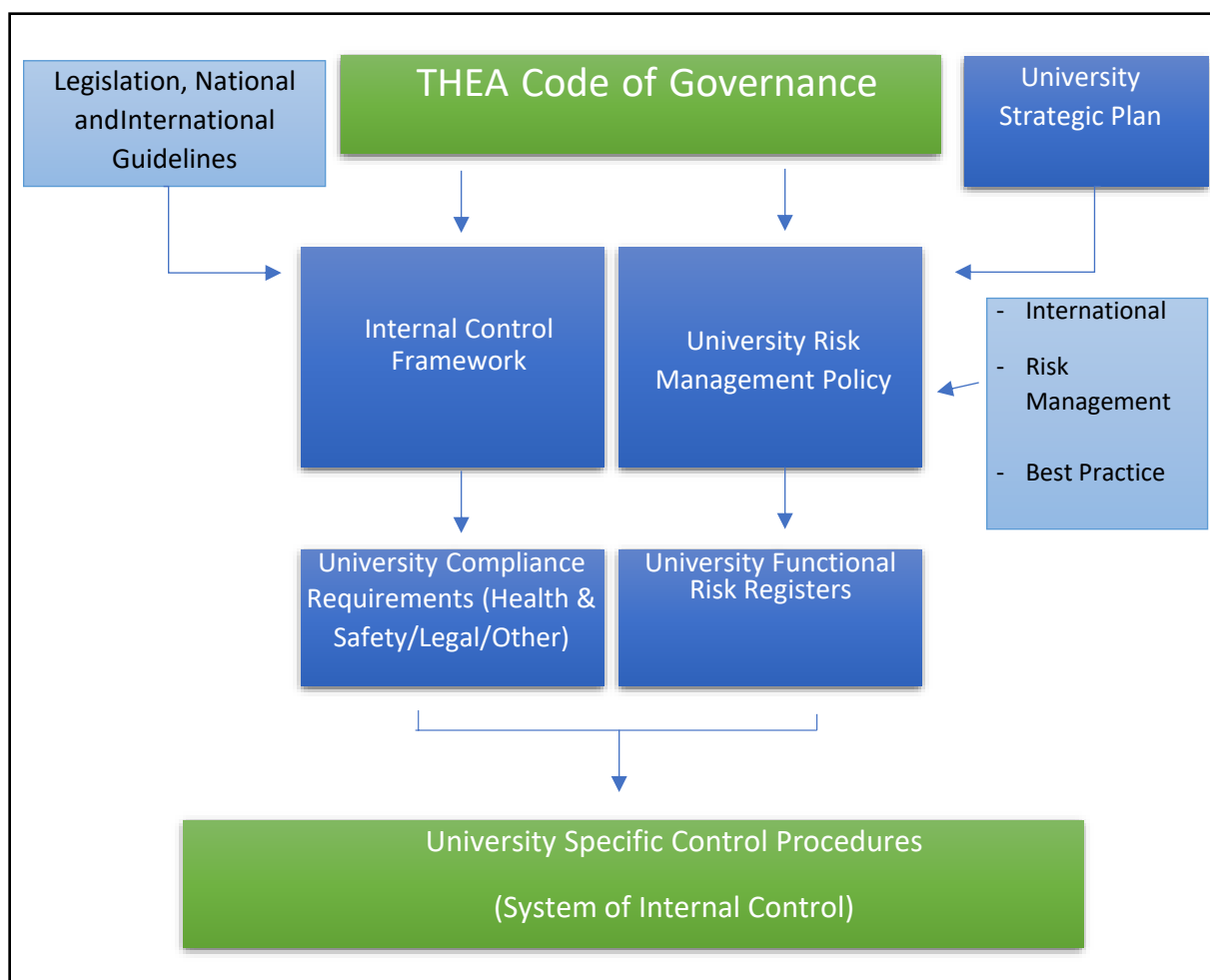
In parallel with this "compliance" agenda (including Health & Safety, Legal Compliance, Financial Control, Operational Controls), the University must look at strategic / business risks in a broader context and in particular in the context of the achievement of the University's Strategic Plan.

4.   Risk Governance – Roles & Responsibilities

The University has adopted the governance model below to support the continuous management, monitoring and oversight of risk.
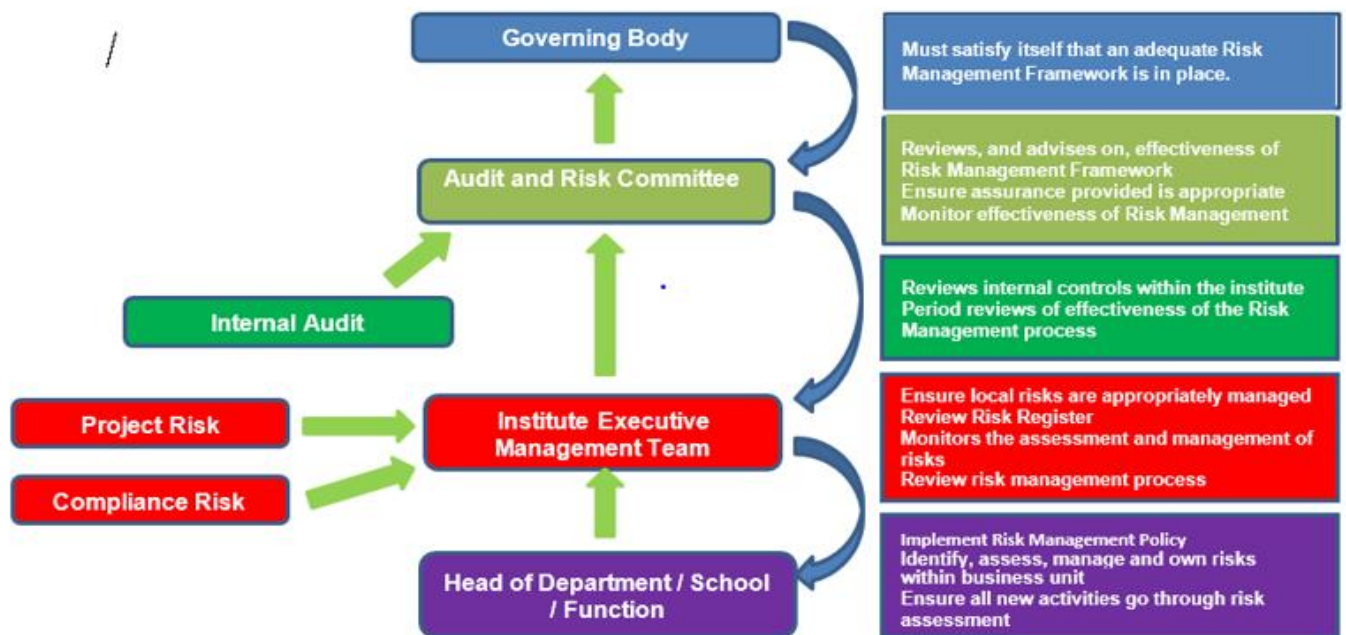
4.1 Governing Body

The Governing Body will:

- Have overall responsibility for the risk management framework within the University;
- Confirm in the annual report that the Governing Body has carried out an assessment of the University's principal risks, including a description of these risks, where appropriate, and associated mitigation measures or strategies;
- Review management reporting on risk management and note/approve actions as appropriate;
- Provide final approval of the University Risk Management Policy and any amendments thereto at least annually;
- Provide final approval of the University's Risk Register and any risk tolerances / risk management plans identified within at least annually;
- Approve the University's risk appetite and risk management plans (via approval of the Risk Management Policy) at least annually;
- Establish an Audit and Risk Committee to give an independent view in relation to risks and risk management systems;

- Make risk management a standing item on the Governing Body meeting agenda.

- Appoint a Chief Risk Officer or empower a suitable management alternative and provide for a direct reporting line to the Governing Body to identify, measure and manage risk and promote a risk management culture in the University;

- Require periodic external review of effectiveness of risk management framework; and

- Ensure there is appropriate risk management expertise in the in the competencies of at least one Governing Body member.   Where composition of the Governing Body does not allow for this, expert advice should be sought externally.

4.2   Audit and Risk Committee

The role of the audit and risk committee is to provide assurance to the Governing Body that an adequate Risk Management Framework is in place and is operating effectively in the University. In providing the required level of assurance, the A&RC will coordinate with the Governing Body in respect of its oversight of the University's risk management framework including:

- Review and challenge the University's Risk Management Policy and any amendments   thereto and recommend to the Governing Body for approval;

- Review and challenge of the University's Risk Register and recommend to the Governing Body for approval;

- Review and challenge of the University's Risk appetite (via approval of the Risk Management Policy) and recommend to the Governing Body for approval;

- Ensure ongoing review of the operation and effectiveness of the University's Risk Management process;

- Ensure that assurance provided by management and external / internal auditors is appropriate;

- Monitor the effectiveness of risk management in relation to risks identified as fundamental to the success or failure of the University's strategic objectives; and

- Report to the Governing Body in relation to the effectiveness of the risk management process on an annual basis.

4.3   The President

The President of the University has overall responsibility for ensuring that procedures and processes are in place to enable adherence to this Risk Management Policy. The President is also responsible for leading and promoting a risk management culture within the University.

4.4   Chief Risk Officer

The Governing Body should have a Chief Risk Officer in place to provide support to the delivery of Risk Management. The Governing Body has empowered the Chief Risk Officer to support the identification, assessment, oversight including monitoring and reporting of risk and promoting a risk management culture in the University. Additionally, the Chief Risk Officer will:

- Provide independent oversight and challenge of the assessment of risks captured in the Schools and Functions Risk Registers;
- Coordinate the development, review and implementation of the risk management policy;
- Facilitate the development and annual review of the University's risk appetite;
- Maintain the Risk Management Policy, Risk Appetite Statement and University's Risk Register;
- Coordinate the review and approval of the Risk Management Policy by EMT, A&RC and the Governing Body at least annually;
- Coordinate the review and approval of the Risk Appetite Statement and University's Risk Register by EMT, the A&RC and the Governing Body;
- Act as a support function to Management by providing assistance and guidance relating to the management of risk;
- Report on risk and its developments to the Executive Board and the A&RC concerning risk appetite, risk policy, the embedding of the policy, risk incidents and the risk profile across the Institution;
- Manage and monitoring of the risk incident and near miss reporting processes and performing trend analysis of all incidents reported;

- Support the embedding and understanding of the risk management policy at all levels in the Institution through the provision of an appropriate level of risk training and awareness; and
- Promote a risk aware culture;
- Recording and maintaining details of incidents or near misses across the University on an incident log. The log should capture the incident, lessons learnt and remedial action plans; and
- Consider trends in incident reporting and consider if there is the potential for similar incidents to also occur in other parts of the University and ensure any lessons learned are shared across the University.

4.5   University Executive Board

The University's Executive Board is responsible for:
- Ensuring Risk Management is an agenda item at Executive Board meetings;
- Implementing the University's Risk Management Policy and advocating a risk management culture;
- Identifying and monitoring risks;
- Ensuring that each risk has a person responsible for its management;
- Adequate risk management training and awareness is provided to all staff to assist with embedding a sound risk culture and effective risk management practices.
- Ensuring that controls identified are working, provide periodic positive assurance that they are working and/or report if they are not working;
- Ensuring that individuals understand what level of risk they are empowered to take on behalf of the University;
- Ensuring local risks are appropriately managed (through consideration of reports on local risk on a regular basis from Heads of Schools / Functions who are members of the Committee);
- Taking particular note of any risks identified locally that should be escalated to the University's Risk Register;
- Reviewing and updating the University's Risk Register at the end of each semester in light of reports on local risk analysis and other relevant matters, paying special

attention to new risks or risks whose rating has escalated since the time of the last review;

- Monitoring the assessment and management of risks that could impact on the achievement of the University's objectives;

- Report to the audit and risk committee once per semester in respect of the University's' Key performance indicators on risk and annually in respect of the University's Risk Register and the implementation of the Risk Management Framework; and

- Ensure alignment between risk management, the Strategic Management Framework, the Internal Control Framework and the KPI Framework.

4.6   Head of Faculty / Head of Function

Heads of Faculty / Functions are responsible for the following in relation to risk management:

- Implementation of University Risk Management Policy within their area of control and the development of a risk-aware culture;

- The identification, assessment, management and ownership of risk within their area of control;

- The establishment and regular review of the Faculty and Functions risk register in their area and its submission together with a report detailing the trajectory of any changes in the top 10 risks to the Chief Risk Officer within 30 days after the end of each semester. (Which for practical purposes these reporting deadlines are 31st January and 31st July). The identification of new and emerging risks that cannot be managed locally and the reporting of such risks to the Chief Risk Officer on a regular basis for consideration of inclusion on the University's Risk Register;

- Ensuring that all substantial projects for example research projects or new programmes undergo risk assessment and that such assessment is included in the project / programme proposal, and reporting on same to the University Executive Board; and

- Identify and respond to changes in both the internal and external environments which may pose a threat to the attainment of the strategic and / or operational goals of the University or their Function.

4.7   All staff/Employees

- Ensure they are aware and understand the risk management processes and embed them as part of their day to day roles.
- Correctly execute risk management procedures and controls.
- Being aware of the nature of risks in their day to day work.
- Proactively identify risks and promptly escalate any incidents, exceptions, concerns and/or control issues to management.
- Being involved on training and upskilling in risk management where offered.

4.8   Internal Audit

- Providing independent and objective assurance to the A&RC on the robustness and effectiveness of the risk management policy and the adequacy and appropriateness of internal controls.
- Internal Audit is responsible for the review of internal controls within the University. In developing its Annual Internal Audit Plan, in consultation with the A&RC and the President, cognisance will be taken of the University's Risk Register.
- The internal audit reviews of University activities/ departments/ functions/ units will include a periodic assessment of the effectiveness of their respective risk management processes and will report to the Governing Body, through the A&RC, on how those risks are being managed.

5.   Principal Risk Categories (Risk Taxonomy)

Risks are categorised in four pillars, in line with the THEA Risk Management Policy. These are as follows:

Strategic: The inability to achieve the University's strategic goals or objectives as set out in the Strategic Plan and risk of not availing of opportunities when they arise.

Financial: The exposure of losses arising as a result of the need to improve the management of the University's financial assets.

Operational: The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

Compliance: The risk of legal sanctions, material financial loss, or reputational loss the organization may suffer as a result of its failure to comply with laws, its own regulations, code of conduct, and standards of best / good practice.

Atlantic TU have decided not to articulate Reputational risk as a standalone risk category as it is seen as a potential impact or consequence resulting from any of the other key risk categories materialising.

6.   Risk Management Process

The University recognises that risk management is a continuous and developing process, which runs throughout the University's strategy, and affects the implementation of that strategy.

The University's risk management process aims to ensure that all risks, including significant risks, to which the University is exposed, are identified and understood. Appropriate internal controls will be implemented to protect the University and to ensure that significant risks are mitigated adequately.

The University's Risk Management Framework provides assurance from academic and administrative functions to the Executive Board and, through the team, to the A&RC and Governing Body.

Effective risk management focuses on understanding and measuring risk and control rather than necessarily avoiding or totally eliminating it.

This Risk Management Process is outlined within Atlantic TU Risk Management Procedural document.

| 1. Identify | 2. Assess | 3. Mitigate | 4. Monitor and Report |

7.   Risk Appetite

The purpose of the University's Risk Appetite process is to specify the types of risk and associated thresholds, which the University is willing to accept in pursuing its strategic objectives and ensure their monitoring and oversight. It sets out broadly 'acceptable' levels of exposure for each of the University's material risks.

The Risk Appetite Statement forms part of the University's broader risk management approach and policy. The risk management policy comprises a range of measures for identifying and assessing risk, implementing and monitoring the adequacy of control measures, managing incidents and Near Misses, and reporting the status of risk, control and remedial actions to the University's EMT, A&RC and the Governing Body. Risk Appetite is considered as part of and informs the University's business planning processes and strategic objective setting.

The risk management policy sets out the risk management roles and responsibilities including responsibilities in relation to risk appetite.

8.   Operational Incident and Near Miss Management

While the risk identification and assessment process focuses on potential adverse consequences, incident reporting captures details of individual incidents that have occurred.

An **operational risk** incident is any unexpected outcome within the University which is a consequence of inadequate or failed internal processes, people or systems, or which has arisen as the result of an external event. Examples include internal / external fraud, payment errors, data protection issues / breaches, health & safety issues and process failures.

A **near miss** is an undesired event or sequence of events with potential to cause serious disruption or harm to the University but is avoided.

Accurate collection of incidents and near miss data can have many benefits for the University as it:

- Provides a rich stream of intelligence for strengthening the relevant processes;
- Raises awareness of underlying causes of incidents ('root cause'), thus influencing behaviour and controls designed to prevent re-occurrence;
- Helps identifying trends and focus efforts and resources on key issues; and
- Informs the development and review of the divisional risk registers.

Appendix 1 - Risk Impact Guidance Table

	Insignificant / Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Financial	1% of Budget or <€50k	2.5% of Budget or <€200k	7.5% of Budget or <€2M	15% of Budget or <€10m	25% of Budget or >€10m
Business Process and Systems	Minor errors in systems or processing requiring corrective action, or minor delays Email disruption - 15 minutes delay	Minor procedural rules occasionally not complied with and subsequently identified and corrected Email disruption – 1 hour	One key accountability requirement not complied with or bypassed Email disruption – 3 hours	Non-compliance with several key control requirements Email disruption – full Day	Ongoing non-compliance with key legal, regulatory and governance obligations Email disruption – several days
Health, Safety & Welfare	Injuries or ailments not requiring treatment.	Minor injury or first aid treatment case.	Serious injury causing hospitalisation or multi pre-medical treatment cases.	Life threatening injury or multiple of serious injuries causing hospitalisation.	Death or multiple of life-threatening injuries.
Reputational	Internal review requires minimal senior management time to correct	Scrutiny required by internal committees or internal audit to prevent escalation. requires senior Management time to address	Scrutiny undertaken by external committees or External Auditor, requires significant senior Management time to correct	Intense public political and media scrutiny, e.g. front page, headlines, tv, etc requires significant senior management intervention	Judicial review, commission of inquiry or ongoing adverse national media. requires significant board and senior management intervention
Interdependencies	Minor disputes with other bodies and agencies	Minor disputes with other bodies and agencies requiring senior management time to rectify	Limited co-operation by key stakeholders / agencies on priorities areas	Lack co-operation by key stakeholders / agencies on some priority areas	Serious noncollaboration by Stakeholders working contrary to MOUs MOAs SLAs

Appendix 2 - Risk Register

The following template shall be used for both the University Risk Register and the Faculties and Functions Risk Registers to capture and rate risks identified.

Risk Id	Risk Description	Risk Causes	Risk Impact	Strategic / Business Objective	Risk Category	Risk Owner	Existing Controls Description	Impact	Likelihood	Risk Rating	Change in rating from previous review	Action Plan Description	Action Plan Owner	Action Plan Due Date	Action Plan Status (Open / Closed)
								1	3	3					
								2	5	10					
								5	5	25					