

Risk Management Policy



Policy owner Chief Risk Officer **Approval date and body** UMT, January 17th 2024

1. Purpose

The purpose of this policy is to affirm the University's commitment to providing a framework that allows for the identification, assessment, management, monitoring and reporting of risk.

The management of risk by the University is necessary in order to –

- Support the strategic objectives of the University
- Achieve operational objectives
- Protect the University community
- Ensure financial sustainability
- To comply with the requirements of the HEA Code of Governance for Irish Universities.

Detailed risk management provisions, guidance documents, templates and training materials are to be found in the documents referred to below and at www.ucd.ie/riskmanagement

2. Definitions

- **Risk:** The potential effects of uncertain influences on the achievement of objectives. Risk / Uncertainty can have a negative or a positive impact on the University's objectives. By managing / minimising / exploiting uncertainty the University can achieve its strategic and operational objectives and enhance sustainability. Risks can be financial, strategic, reputational, compliance related, etc.
- **Risk Management:** How the University manages risk / uncertainty.
- **Risk Management Framework:** The totality of the University's integrated risk management measures.
- **Risk Category:** A high level description of the various categories of risks that can arise within University operations, for example Reputational or Financial Risks.
- **Risk Appetite:** The level of risk or uncertainty that the University is willing to accept in the pursuit of its strategic objectives. It is descriptive in nature, e.g. having a Low Risk Appetite. Different

categories of risks will have a different risk appetite associated with them. For example the University has a very low tolerance for risks that impact on financial sustainability; whilst the University's acceptance of risks associated with internationalisation projects is higher. Refer to the University's [Risk Appetite Framework](#) for further information.

- **Risk Appetite** and **Risk Category** can be linked together in a descriptive way, for example by stating that the University has a Low Risk Appetite for Financial Risks; or a Moderate to High Risk Appetite for Strategic Initiative Risks.
- **Risk Score:** The numerical score applied to a risk using a combination of **likelihood** (the chance of an event occurring) and **impact** (the outcome of the event).
- **Risk Tolerance** is the maximum level of risk that the University is comfortable accepting for a particular **Risk Category** expressed as a number.
- **Risk Appetite, Risk Category** and **Risk Tolerance** can be linked, for example the University has a Low Risk Appetite for Financial Risks with a Risk Tolerance Score of 15.
- **Risk Treatment / Risk Mitigation** measures are actions designed to reduce a risks score by addressing at least one of two variables that make up that score (likelihood and impact).
- **Risk Rating** is a descriptive term (Red, Amber or Green) used to describe a risk based on its **Risk Score** and the associated **Risk Tolerance**.
- **Risk Velocity** is the 'time to impact' for a particular risk once it begins to emerge or develop and is descriptive in nature, e.g. risks that are considered to have a 'Fast Velocity' are those that can emerge over a matter of weeks with very limited early warning.
- **Inherent & Residual Risk** Risks are assessed on an inherent (i.e. considering current risk mitigation measures) and residual (i.e. considering any additional mitigation measures that could be put in place) basis. Therefore there are two risk scores for any one risk on a Risk Register.
- **Risk Register:** A repository for details of risks, risk control measures, risk ratings and other information related to risk management.
- **Risk Owners and Action Owners:** All identified risks are assigned a Risk Owner and an Action Owner, with the former ultimately accountable for the risk and the latter responsible for ensuring ongoing management of each risk. At a strategic and organisational level Risk Owners are members of the UMT; at a local level within a School or a Unit or a Project the Risk Owner is the relevant Head of School or Unit or Project Manager. Action Owners are those persons tasked by the Risk Owner with ensuring that the control measures identified are implemented.

3. Scope

This policy applies to all Colleges, Schools, Research Institutions and Units within the University and across all areas of operations. The entirety of the organisations activities are subject to this policy.

It also applies to the operations of the University's wholly owned subsidiary companies.

4. Principles

4.1 Risk Management Principles

UCD's Risk Management Framework is designed to assist the University in identifying, measuring, monitoring, reporting and managing risks as the University works toward achieving its strategic objectives.

To this end the University is guided by the principles of risk management as laid down in *International Standard ISO:31000 Risk Management Guidelines*. In summary these are –

- Risk management is an integral part of activities
- The approach to risk management is structured, comprehensive, dynamic and mindful of organisational culture
- Processes are proportionate and aligned with the degree of risk
- Stakeholders are consulted and involved in risk management
- Decisions are made using the best available data
- There is a commitment to continuous improvement

4.2 The UCD Risk Management Process

The risk management process at UCD comprises four main steps:

- Risk Identification
- Risk Assessment and Evaluation
- Implementation of Control Measures
- Monitoring and Control

Further detailed information on the Risk Management Process can be found in the [UCD Risk Management Handbook](#)

4.3 The Three Lines of Defence Model of Risk Management

UCD operates a 'Three Lines of Defence' model of risk management. Within the University the 'Three Lines of Defence' are identified as:

- **Line 1** – The Unit that owns the risk. In UCD there are layers of risk owners, starting at Unit / School / Project Level and moving upward via College / UMT Function level to the Enterprise Level Risk which is owned by the UMT.
- **Line 2** – The second line of defence are those specialist functions that provide oversight and / or guidance around risk management. These include the Risk Management Office, but also other key specialist functions such as UCD Legal, UCD Quality Office, UCD Safety, UCD HR, etc.
- **Line 3** – Those who provide independent oversight of the risk management framework, namely the Audit and Risk Management Committee (on behalf of the Governing Authority) and Internal Audit.

For further details on the Three lines of Defence Model refer to the [UCD Risk Management Handbook](#)

4.4 Risk Management Reporting

The Chief Risk Officer will provide updates on the effectiveness of the University's Risk Management Framework to the University Management Team at least once per semester; to the Governing Authority at least twice per year; and will at the discretion of the Committee Chair attend and report to all meetings of the Audit and Risk Management Committee.

5. Roles and responsibilities

- **Governing Authority** - The Governing Authority has ultimate responsibility for risk and internal control within the University.

- **Audit and Risk Management Committee** - A subcommittee of the Governing Authority which advises the latter on risk management issues and on the strategic processes for risk management in UCD.
- **President and the University Management Team** - The President and the UMT are responsible for the executive management of risk at a strategic and organisational level. The President and UMT maintain an Enterprise Level Risk Register setting out the most important risks for the institution as a whole. The President and UMT have primary responsibility for the identification and management of these risks. Each of the risks identified has a Risk Owner who is a member of the UMT.
- **College Principals:** Primary responsibility for the management of risk within a College and its constituent schools lies with the College Principal. Through the College Executive Committee, the College Principal will ensure that risks are managed and reported effectively. A Risk Register(s) will be maintained for the College setting out the important risks. Each of the risks identified is assigned a Risk Owner who is a member of the College Executive Committee and an Action Owner who possesses the relevant knowledge/expertise to manage the risk on an ongoing basis. The risk registers in place at the College level will align as appropriate with the high-level risks identified in the UMT Enterprise Level Risk Register(s). At the discretion of the College Principal a single Risk Register can be maintained across the College or multiple School / Research Unit risk registers can be maintained. The Risk Management Office can advise on this.
- **Vice Presidents / Directors of Support Units (UMT Level):** Primary responsibility for the management of risk within a UMT members' portfolio lies with the relevant UMT member. Working with their Senior Executive Team, the UMT member will ensure that risks are managed and reported effectively. A Risk Register(s) will be maintained for the UMT members portfolio setting out the important risks. Each of the risks identified is assigned a Risk Owner who is a member of the Senior Executive Team and an Action Owner who possess the relevant knowledge/expertise to manage the risk on an ongoing basis. The Risk Registers in place at the UMT member level will align as appropriate with the high-level risks identified in the UMT Enterprise Level Risk Register(s). At the discretion of the UMT member a single Risk Register can be maintained across the portfolio or multiple Unit risk registers can be maintained. The Risk Management Office can advise on this.
- **Heads of Schools / Unit Heads / Project Managers:** Day to day responsibility for the management of risk within a School or Unit or Project rests with the Head of School / Head of Unit / Project Manager. Such persons should ensure that they liaise with their UMT Manager on a regular basis

and provide information necessary for the development of their Project / School / UMT Function Risk Register. Such persons are encouraged to promote a culture of risk management at a local level by developing Project / School / Unit level Risk Registers and ensuring that staff have access to risk management training. Assistance on this can be obtained from the Risk Office.

- **All Faculty and Staff Members:** All faculty and staff have a critical role to play in risk management. Employees of the University are expected to effectively manage risk within their own areas of responsibility and report risks having wider potential impact or requiring broader coordination and response to their line manager.
- **Risk Management Office:** Led by the Chief Risk Officer, the Risk Management Office is responsible for overseeing the implementation of the University's Risk Management Framework and providing advice, guidance and training to cohorts of person across the University.
- **Risk Management Advisory Committee:** The University's Risk Management Advisory Committee (RMAC) is the University's management level risk committee and is a key part of the organisations Three Lines of Defence Risk Management Framework. At a high level its function is to guide and oversee the implementation of the University's Risk Management Framework via the Chief Risk Officer, in particular the processes that support the identification, assessment, management and reporting of risk. The RMAC **Terms of Reference** can be found at www.ucd.ie/riskmanagement

6. Related documents

All of the follow resources can be accessed at www.ucd.ie/riskmanagement

- Risk Management Handbook
- Risk Appetite Framework
- Risk Register Templates
- Risk Management Guidance Materials
- Online Training

7. Version history

Rev. 0 – Approved January 17th 2024