Enterprise Risk Management Policy

Contents

1. Introduction

The University recognises the importance of adopting a proactive approach to risk management to support both the achievement of its strategic objectives and compliance with good governance requirements.

The University is committed to ensuring that risk management is seen as everybody's responsibility, embedded in the regular day-to-day business, informs the strategic and operational planning and performance cycle. Enterprise Risk Management (ERM) promotes a comprehensive framework for making risk-based decisions that support achieving our strategic goals. At preset these focus on education, research, internationalisation, and supporting our broader community in the Midwest region. As we develop and revise our Strategic Plan, these goals and risk emphases may also change. ERM enables better management of uncertainty and of associated risks and opportunities. In particular, it guides the University to address risks comprehensively and coherently instead of trying to manage them individually or in isolation.

1.1. Purpose of UL Enterprise Risk Management Policy

The purpose of this policy is to:

Confirm the University's commitment to putting in place a modern, proactive system of risk management, consistent with our vision, mission, values, and goals, using public resources and best meeting our corporate governance responsibilities.

It is designed to:
- Assist our staff in understanding their role and the need to adopt a consistent approach to the assessment and management of risk.
- Set out the systems and processes required to ensure that risks are managed consistently across the University.
- Set out the systems and processes for risk reporting.
- Contribute to bringing about a culture where open communication is encouraged to identify and mitigate potential risks before they occur.

This policy supports this purpose by:

1. Establishing a framework for the University's management to identify and assess risks while developing strategies, procedures, and controls to address them.
2. Providing reasonable assurance by identifying and managing potential events that may expose the University to risk in achieving its strategic objectives.
3. Managing risk as set out in the Risk Appetite Statement.

This policy is a part of the University's governance arrangements. The policy sets out the following:

— Definitions.
— Risk Appetite.
— Risk Management Framework:
  – Key principles.
  – Roles and responsibilities.
  – Risk Management Process.

Effective risk management involves identifying and mitigating potential risks, which helps us identify and capitalise on opportunities. This approach enables us to proactively manage uncertainties while maximising the potential for success in all fields of our activities – academic, administrative, and support.

Some of the benefits associated with risk management include:

- Improve our resilience in the face of threats to achieving what matters to our University and its staff.
- Achieve and demonstrate good corporate governance.
- Comply with legal and regulatory requirements.
- Transparent processes and good practice.
- Risk-aware staff and risk-aware culture
- Support for management decisions.
- Structured and swift response to emerging and evolving risks.
- Improved public accountability and transparency.
- Increased quality and efficiency in processes.
- Immediate risk prioritisation and
- Positive attitude to implementing risk controls.

1.1   Scope

1.2.1 To whom does the Policy apply?

This Policy applies throughout the University. Our subsidiary companies are required to provide for and maintain a comparable risk management system.

The Governing Authority has a statutory obligation to provide for and maintain a risk management system within the University as part of an effective internal controls system.

Section 5 below details the various individuals/committees responsible for implementing and monitoring this Policy. In addition, the Risk Management Officer (RMO) is responsible for ensuring that processes and procedures are in place to enable the implementation of this policy. A risk management handbook has also been prepared to support the RMO and those with particular responsibility for managing risk, which deals with core principles in significantly more detail.

1.2.2 Definitions

Risk	is the effect of uncertainty on objectives. In the context of the University and its activities (and those of its subsidiaries / joint ventures), risk is any condition, circumstance, potential event, or threat that may impact upon the achievement of objectives and/ or significantly impact day-to-day operations. Note that an effect may be positive, negative, or a deviation from the expected. This also includes failing to avail of any opportunity to help the University meet its objectives.
Controls	are measures that contain and/or modify risk. To be effective, a control must be in place, be tangible, working effectively and operating to reduce the likelihood or impact of a risk. Controls include any process, policy, device, practice, or other conditions that are in place and contain and/or modify risk.
Actions	are future measures that contain and/or modify a risk, reducing its likelihood or impact (or both). Once completed, actions become controls.
Risk Treatment	describes a process of modifying risk. This may include implementing effective controls and taking additional actions at the University.
Inherent risk	the risk level before control and/ or action measures are in place.
Residual risk	the risk level remaining after considering existing controls.
Target Risk	is the planned level after considering controls and action measures. This level aligns with the University's risk appetite.
Risk appetite	is the amount and type of risk the University is willing to accept to achieve its strategic objectives. It influences the University's operating style.
Risk tolerance	refers to the University's readiness to bear the residual risk to achieve its objectives. It is the level of deviation from risk appetite that we are prepared to tolerate in a given situation.

2. Context

2.1 Legal and Regulatory Context

The focus on governance in corporate and public bodies continues to increase. In developing this Enterprise Risk Management Policy, account has been taken of the following statutory and regulatory instruments:

- ✓ 1997 Universities Act (as amended by the Higher Education Authority Act 2022)
- ✓ Joint Higher Education Authority & IUA (Irish Universities Association) report on the governance of Irish Universities 2007.
- ✓ Code of Practice for the Governance of State Bodies (State Code) 2016
- ✓ ISO 31000 (2018) Risk Management Principles and Guidelines.
- ✓ ISO 31050 Guidance for Managing Emerging Risks to Manage Resilience (2023)

The State Code provides the Governance of

"It is the responsibility of the Governing Authority to ensure that a robust risk management system is in place in the University."

Per the Code, a risk management system involves:

- Establishing an Audit and/or Risk Management Committee to provide an independent view of risks and risk management systems.
- Making risk management a standing item on the Governing Authority (GA) and relevant subcommittee meeting agendas.
- Advising the relevant chancellor of the need to include risk management experience/expertise in the competencies of at least one Governing Authority member. Where the composition of the Governing Authority does not allow for this, expert advice should be sought externally.
- Identifying risks that threaten the achievement of the University's objectives.
- The evaluation of the likelihood of occurrence and potential impact of the risks identified.
- The segregation of risks according to their gravity.
- An appraisal of the techniques employed to manage the major risks and to identify any further steps that should be taken.
- An appraisal of residual risk levels – after applying mitigation techniques and whether the residual risk is acceptable.
- Continuous monitoring of the effectiveness of controls and management techniques and decision-making informed by the risk management process.

3. Policy Statements

The University is committed to the proactive management of risk on an enterprise-wide basis, including all risks related to its academic mission or management processes. This involves identifying risks that threaten the core objectives of the University, as set out in the Universities Act 1997 and in its Strategic Plan. Effective risk management helps the University anticipate and mitigate potential threats, ensuring operational stability and resilience in uncertainty. It safeguards our reputation, strengthens the control environment, and helps us comply with our legal and regulatory obligations and the requirements of the Code of Practice for the Governance of State Bodies. The University adopts the risk management principles set out in the ISO 3100 (2018) Standard and actively works towards complying with these principles to ensure effective risk management and will abide by these principles.

3.1. Principles for Risk Management

The key purpose of the Enterprise Risk Management Policy is to detail a system of risk management that can assist the University in effectively identifying, assessing, measuring,monitoring, reporting, and managing risks arising within the University as it seeks to achieve its strategic objectives. This is done using the International Standard ISO 31000 principles of Risk Management and the requirements as outlined in the Higher Education Authority Act 2022, as incorporated into the Risk Management Framework currently in place in the University.

In addition to that, regard should be had to the following core principles:

(a) Governance – The University must have a proactive management-led approach to risk management as part of its governance framework;

(b) Structures – Managing risk requires a systematic, timely and structured approach with clearly defined risk management structure, process and responsibilities

(c) Management – The system of risk management should be appropriate to the scale,
nature and range of activities and risk appetite of the University and should be subject to continuous improvement.

(d) Reporting – the University's risk management systems must be subject to monitoring and reporting at various key levels of management (e.g., Department, Faculty, Division, etc.)

4. Related Procedures for Enterprise Risk Management

4.1. Roles and Responsibilities

The management of risk is the responsibility of all staff.

Governing Authority	The Governing Authority (GA) is accountable to the Higher Education Authority (HEA) and the Department of Further and Higher Education, Research, Innovation and Science (DFHERIS) for the funding provided to it. As described in the State Code, the Governing Authority fulfils key functions regarding the University, including providing for and maintaining a risk management system.
Audit and Risk Committee and other Governing Authority Committees	The GA Audit and Risk Committee (ARC) is responsible for providing oversight and advice to the Governing Authority concerning the operation of the University's risk Enterprise Risk Management Policy. As assigned by the Governing Authority and in consultation with the ARC, other GA Committees provide oversight of specific risks relevant to their area(s) of responsibility.
The President and Executive Committee	The Executive Committee (EC), led by the President, is responsible for executive decision-making in the University. This includes implementing and ensuring compliance with the University's Enterprise Risk Management Policy.

Corporate Secretary	As part of their functions, the Corporate Secretary (CS) performs the function of the Chief Risk Officer and, in this capacity, provides a direct reporting line to the GA and the ARC. The Chief Risk Officer oversees the identification, assessment and mitigation of risks to ensure the University's stability, support compliance, and promote a risk-aware culture throughout the University.
Risk Management Officer	The Risk Management Officer (RMO) reports directly to the Corporate Secretary and supports the identification, assessment, and oversight, including monitoring and reporting risk and promoting a risk management culture in the University. Additionally, under the direction of the CS, the RMO will: — Provide independent oversight and challenge of assessing risks captured on the Risk Registers. — Coordinate developing, reviewing, and implementing the Enterprise Risk Management Policy. — Facilitate the development and annual review of the University's risk appetite. — Maintain the Enterprise Risk Management Policy, risk appetite statement, and University risk register. — Coordinate the review and approval of the Risk Management Policy and Appetite Statement by the Executive Committee, ARC and the Governing Authority at the required intervals, as set out in Codes or in policy. — Act as a support function to Management by providing assistance and guidance relating to risk management. — Report on risk and its developments to the Executive Committee and the ARC, including risk appetite, risk policy, the embedding of the policy, risk incidents, and the risk profile across the Institution. — Manage and monitor the risk incident and near-miss reporting processes, performing trend analysis of all incidents reported. — Provide an appropriate level of risk training and awareness to support the embedding and understanding the Enterprise Risk Management Policy at all University levels. — Promote a risk-aware culture. — Consider trends in incident reporting, consider whether similar incidents could occur in other parts of the University, and ensure any lessons learned are shared across the University.

University Risk Review Group	The University's Risk Review Group (ULRRG) aims to enhance the execution of campus strategic and operational risk management and provide comprehensive risk reporting supporting the University's Strategic Plan. The group also ensures a consistent approach to project delivery and helps manage associated operational risks. Additionally, it serves as a point of contact for operational risks with University-wide implications and assists the Executive Committee in overseeing organisational risks. The composition of the URRG is occasionally agreed upon by the EC.
Faculty/ Division with Management Responsibilities	All employees and Academic staff with management responsibilities are responsible for: — Implementing and ensuring compliance with the University's Enterprise Risk Management Policy in their area of responsibility. — Ensuring that appropriate and effective risk management processes are in place within their assigned areas of responsibility. — Risk assessing all strategies, business plans/service developments, including changes to service delivery. — Developing specific objectives within their service or operational plans that identify future risks. — Ensuring that a process of risk identification is in place throughout all areas of responsibility and that risk assessments are conducted in accordance with this policy. — Maintaining a risk register and formally reporting on risk to the next management level. — Ensuring that all staff identify risks within their working environment and are aware of their personal responsibilities in accordance with this Policy.
Staff	All staff are required to: — Comply with this Policy in the identification and management of risk. — Understand that risk management is integral to their academic / research /managerial practice within the University. — Have knowledge of the related risk management procedures that support this, Policy. — Identify and report any potential risks to their Line Manager. — Complete risk management training appropriate to their role. Whereas every staff member is responsible for identifying and managing risk within the context of their work, certain common roles and responsibilities in the University level govern communication, notification, and escalation of identified risks, controls, and actions.

Fig 1. Overview of Risk Management at the University of Limerick

4.2. Risk Management Process

Categorisation by Risk Impact
This policy requires that identified risks be categorised and assessed in relation to the primary area upon which they impact.

Categories by Risk Impact

Impact Category	1 Minor	2 Moderate	3 Serious	4 Extreme

Impact Assessment Criteria at a Faculty & Division

	1 Minor	2 Moderate	3 Serious	4 Extreme
Constituent Strategy 1) Research & Innovation 2) Teaching & Learning 3) International 4) Student Experience 5) Engagement	Some delay with implementing a strategic objective or initiative	Significant delay with implementing a strategic objective or initiative	Failure to deliver on one or more of the strategic objectives or initiatives	Failure to deliver one or more of the missions critical activities and/or strategic objectives
Operational 1) Physical Infrastructure 2) Unit Effectiveness 3) Health & Safety***	Short term disruption to a critical activity	Short term significant disruption to critical activities	On-going & significant disruption to critical activities	Complete shutdown of critical activities for an extended period
Financial	Up to €300k	€300k to €750k	€750k to €1.5m	Above €1.5m
Reputational	Some negative comments in local press / media	Critical article in local media or criticism from within UL Senior Management	Continuing & significant publicity in local or national media regarding the UL management	Unit loses confidence of the public and / or UL Management

Impact Assessment Criteria at a University level

	1 Minor	2 Moderate	3 Serious	4 Extreme
Constituent Strategy 1) Research & Innovation 2) Teaching & Learning 3) International 4) Student Experience 5) Engagement	Some delay with achieving more than 1 of the constituent strategies or significant delay with a single constituent strategy	Significant delay with achieving more than 1 constituent strategy	Failure to deliver on one or more of the following constituent strategies: - International - Student Experience - Engagement	Failure to deliver on one or more of the following mission critical strategies: - Teaching & Learning - Research & Innovation
Operational 1) Physical Infrastructure 2) Unit Effectiveness 3) Health & Safety***	Short term disruption to a critical University activity	Short term & significant disruption to critical University activities	On-going & significant disruption to critical University activities	Complete shutdown of university activities for an extended period
Financial	Up to €2m	€2m – €5m	€5m – €10m	Above €10m
Reputational	Adverse & widely reported media coverage regarding the University	Widely reported (but unproven) allegations of serious misconduct	Widely reported & proven mismanagement with Government review	Widely reported & proven mismanagement with Government sanction against the University &/or loss of public confidence

*** Due regard is to be given to the Occupational Health & Safety Hazard and Risk Assessment

Fig 2. Risk Impact Table at a Faculty/Division level and University level (Fundamental Risk Register)

4.3. Risk Appetite

What is a Risk Appetite and a Risk Appetite Statement?

Risk appetite is the level of risk the University is willing to accept to achieve its strategic objectives. For example, the University may determine that it has a low-risk tolerance concerning compliance risk but may be willing to accept a level of risk concerning financial risk. The Governing Authority sets the University's risk appetite, articulated through the Risk Appetite Statement.

This statement defines the risk appetite and tolerance for specific risk areas. The University may choose to be either risk-taking or risk-averse, and its willingness to accept various levels of risk will vary depending on the type of risk.

The University has a higher appetite for risk in encouraging and promoting critical enquiry, academic freedom, research and innovation, international development, freedom of expression, and open debate. The University has a very low appetite for risk where there is a likelihood of significant and lasting reputational damage; significant and

lasting damage to its provision of world-class research or teaching; significant financial loss or significant negative variations to financial plans; loss of life or harm to students, staff, collaborators, partners or visitors, illegal or unethical activity, and regulatory compliance. No endeavours that expose the University's reputation to unacceptable risk should be undertaken.

The University defines risk tolerance as the deviation from the risk appetite that it is prepared to tolerate. Depending on the nature of the risks, tolerance levels will typically be temporary and should have an associated reduction plan.

The University's approach to risk management is generally cautious. It prefers safe options where the expected level of benefit is limited. While the University must accept that it cannot manage all risks, it is willing to accept well-managed risk-taking in certain circumstances.
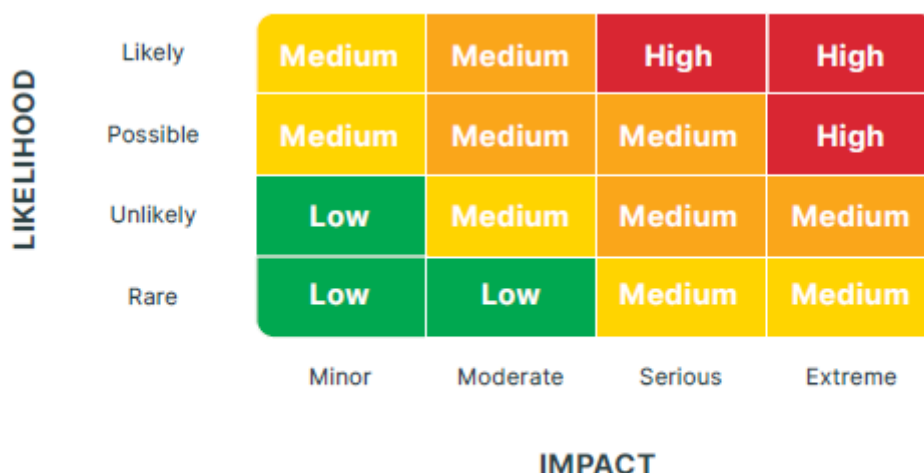
LIKELIHOOD	Minor	Moderate	Serious	Extreme
Likely	Medium	Medium	High	High
Possible	Medium	Medium	Medium	High
Unlikely	Low	Medium	Medium	Medium
Rare	Low	Low	Medium	Medium

IMPACT

Figure 3: University Risk Rating Matrix

How to use Risk Appetite?
Decision makers and risk owners across the University should use the University's risk appetite statement to guide them to areas where they have more freedom to innovate and where greater caution is expected.

Risks outside of appetite must be addressed to bring them back within tolerance and to the desired target level of risk appetite. There can be circumstances where a risk, when rated, is outside of the University's risk appetite or tolerance, where defined, or when a risk continues to have a high residual risk rating above the target risk rating.
This may be acceptable for a defined period, but provided that this is agreed upon by the relevant risk-owner/accountable person or within the existing governance structures (e.g., Executive Committee).

However, the rationale for the decision and the decision itself should be clearly documented and retained for audit purposes. There also needs to be a plan with definitive timelines identified within which the decision will be reviewed.

The Risk Appetite Statement should always be used in conjunction with the Risk Process outlined below.
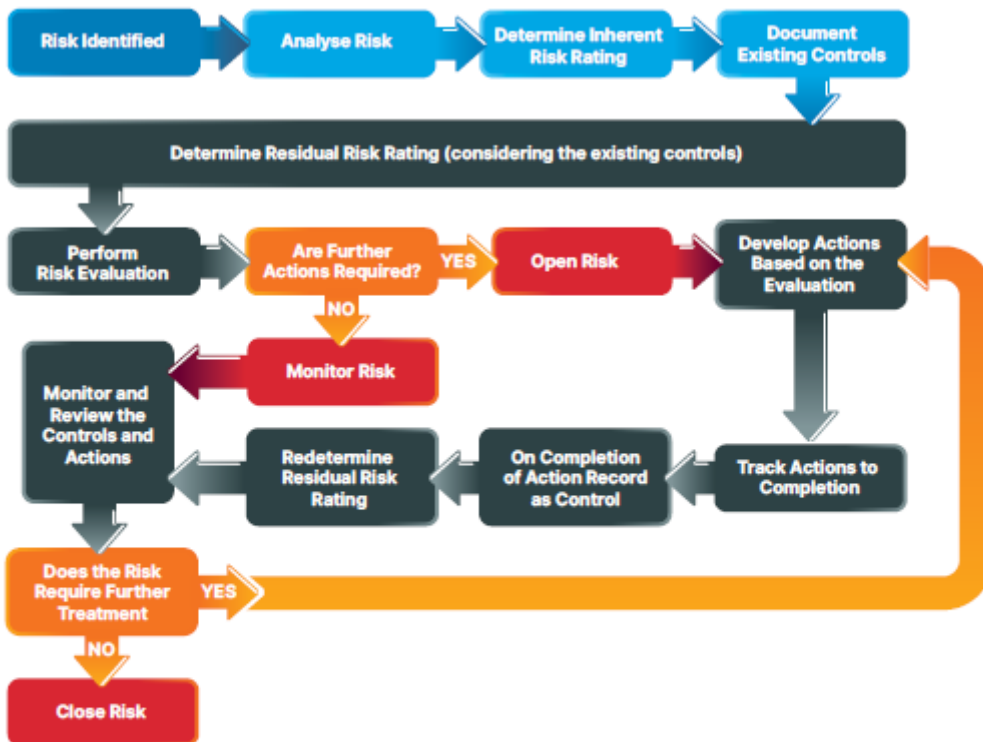

Figure 4: Risk Management Cycle

4.4. Risk Management Cycle

To demonstrate the cycle, please see below for an example of a risk using the cycle described on the previous page.

Step	Details
1. Risk Identified	**The risk of a fire in a laboratory.**
2. Analyse Risk	**Potential Causes:** Flammable chemicals, electrical faults, equipment overheating, human error.
	Potential Consequences: injury or loss of life, damage to property, loss of research data, and interruption of research.
3. Inherent Risk Rating	Likelihood: 3
	Impact: 4
	Inherent Risk Rating: 12 (High)
4. Document Existing Controls	Fire alarms and smoke detectors
	Fire extinguishers
	Fire suppression systems (e.g., sprinklers)
	Safety training for all lab personnel
	Proper storage of flammable substances
	Regular inspections and maintenance of electrical equipment
	Emergency evacuation plans
5. Residual Risk Rating	Likelihood: 2
	Impact: 3
	Residual Risk Rating: 6 (Medium)
6. Performance Risk Evaluation	**Effectiveness of Controls:** Regularly tested and effective
	Incident History: No recent incidents
	Compliance with Regulations: Full compliance

Step	Details
7. Are Further Actions Required?	**No:** The risk is currently managed effectively with existing controls.
8. Monitor and Review	**Regular Monitoring:** Continue regular inspections, maintenance, and safety drills.
	Review Frequency: Quarterly reviews and after any near-miss or incident.
9. Does the Risk Require Further Treatment?	**No:** Existing controls are sufficient to manage the risk effectively.
Conclusion	**Close Risk:** The risk of fire in the laboratory is effectively controlled.
If Yes to Further Actions Required	**Example Scenario:** An incident reveals that current chemical storage protocols are insufficient.
	Develop Actions: Improve protocols, provide additional training, and update safety data sheets.
Track Actions to Completion	Assign responsible personnel, set deadlines, and monitor progress until completion.
Record as Control	Document new controls and integrate them into the lab's safety procedures.
Redetermine Residual Risk Rating	Likelihood: 1
	Impact: 2
	New Residual Risk Rating: 1 x 2 = 2 (Low)
Monitor and Review	**Continuous Monitoring:** Ensure new controls are functioning as intended.
	Regular Reviews: More frequent initially, then revert to standard frequency.
Does the Risk Require Further Treatment?	**No:** If new measures are effective, the risk can be closed.
	Yes: If further issues are identified, continue developing actions based on evaluation.

4.5. Management of Risk

Once risks have been identified, recorded, analysed, and agreed on treatments implemented, managers need to ensure a process for reviewing risk profiles and activities in their area of responsibility. An appropriate monitoring and reporting regime should be established to track how effective the treatment is in controlling the risk.

Risk management should become an agenda item on management meetings or committees wherever possible rather than a separate process. Regular reviews aim to identify new risks and monitor existing ones to ensure that controls are still effective and appropriate and that actions are completed as required. How frequently a review process and reporting cycle occurs will depend on the residual risk rating versus what the target risk rating has been set to achieve. However, it is suggested that this should not be less than quarterly.

In addition, risk assessments should be reviewed if the service/organisation changes, such as when new resources or procedures are introduced that would impact the risk. Changes made to the risk assessment should be brought to the attention of relevant staff and others.

This continual review aids in the ongoing assurance that risks are being identified and managed. Such assurances are seen as part of the University's lines of defence.
The putting in place of tangible mitigations and controls is crucial within the risk management system because they provide concrete measures to prevent, minimise, or eliminate potential threats. This ensures operational/organisational stability, whereas vague or poorly defined controls or mitigations are ineffective.

4.6. Risk Management as Three Lines Model

The Governing Authority
- Holds and ensures statutory accountability for oversight of the University.
- Agrees with the overall risk management strategy and ensures alignment with strategy and organisational goals.
- Nurtures a culture which promotes ethical behaviour and accountability.
- Ensure structures and processes for governance are in place, including supporting committees as required.
- Delegates or assigns responsibility in a manner that supports the Chief Officer and senior management in achieving the objectives of the University.
- Decides upon the University's appetite for risk regarding the opportunities that come with the assumption of such risk and exercises oversight of risk management.
- Maintains oversight of compliance with legal, regulatory, and ethical expectations.

Management First line roles – Executive Committee
- Leads and directs actions (including managing risk) and the application of resources to achieve the University's objectives.
- Maintains a continuous dialogue with the Governing Authority and reports on planned, actual, and expected outcomes linked to the University's objectives and risk.
- Establishes and maintains appropriate structures and processes for managing operations and risk.
- Ensures compliance with legal, regulatory, and ethical expectations.

Second-line roles – Risk Management Function
- Provides complementary expertise, support, monitoring, and challenges related to the management of risk, including:
- Supports the development, implementation, and continuous improvement of risk management practices at a process, systems, and entity level.
- Supports the achievement of risk management objectives, such as: compliance with laws, regulations, and acceptable ethical behaviour; internal control; information and technology security; sustainability; and quality assurance.
- Provides analysis and reports on the adequacy and effectiveness of risk management.

Third-line roles - Internal Audit
- Maintains primary accountability to the Governing Authority and is independent from management responsibilities.
- Communicates independent and objective assurance and advice to management and the Governing Authority on the adequacy and effectiveness of governance and risk management to support the achievement of University objectives and to promote and facilitate continuous improvement.
- Reports impairments to independence and objectivity to the Governing Authority and implements safeguards as required.

External Assurance Providers
Provide additional assurance to:
- Satisfy legislative and regulatory expectations that protect stakeholders' interests.
- Satisfy requests by management and the Governing Authority to complement internal sources of assurance.
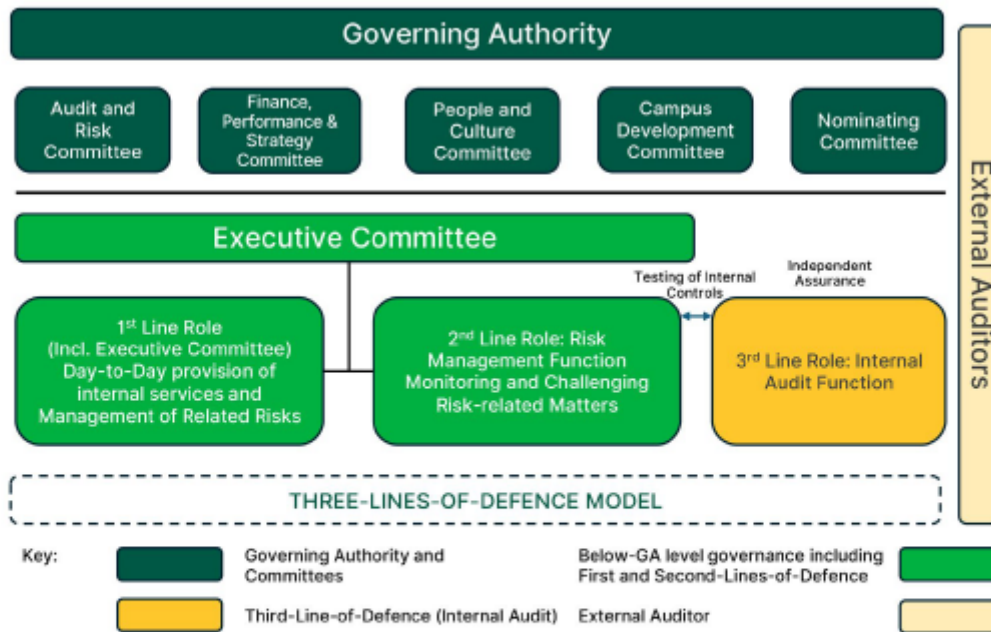
Figure 5: Three Lines of Defence Model, System of Internal Control

5. Policy Statement

The University is committed to the proactive management of risk on an enterprise-wide basis, including all risks related to its academic mission or management processes. This involves identifying risks that threaten the core objectives of the University, as set out in the Universities Act 1997 and in its Strategic Plan.

Effective risk management helps the University to anticipate and mitigate potential threats, ensuring operational stability and resilience in the face of uncertainty. It safeguards our reputation, strengthens the control environment, and helps us comply with our legal and regulatory obligations and the requirements of the Code of Practice for the Governance of State Bodies. The University adopts the risk management principles set out in the ISO 3100 (2018) Standard. It actively works towards complying with these principles to ensure effective risk management and that they will abide by them.

6. Document Control

Document Version	Version 1.0
Document Owner	Corporate Secretary Office
Approved by	Executive Committee
Date	26 June 2024
Approved by	Audit and Risk Committee
Date	6 September 2024
Approved by	Governing Authority
Date	29 October 2024
Effective Date:	29 October 2024
Scheduled Review Date:	29 October 2024