UNIVERSITY of LIMERICK

OLLSCOIL LUIMNIGH

RISK MANAGEMENT POLICY

Approved by Governing Authority February 2016

1. BACKGROUND

1.1 The focus on governance in corporate and public bodies continues to increase. It resulted in an expansion from the Code of Practice for the Governance of State Bodies originally issued in 1992 by the Department of Finance to that updated and reissued in 2001. A further update in 2009 was issued to increase accountability and transparency in the manner in which these bodies operate. This 2009 Code, while covering much of the same areas as the previous 2001 Code, updated requirements, responsibilities and accountabilities in certain areas such as internal audit, audit and risk management.

1.2 Given their pivotal position in society and in national economic and social development together with their reliance on public as well as private funding, good governance is particularly important in the case of universities. The principle of good governance in Irish universities is well established. It was enshrined initially in the Universities Act, 1997 and subsequently detailed in the 2001 Framework: "*The Financial Governance of Irish Universities"*. Subsequently, the universities adopted the HEA/IUA "Governance of Irish Universities", its principles and its reporting requirements, implementing it with effect from 2007. Since then, compliance reports have been submitted on an annual basis to the HEA as required by the Code. The 2007 Code was updated in 2012 to bring it into line with the Code of Practice for State Bodies. The Code states that:

> *"Good governance arrangements are essential for organisations large and small and whether operating in the public or private sectors. Governance comprises the systems and procedures under which organisations are directed and controlled. A robust system of governance is vital in order to enable organisations to operate effectively and to discharge their responsibilities as regards transparency and accountability to those they serve. Given their pivotal role in society and in national economic and social development, together with their heavy reliance on public as well as private funding, good governance is particularly important in the case of the universities.*

1.2.1 The 2012 Code and the subsequent UL Code of Governance places a strong emphasis on Internal Control and Risk Management and stipulates that:

- A system of internal control has a key role in the management of risks that are significant to the fulfilment of institutional objectives. A sound system of internal control contributes to safeguarding the interests of all relevant parties and the university's assets. Internal control facilitates the effectiveness and efficiency of operations; helps ensure the reliability of internal and external reporting and assists compliance with laws and regulations.

- Effective financial controls, including clear delineation and separation of functions and the maintenance of proper accounting records, are an important element of internal control. They help ensure that the

university is not unnecessarily exposed to avoidable financial risks and that financial information used and published is reliable. They also contribute to the safeguarding of assets, including the prevention and detection of fraud.

- A university's objectives, its internal organisation and the environment in which it operates are continually evolving and, as a result, the risks it faces are continually changing. A sound system of internal control therefore depends on a thorough and regular evaluation of the nature and extent of the risks to which the university is exposed.

- A sound system of internal control reduces, but cannot eliminate, the possibility of poor judgement in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

- A sound system of internal control therefore provides reasonable, but not absolute, assurance that the university will not be hindered in achieving its objectives, or in the orderly and legitimate conduct of its business, by circumstances which may reasonably be foreseen. A system of internal control cannot provide protection with certainty against failing to meet objectives or prevent all material failures, errors, losses, fraud, or breaches of laws or regulations.

- Systematic assessment and management of risk is becoming an increasingly important part of internal control. Risk identification and management is seen as necessary to maximise the likelihood of achieving an institution's desired objectives and outcomes.

- It is the responsibility of the governing authority to ensure that a robust system of internal control and risk management is in place in the University.

- The governing authority should ensure that the risk assessment and management process is integrated into existing management systems. It should be kept as simple as possible. Roles and responsibilities should be clearly assigned and a person at a senior level with overall responsibility for it should be nominated who ensures a direct reporting line to the Governing Authority. Risk Management expertise should be included in the membership of the Audit & Risk Management Committee also.

2. PURPOSE OF UL RISK MANAGEMENT POLICY

2.1 The purpose of this Policy is to provide a framework for management to identify, assess and rate risks, and to develop strategies 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 objectives.

2.2 The Policy sets out the following:

- Definitions;
- Roles and responsibilities;
- Risk Management Framework
  - Risk Identification and Assessment;
  - Risk Monitoring and Reporting;
  - Risk Appetite;
  - Management of Risk.

2.3 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 good practice;
- Support for management decisions;
- Provision of competitive advantage by adapting to new circumstances;
- Improved public accountability;
- Increased quality and efficiency in processes;
- Immediate risk prioritisation;
- Positive attitude to implementing risk controls.

3. DEFINITIONS

3.1 Risk: Risk may be defined as the University not benefiting from opportunities available, suffering damage or disadvantage, or not achieving its objectives due to an internal or external event. Risks, by their very nature, may or may not occur and fall into a variety of categories, some of the most common being:

- *Strategic Risks*: the inability to achieve the University's strategic and operational objectives as set out in the Strategic Plan and also, not availing of opportunities when they arise;
- *Operational Risks*: the inability to prevent a loss resulting from inadequate internal processes and systems;
- *Financial Risks*: exposure to losses arising as a result of inadequate controls or the need to improve the management of the University's financial assets;
- *Reputational Risks*: exposure to losses arising as a result of bad press, negative public image and the need to improve stakeholder relationship management.

In addition, risks can exist at different levels:

- Corporate or Strategic Level (Fundamental)
- Faculty/Division level;
- Project level.

3.2 Risk Identification: The process of determining what can happen, why and how.

3.3 Risk Analysis: The systematic use of available information to determine the likelihood of specific events occurring and the magnitude of their consequences/impact on the University.

3.4 Risk Assessment: Risks are assessed and prioritised on the combined basis of their likelihood of occurrence and the resulting impact should they materialise.

3.5 Risk Register: A risk register is a risk recording and monitoring tool for the management of the University. It is a hierarchical entity and a review of the Fundamental Risk Register (corporate or strategic level risks) will be informed by local risk registers (Faculty/Division and project level risks) put in place by Faculties and Administrative Units.

3.6 Risk Appetite: Risk appetite is the amount of risk an organisation is prepared to accept based on the expected return of the development/activity in question. The University can be risk-taking or risk-adverse and different levels of risk appetite can apply to different activities. In deciding its risk appetite the University will decide the threshold beyond which risks move from being monitored to being serious, or finally to the abandonment of the particular activity. Clarity in relation to the University's risk appetite is critical to enable Executive Committee decide on the how best to manage any particular risk.

4. ROLES & RESPONSIBILITIES

4.1 Governing Authority

4.1.1 Overall responsibility for the management of risk within the University lies with the Governing Authority. The Governing Authority will approve the University's Risk Management Policy and will satisfy itself, through its Audit & Risk Management Committee, that the Policy is effective, that an adequate Risk Management Framework is in place in the University and that Fundamental Risks are being managed appropriately by the University Executive. In addition, the Governing Authority, through its Audit & Risk Management Committee, shall require an external review of the effectiveness of the University's Risk Management Framework and its governance on a periodic basis.

4.2 Audit & Risk Management Committee

4.2.1 The role of the Audit & Risk Management Committee is to assure Governing Authority that an adequate Risk Management Framework is in place in the University. In providing the required level of assurance, the Audit & Risk Management Committee will:

- Review the University's Risk Management Policy and make recommendations to Governing Authority for amendments to the Policy as required;
- Keep under review, and advise on, the operation and effectiveness of the University's Risk Management Framework;
- 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;
- Ensure that Risk Management is a standing agenda item at its meetings and report to the Governing Authority on its findings in relation to fundamental risk management and the adequacy of the Risk Management Framework on an annual basis;
- Require an external review of the effectiveness of the risk management framework and its governance on a periodic basis.

4.3 Risk Management Function

4.3.1 The Corporate Secretary of the University has overall responsibility for ensuring that procedures and processes are in place to enable adherence to this Risk Management Policy. Additionally, the Corporate Secretary will:

- Ensure the provision of adequate training and awareness to Risk Register Owners;
- Ensure the communication of the key elements of the University's Risk Management Framework;
- Maintain the University's Fundamental Risk Register, including its review and up-date on an annual basis;

4.4 University Executive Committee

4.4.1 The University's Executive Committee is responsible for:

- Implementing the University's Risk Management Policy;
- Identifying and monitoring Fundamental Risks that could impact on the achievement of the University's strategic objectives and the issuing of reports to the Audit & Risk Management Committee where a new Fundamental level risk arises or where there are significant changes in circumstance surrounding an existing one;
- Undertaking a formal review of the Fundamental Risk Register on an annual basis in light of input arising from formal reviews of local Risk Registers;
- Ensuring that each fundamental risk has a 'Risk Owner' responsible for its management;
- Ensuring that individuals understand what level of risk they are empowered to take on behalf of the University;
- Ensuring local level risks are appropriately managed through on-going review of local Risk Registers and the issuing of reports by members of the

Executive where a new local level risk arises or there are significant changes in circumstance to existing ones;

- Consideration of reports arising from the formal review of local risk registers on an annual basis from Vice Presidents/Deans/Heads of Administrative Units who are members of the Committee;
- Taking particular note of risks identified in local risk registers that should be escalated to the Fundamental Risk Register;
- Encouraging a risk management culture throughout the University so that risk is embedded as part of the University's decision making and operation;
- Critically reviewing the effectiveness of risk management processes;
- Report to the Audit & Risk Management Committee on an annual basis on the University's Fundamental Risk Register and the implementation of the Risk Management Framework.

4.5 Vice Presidents/Deans/Heads of Administrative Units

4.5.1 Vice Presidents/Deans/Heads of Administrative Units are responsible for the following in relation to risk management:

- Implementation of University Policy in relation to Risk Management within their area of control;
- The identification, assessment, management and ownership of risk within their area of control;
- The establishment and regular review of a Local Risk Register in their area and, where the Head of the Administrative Unit is not a member of the Executive Committee, its transmission to their line manager who is a member annually or as required through escalation provisions set out in the Guide to Risk Management in Appendix 1;
- Vice Presidents/Deans/Heads of Administrative Units who are members of the Executive Committee will report annually to the Committee on local risk registers within their areas of control;
- The identification of new and emerging risks that cannot be managed locally and the reporting of such risks to the Executive Committee as required for escalation to the Fundamental Risk Register;
- Ensuring that all substantial projects or new programmes undergo risk assessment and that such assessment is included in the project/ programme proposal, and reporting on same to the Executive Committee;
- Supporting the embedding of risk management in their area and the development of a risk-aware culture.

4.6 Internal Audit

4.6.1 Internal Audit is responsible for the review of internal controls within the University. In developing its Annual Internal Audit Plan, in consultation with the Audit & Risk Management Committee and the President, cognisance will be taken of the University's Fundamental Risk Register and local risk registers. The internal audit reviews of University functions/units will include an assessment of the effectiveness of their respective risk management processes and will provide independent assurance to the Governing Authority,

through its Audit & Risk Management Committee, that risks are being managed appropriately.

5. RISK MANAGEMENT FRAMEWORK

5.1 The Risk Management Framework is an iterative process consisting of steps when taken in sequence, enable continual improvement in decision making. It constitutes a logical and systematic method of identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable the University to minimise losses and maximise opportunities. The University of Limerick Risk Management Framework provides assurance from academic and administrative functions to the senior management team and, through the team, to the Audit & Risk Management Committee and Governing Authority. Effective risk management focuses on understanding and measuring risk rather than necessarily avoiding or totally eliminating it and comprises the following components:

5.2 Risk Identification: The purpose of risk identification is to produce a list of the potential risks that could impact on the University achieving its objectives. Risks will be identified (commonly under four pre-defined categories as set out in Section 3.1) and prioritised using a variety of techniques such as interviews, workshops, Faculty/Divisional/Functional area meetings etc.

A formal risk identification and review exercise will be undertaken on an annual basis in order to update both the Fundamental Risk Register and local risk registers. Faculties/Divisions and other functional areas as appropriate will be assisted in this regard by the Corporate Secretary's Office through the Risk Management Officer.

5.3 Risk Assessment: The size of any risk can be measured using two dimensions, the effect on the University should the risk materialise (impact) and the probability of the event occurring (likelihood). To ensure consistency of application across the University, risks identified must be assessed and measured in accordance with inherent and residual risk criteria as shown in the table below:

Assessment	Inherent	Residual
Impact	The extent of impact on the University's operations if the risk arises in the *absence* of current controls.	The extent of impact on the University's operations if the risk arises in the *presence* of current controls.
Likelihood	The probability of the risk arising in the *absence* of current controls.	The probability of the risk arising in the *presence* of current controls.

5.3.1 Appropriate quantification of risk is critical to an effective Risk Management Framework. Not all risks are equal and effective risk management is only possible if risks are prioritised appropriately. Generally, risks should be

prioritised according to their ability to affect the University achieving its objectives and therefore may change as objectives change. Certain risks will be deemed to be Fundamental Risks and will be recognised as being of greater strategic or operational importance to the University than Non-Fundamental Risk. This approach enables risk management resources to be targeted to the most important areas whilst still recognising less important risks.

The method of assessment of risk is set out in the "Guide to Risk Management" attached as Appendix 1 to this Policy.

5.4 **Risk Monitoring and Reporting**: The following monitoring and reporting requirements will apply:

5.4.1 Each Vice President/Dean/Head of Division will develop a 'local' risk register which should be subject to on-going review. This on-going review will also enable updating the risk register in the following situations: :

- within one month of any internal audit report where a recommendation from the Internal Auditors graded as 'fundamental' is recorded;
- following major changes to the structure, funding or strategic direction of the Faculty/Division the relevant Vice President/Dean/Head of Division will ensure this is reflected in the local risk register
- following a specific request by the Executive Committee:
- Will undertake a formal review of their local Risk Register annually , notwithstanding the above conditions.

Following the completion of a formal review of their local risk register or in the event of any fundamental/exceptional item arising, the Vice Presidents/Deans/Head of Division will prepare a report using the standard risk and control template and risk register template attached as Appendix 2 to this Policy. The report will be submitted to the Executive Committee for consideration and discussion on anannual basis or immediately depending on the level of the risk as set out in the "Guide to Risk Management" (Appendix 1).

5.4.2 The Executive Committee will consider reports on local risk registers following completion of their annual review. The Executive Committee will consider on-going developments within the University and any emerging risks as required. Based on such consideration, the Executive Committee will review the University's Fundamental Risk Register and amend the Register as required. Where deemed necessary by the Chairman of the Executive Committee, the emergence of new risks may be considered immediately by the Executive Committee. The Executive Committee will submit a report to the Governing Authority Audit & Risk Management Committee on the Fundamental Risk Register and the effectiveness of the Risk Management Framework annually.

5.4.3 The Audit & Risk Management Committee will report at least annually to the Governing Authority on the management of the Fundamental Risk Register and the implementation of the University's Risk Management Framework.

5.5 **Risk Appetite:** The University's risk appetite defines how it accepts and manages risk. Risk elements arising from proposed or actual developments/activities within the University may fall into three categories:

(i) Risks that are trivial and therefore acceptable and do not need to be managed;

(ii) Risks that are acceptable and routinely arise in certain types of activity that will need to be managed;

(iii) Risks that are unacceptable and therefore the development/activity should not proceed.

The concept of risk appetite applies to major developments/activities and is concerned with the placing of a boundary between (ii) and (iii) above. It therefore reflects the University's tolerance of risk.

5.5.1 A major development/activity may be defined as having a value in excess of €500,000 which may pose a significant reputational risk to the University. Any such proposed development/activity and associated risks when identified must be reported to the Executive Committee for consideration immediately they arise. This process must be followed also where there is any doubt whether or not a risk associated with any development/activity might be deemed acceptable to the University.

5.6 **Management of Risk:** Upon completion of a risk assessment and taking account of the University's risk appetite, the University may decide to:

- treat the risk (e.g. use of internal controls);
- terminate the risk;
- tolerate the risk (accept the risk with or without monitoring), or
- transfer the risk (e.g. by using insurance, sub-contracting).

6. REVIEW OF POLICY

6.1 This policy will be reviewed periodically to ensure adherence to best practice thereby continuing to enhance the decision-making and operation of the University.