

Code: QA301

Title: **Risk Management Policy**

Date: November 2023

Policy Owner: Chair of the Risk Management Group

Approval: RMG, ARC and Údarás na hOllscoile

1. **Introduction**

|  |
| --- |
| **“Risk management and internal control are important and integral parts of a performance management system and crucial to the achievement of outcomes. They consist of an ongoing process designed to identify and address significant risks involved in achieving a university’s outcomes.”**  *Code of Governance for Irish Universities 2019* |

Risk involves uncertainty. It raises issues of probability and potential impact: the probability (likelihood) of the occurrence of events, circumstances or developments, and the potential impact (consequence) of these events, circumstances or developments to interfere in or affect a university’s ability to achieve its goals and objectives.

In summary, effective risk management helps the University achieve its strategic and operational objectives by managing and mitigating the risks, which have the potential to affect the achievement of those objectives.

The importance of risk management has been emphasised in publications such as the Department of Public Expenditure and Reform’s *Risk Management Guidance for Government Departments and Offices* (February 2016) and the *Code of Governance for Irish Universities* (September 2019). These two documents in particular contain guidance on the objectives, structures, processes and tools that should be used to effectively manage organisational risks. These documents are also supplemented by a wealth of best practice publications and reports, which have emerged in recent years.

This document describes the risk management framework in operation within the University of Galway, which is designed to support the ongoing monitoring, review and management of risks and was developed in line with best practice guidelines.

Over many years, the University has operated an internal control environment that has successfully managed risk, and has had in place insurance arrangements to mitigate against the impact of specific key exposures. The University operates a comprehensive set of processes for the identification, evaluation and management of significant risks.

**Supporting documents**

The following documents supplement the risk policy and provide additional guidance to staff and those responsible for the risk management process.

* **Risk Management Procedure –** This provides an overview of the process to follow in relation to risk management and the creation of risk registers.
* **Blank risk register template**

These documents are located on the Risk Management section of the President’s Office website ([www.universityofgalway.ie/riskmanagement](http://www.universityofgalway.ie/riskmanagement)) and will be updated in line with best practice and reviewed annually in line with the risk policy review.

1. **Risk Management**
   1. **Code of Governance for Irish Universities September 2019 (“The Code”)**

In relation to risk management, the Code states: “It is the responsibility of the Governing Authority to ensure that a robust system of risk management is in place in the University”. Per the Code, a risk management system involves:

* establishing an Audit and/or Risk Management Committee to give an independent view in relation to risks and risk management systems;
* making risk management a standing item on the Governing Authority and relevant subcommittee meeting agendas;
* advising the relevant Minister of the need to include risk management experience/expertise in the competencies of at least one governing authority member. Where composition of the Governing Authority does not allow for this, expert advice should be sought externally;
* the identification of 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 the levels of residual risk – after the application of 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.
  1. **Purpose of the University of Galway’s Risk Management Policy**

|  |
| --- |
| **“Risk management can be defined as a set of coordinated activities to direct and control the management of risk within a Department.”**  *DPER Risk Management Guidance February 2016* |

The purpose of this policy is to provide a framework for University management to identify, assess and rate risks, and to develop strategies, procedures and controls 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 support the identification of potential events that may expose the University to risk, to manage this risk against the University’s risk appetite and to provide reasonable assurance regarding the achievement of the University’s objectives.

This policy forms part of the University’s internal control and governance arrangements. The policy sets out the following:

* Definitions;
* Risk Appetite;
* Risk Management Framework:
  + Key principles;
  + Roles and responsibilities;
  + Risk management process;
  + Risk management cycle; and
  + Management of risk.
* Review of the Policy

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:

* Achieve and demonstrate good corporate governance;
* Comply with legal and regulatory requirements;
* Transparent processes and good practice;
* Risk-aware staff;
* Support for management decisions;
* Structured and swift response to emerging and evolving risks;
* Improved public accountability;
* Increased quality and efficiency in processes;
* Immediate risk prioritisation; and
* Positive attitude to implementing risk controls.
  1. **Risk Management Policy Objective**

The University of Galway is committed to establishing and maintaining a robust risk management framework that supports the ongoing management of risk in accordance with the established risk appetite and the University Strategy 2020-25.

The objective of this policy is to ensure the University is equipped to monitor and manage its key risks in line with best practice. Specifically, this framework has been developed to ensure:

1. That a practical process for the formal management of risks is established and that the process is maintained on an ongoing basis.
2. The risk framework addresses the requirements of best practice and the Code of Governance for Irish Universities 2019.
3. **Definitions**

**Risk:** Organisations face internal and external factors and influences that make it uncertain whether and when the extent to which they will achieve or exceed their objectives. The effect that this uncertainty has on the organisation’s objectives is “risk”[[1]](#footnote-2).

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: risks that may be external to the organisation such as the economic and political climate that impact on 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: relating to the procedures/technologies etc. employed to achieve particular objectives.
* Financial risks: relating to the procedures/systems/accounting records in place to ensure that the University is not exposed to avoidable financial risks, including risks to assets, funding and treasury.
* Reputation risks: involving risks to the public reputation of the organisation and their effects.
* Compliance risks: relating to compliance with regulations, legislation, circulars and best practice guidance.

**Risk Identification:** The process of identifying risks, potential and actual, that threaten the achievement of the University’s objectives.

**Risk Assessment:** The review of available information, using particular methods, to determine the likelihood and impact of identified risks.

**Risk Register:** This is the means by which identified and agreed risks are recorded and the register is used to maintain and manage risks going forward.

**Risk Appetite:** Risk appetite is the degree to which the organisation is willing to accept risk.

1. **Risk Appetite**

As noted above, the risk appetite is the tolerance level for risk. The University can be risk-taking or risk-averse and may be willing to accept different levels of risk depending on the risk type. For example, an organisation may have zero risk tolerance with regard to compliance risk but may be willing to accept a level of risk with regard to financial risk. A risk appetite statement is established outlining the appropriate levels of risk to be taken throughout the University and must be approved by Údarás.

The University’s general approach is to limit its exposure to risk across all risk categories. However, there is an appetite to accept a higher degree of risk in pursuit of its key strategic objectives. The University follows a conservative approach to risks, except for areas such as Strategy, Research and Innovation, Teaching and Learning, and International Development, where a higher risk appetite is acceptable, subject to ensuring an understanding of the potential benefits and risks, in pursuit of key strategic objectives.

As per **Appendix 1**, a conservative approach is taken to risks with a residual rating of 12 and above, i.e., high to extreme. Any emerging risks of this nature should be brought to the attention of UMT immediately.

The University’s appetite for risk across a number of categories is outlined at **Appendix 2**.

1. **Risk Management Framework**
   1. **Key Principles**

The following key principles outline the University’s approach to risk management and internal control:

* Údarás na hOllscoile has ultimate responsibility for overseeing the management of risk within the University as a whole.
* Responsibility for the management and implementation of the risk register is devolved and explained further in section 5.2.
* All members of the University community have a responsibility to engage in effective risk management.
* Risks and mitigating controls are identified which consider the Professional Supports Units (“Units”), Colleges and University objectives as set out in the strategic plan and unit operational plans.
* There are occasions where risks are unavoidable and instead must be managed. Controls are put in place to reduce the risk to a level which is so far as reasonably practicable.
* The risk management process will be fully embedded in the normal management structures and processes so that risk issues are considered by those involved in the day-to-day running of the University who are charged with the achievement of objectives. Where relevant, proposals brought forward for decisions should include a specific section on the assessment of risk and how it will be managed.
* The assessment of risks will be completed at all levels of the University.
* The University’s standard means of scoring risks is based on the likelihood of a risk becoming a reality combined with the severity of that risk (see Appendix 1).
* The main forum for risk management of the capital programme is the Capital Programme subcommittee of the Finance and Resource committee.
  1. **Roles and responsibilities**

***“The management of risk is the responsibility of all staff.”***

Roles and responsibilities are detailed below:

| **Structure** | **Responsibility** |
| --- | --- |
| **Údarás na hOllscoile (Governing Authority)** | Overall responsibility for the management of risk within the University. Údarás will approve the University’s risk management framework. Key elements of their oversight of risk management include but are not limited to:   * Satisfying itself that the policy is effective through the work of the Audit and Risk Committee; * Satisfying itself that an effective risk management framework is in place and that key strategic and operational risks are being managed; * Making risk management a standing meeting agenda item; * Approving the risk management policy and setting the risk appetite of the University; * Reviewing management reporting on risk management and noting/approving actions as appropriate; and * Requiring external review of effectiveness of risk management framework on a periodic basis. |
| **Audit and Risk Committee (ARC)** | Subcommittee of the Governing Authority (GA) who provide independent advice to the GA regarding the suitability and robustness of the organisation’s risk management framework. The Chair of ARC provides regular reports to GA. |
| **UMT** | Overall responsibility for implementation of this policy. As well as responsibility for the Units or Colleges which report to them, they will also implement the policy through the following risk groups: |
| 1. **Risk Management Group (RMG)** | Membership consists of all UMT and two external nominees. This group reports to the Audit and Risk Committee. Oversight and facilitation of the development of policy and risk registers with focus on operational risks and emerging risks from the University Risk Forum. |
| 1. **University Risk Forum** | Attended by nominated staff with responsibility for risk management. This forum facilitates a discussion on risk and risk registers to ensure consistency and provides an avenue for the identification of common risks and joint owners. The group meets twice annually and reports to the RMG. A member of UMT chairs this forum. |
| **Units/ Colleges** | Senior management within Units and Colleges, such as Heads of School and Heads of Unit, are responsible for ensuring compliance with the risk management framework. |
| **Director of Strategy Implementation (President’s Office)** | Policy Owner with responsibility for ensuring the implementation of the University’s risk management framework through review, guidance and training. Chair of the RMG and reports directly to the President. |

* 1. **Risk Management Process**

Risk management is a continuous cyclical process of identifying risks, assessing and prioritising the risks, developing action plans to improve how risks are managed and completed by a system of regular monitoring and reporting.

University strategy and unit operational plans and objectives considered at all stages

* 1. **Risk Management Cycle**

The Risk Management Procedure document provides further information in relation to the above.

* 1. **Management of Risk**

Upon completion of a risk assessment and taking account of the University’s risk appetite, the University will respond to the risk in one of the following ways;

* **Treat** the risk – use or enhance existing internal controls or implementation of new controls.
* **Terminate** the risk – a decision is made not to undertake the activity that is likely to trigger the risk.
* **Tolerate** the risk – accept the risk with or without monitoring.
* **Transfer** the risk – share the exposure, either totally or in part, with a partner or contractor, or through insurance. Any partnership will need to be carefully monitored as it may not be possible to transfer all risks and certain aspects may remain, such as loss of reputation.

It is the University’s aim to reduce the risk to “**a level as low as reasonably practicable**”.

1. **Review of the policy**

The policy will be subject to an annual review and presented to RMG, ARC and Governing Authority for approval.

*Visit the* ***P&P Repository*** *on the* ***Quality Office website*** *for other policies, procedures, regulations and guidelines (*[*www.universityofgalway.ie/quality/repository*](http://www.universityofgalway.ie/quality/repository)*)*

**Appendix 1 – Risk Assessment**

|  |  |  |
| --- | --- | --- |
| **Assessment** | **Inherent** | **Residual** |
| **Impact** | The extent of the impact on the University’s operations if the risk arises in the absence of any key controls. | The extent of impact on the University’s operations if the risk arises and controls are in place and operating effectively. |
| **Likelihood** | The probability of the risk arising in the absence of controls. | The probability of the risk arising if controls are in place and operating effectively. |

**Explanation of impact and likelihood**

|  |  |  |
| --- | --- | --- |
| **Impact** | | **Examples of impact** |
| **Severe** | 5 | * Financial impact over €1 million. * Impact results in strategic objectives not being met. * Closure or disruption of the University for greater than two days * Serious debilitating injury or loss of life * Prominent coverage of the University in national news media. |
| **Serious** | 4 | * Financial impact of €500,000 - €1 million. * Reduction in income or funding of greater than 10% per annum. * Systematic irregularity in the system of internal control resulting in a widespread change in processes. * Closure or disruption of the University for up to two days. * Injury requiring hospitalisation. * Adverse media coverage. |
| **Significant** | 3 | * Financial impact of €100,000 - €500,000. * Reduction in income or funding of greater than 5% per annum. * Delays in the delivery of operational and academic processes impacting on student experience. * Closure or disruption of the University for up to 24 hours. * Injury requiring medical attention. * Adverse local media coverage and reputational damage with funders. |
| **Minor** | 2 | * Financial impact of €5,000 - €100,000. * Minor delay in the delivery of operational and academic processes impacting on the student experience. * Closure or disruption of the University for up to 12 hours. * Minor injury. * Adverse reaction of those impacted by the event. |
| **Insignificant** | 1 | * Financial impact less than €5,000. * Closure or disruption of the University for up to two hours. * Cuts/bruises. |

|  |  |  |
| --- | --- | --- |
| **Likelihood** | | **Explanation** |
| **Very probable** | 5 | Will occur within the next 12 months. |
| **Quite probable** | 4 | Likely to occur within the next one to two years. |
| **Possible** | 3 | May occur within the next one to three years. |
| **Improbable** | 2 | Unlikely to occur within the next one to five years. |
| **Very unlikely** | 1 | Rare and unlikely to occur for the foreseeable future. |

**Calculate scoring**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Likelihood** |  | **Very unlikely** | **Improbable** | **Possible** | **Quite possible** | **Very probable** |
|  | **Multiplier** | **1** | **2** | **3** | **4** | **5** |
| **Impact** |
| **Severe** | **5** | **5** | **10** | **15** | **20** | **25** |
| **Serious** | **4** | **4** | **8** | **12** | **16** | **20** |
| **Significant** | **3** | **3** | **6** | **9** | **12** | **15** |
| **Minor** | **2** | **2** | **4** | **6** | **8** | **10** |
| **Insignificant** | **1** | **1** | **2** | **3** | **4** | **5** |

**Risk Appetite response**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rating** | **Risk rating** | **Level of concern** | **Target resolution & review** | **Risk response** | **Immediate action required** |
| 20 - 25 | Extreme | Unacceptable level of risk exposure which requires immediate corrective action to be taken. The activity or project should not proceed or ongoing work ceased until a response is determined. | **1 - 3 months**  Status review at each UMT meeting (every two weeks) | Terminate  Treat  Transfer | UMT to be notified |
| 12 – 19 | High | Unacceptable level of risk exposure which requires constant active monitoring, and measures to be put in place to reduce exposure. | **3 - 6 months**  Status review provided monthly to UMT | Terminate  Treat  Transfer | UMT to be notified |
| 8 – 11 | Medium | A mitigation/action plan must be developed and implemented to reduce exposure. | **6 – 12 months**  Reviewed quarterly with monthly reporting to Head of School/Unit. | Treat  Transfer | Head of School/ Unit |
| 3 – 7 | Low | Tolerable level of risk exposure arising from established controls in place. | Review every 6 months or as and when a change occurs. | Tolerate | N/A |
| 1 - 2 | Insignificant | No concern. |

**Appendix 2 – Risk categories**

|  |  |
| --- | --- |
| **Category** | **Description** |
| **Reputation** | A negative impact on the University’s reputation with stakeholders and funders. |
| **Legal & compliance** | Non-compliance with legal and best practice requirements. |
| **Financial** | A negative impact on the University’s finances. |
| **Teaching and learning** | Disruption in the delivery of teaching and learning to students. |
| **Student experience** | Negative impact on the entire student experience. |
| **Research & innovation** | Reduction in the quality and quantity of research. |
| **Strategic initiatives** | Impact on the ability to meet strategic objectives. |
| **International development** | Reduction in international student recruitment or negative impact with international business partners. |
| **People & culture** | Reduction in staff wellbeing, dissatisfaction amongst staff or development of sub cultures. |
| **Environment and social responsibility** | Impact on ability to meet sustainability strategy and wider climate action plan. |
| **IT Systems & business continuity** | Disruption to IT systems and University operations for a period of time. |
| **Operational processes** | Disruption to local operational procedures or systems of internal control. |
| **Health & Safety** | Physical harm, injury, illness or a fatality to staff, students and visitors. |
| **Cybersecurity** | Criminal or unauthorised use of the University’s electronic data. |
| **Global, economic and geostrategic environment** | Impact on University operations as a result of the global, economic and geostrategic environment. |

**Appendix 3 – Risk appetite per risk area category**

|  |  |
| --- | --- |
| **Categories** | **Description** |
| **Reputation** | It is critical that the University preserves its high reputation. The University strives to ensure that all activities undertaken will protect and enhance its reputation and therefore has a **low** appetite for risk in the conduct of any of its activities that could lead to undue adverse media attention, or could lead to loss of confidence by the international community, research community and stakeholders. |
| **Legal & Compliance** | The University places great importance on compliance, and has a **low** appetite for any breaches in laws, regulations, research ethics, professional standards, bribery or fraud. The University wishes to maintain accreditations related to courses or standards of operation and has no appetite for risk relating to actions that may put this in jeopardy. |
| **Financial** | The University aims to maintain its long-term financial viability and its overall financial strength. It has a **low** risk appetite in this area.  The University will provide a sustainable financial environment that supports both its ongoing operations and its strategic development. Recognising the significant skill and judgement required in the development and implementation of appropriate financial strategies, it will ensure that related risks are managed and mitigated through the application of professional expertise and prudent, transparent and accountable decision-making. |
| **Teaching & Learning** | The University aims to educate students who, as graduates, will demonstrate a capacity for independent critical thinking, creativity and innovation, dynamic teamwork, socially responsible leadership, and a commitment to lifelong learning. It wishes to provide a stimulating learning environment for students of the highest possible quality. It recognises that it will involve an increased degree of risk in advancing delivery and quality in this area and is comfortable in accepting a **medium** risk appetite, subject to ensuring that potential benefits and risks are fully understood before developments are authorised and that appropriate measures are established to mitigate risks to maintain the required standards in this area. |
| **Student Experience** | The University is committed to the further development of facilities and support arrangements for the student learning and living experience and in ensuring that programmes are accessible to all backgrounds and disabilities. The University will maintain a **low** appetite for any risks that threaten the delivery of objectives in this area. |
| **Research & Innovation** | The University wishes to enhance its reputation as a research institution that is excellent, globally collaborative, creative, interdisciplinary and entrepreneurial. A university that produces research that serves and anticipates economic, societal and cultural needs. It wants to play a transformative role in Irish Society by using inspirational research to generate new knowledge, to respond to the needs of businesses and other institutions, and to realise human capital. Its ambition is to be at the leading edge in the creation of knowledge. It wishes to grow its research activities and recognises that this will involve accepting a **medium to high** risk appetite.  Risks will be acceptable subject to a) limitations imposed by ethical considerations and health and safety, and b) risks and potential benefits are fully understood, reviewed and authorised before accepted. |
| **Strategic Initiatives** | The University sets an ambitious vision and strategic objectives to ensure it remains at the leading edge of research and teaching. It recognises that this requires some degree of risk and that external and internal forces, which can often not be predicted, may have a significant impact on achieving key strategic objectives. This can often involve significant changes in structure and/or culture that can further affect the University achieving its strategic objectives over the short term. The University is accepting a **medium to high** risk appetite in this area. |
| **International Development** | The University aims to achieve a reputation as one of the world’s top-tier universities, with relationships of substance that span the globe. It wishes to educate students who are globally conscientious and internationally engaged, and who excel as scholars, citizens and global leaders. It will recruit and retain staff who are internationally renowned in their fields and embedded in international networks of scholarship. It aims to achieve global impact in its activities, collaborations and staff/student exchanges with leading institutions around the world. It has a strong appetite for developing such networks where it supports the objectives and strategy of the University. The University thus have a **medium to high** risk appetite for International Developments. |
| **People & Culture** | The University aims to value, support, develop and utilise the full potential of staff to make the University a stimulating and safe place to work. It wishes to consolidate and refine existing academic and research structures and associated processes, and to restructure its services into larger, more flexible and effective units, for the maximum benefit of users and providers. It places importance on a culture of academic freedom, equality & diversity, dignity & respect, the development of staff and the health & safety of staff, students and visitors. It has a **low to medium** appetite for any deviations from its standards in these areas. |
| **Environment and Social Responsibility** | The University aims to make a significant, sustainable, and socially responsible contribution through its research, education, knowledge exchange, and operational activities. It recognises that this should involve an increased degree of risk and has a **low to medium** appetitesubject always to ensuring that potential benefits and risks are fully understood before developments are authorised and that sensible measures to mitigate risk are established. |
| **IT Systems and Business Continuity** | The University has **no appetite** for inadequate or failed internal systems. This can include, inadequate design of systems or lack of infrastructure, etc. |
| **Operational processes** | The University has a **low** risk appetite for inadequate or failed internal processes. This can include inadequate policies and procedures, inadequate adoption of management practices, lack of clarity over roles and responsibilities, inadequate design of processes and systems, inadequate or lack of infrastructure, etc. |
| **Health & Safety** | The University has no appetite for risks related to activities which could lead to Physical harm, injury, illness or a fatality to staff, students and visitors.  Health & safety risks relating to research and innovation activities will need to be assessed alongside the risk appetite relating to ‘research and innovation’ activities. |
| **Cybersecurity** | Following an independent review of the University’s vulnerability to criminal or unauthorised use of our electronic data in 2023, our appetite for risk in this area ranges from **insignificant to** **low**.  This is in acknowledgement of the residual risk of an evolving cybersecurity landscape even when all recommended mitigations and controls are in place. |
| **Global, economic and geostrategic environment** | The University has a **medium to high** risk appetite in this area.  Many risks in this area are considered and scored by the Risk Management Group as part of their annual Strategic Risk Register exercise. |

**Risk Appetite Summary**

**A screen shot of a computer screen

Description automatically generated**

1. DPER Risk Management Guidance February 2016 [↑](#footnote-ref-2)