UNIVERSITY OF EXETER

Risk Management Policy

1. Introduction

Effective risk management is an essential element of good management and governance practice and is one of the key tools used by the University to achieve its objectives. There are a suite of internal controls and corporate governance arrangements to support this, such as policies, audits and feedback mechanisms. Risks identified via these internal controls are reported into the risk register**,** for consideration and management.

A risk is defined as "the effect of uncertainty on objectives" *(ISO 31000)*. Taking time to evaluate any risks that we may face will ensure that informed decisions are made that help us to achieve our objectives.

Risk Management can be defined as "coordinated activities to direct and control risks with the organisation" *(IRM, A Standard for Risk Management).* The University has processes, which methodically addresses the risks associated with the activities, supporting the attainment of our goals. Good management of risk increases the probability of success and decreases the probability of failure and uncertainty. The purpose of risk management is to reduce any possible negative impact a risk may have on the University, and to seize opportunities that arise.

This policy sets out our approach for managing risk with the University of Exeter.

2. Purpose of this policy

- To set out the University approach to risk management and signpost to the processes for identifying, assessing, recording, reporting and managing risks across all areas of the University.
- To set out the roles and responsibilities of Council, Audit and Risk Committee, Dual Assurance Groups, University Executive Board (UEB), Senior Management in Faculties and Professional Service and Corporate Risk Owners.
- To ensure that UOE continues to develop its organisational culture around the importance of effective management of risk
- To set out how the risk management policy will be monitored, to ensure it is implemented and remains effective.

The policy is supported by process documents and supporting training materials, which set out how risk management and reporting works in practice (*in development, to align with digital risk register*).

3. Key principles

The University is a vibrant and engaging environment where we use the power of our education and research to create a sustainable, healthy and socially just future.

During our endeavors, we encounter numerous risks. We recognise in the pursuit of our objectives and ambitions we may need to take risks in order to meet our strategic aims. Subject to robust risk assessment, we will manage these risks effectively to ensure that our decisions fulfil our duties to:

- Act ethically and responsibly in compliance with the law and charitable and royal status'
- Encourage critical enquiry, debate and freedom of expression within the law
- Uphold the University values
- Maintain the excellent reputation of the University

The University's fundamental principles of risk management are as follows:

- Risks to the University are managed in such a way that they are visible to the Senior Leadership Team across all areas of University activity, acknowledging that risks are inherently interconnected and not managed in silos
- Risk management is achieved both from a "top down" and "bottom up" view to enable full opportunity for risks to be identified and managed
- All levels of management have an open and receptive attitude to managing risks, ensuring that they are identified, assessed, managed and reported appropriately across all levels of the organisation.
- Risks will be scrutinized during the risk cycle, to ensure proportionality and to ensure there is an accurate record of the risks that exist within the organisation.
- Training, support and risk management tools are available to all staff to ensure competency in risk management, registration and reporting.

4. Governance of Risk Management

a) The Compliance Committee, a committee of the University Executive Board, reviews and scrutinizes the first draft of the risk report, which is updated from the risk registers each term, and recommends it to the University Executive Board (UEB), incorporating any amendments agreed with risk owners. The Compliance Committee monitors that legislative, regulatory or policy requirements are being met, forming part of the internal control risk management process.

b) UEB has overall responsibility for the institutional management of risk, with Council retaining oversight of risk management as the accountable body. UEB monitors the University's risk profile including Corporate and Operational Risk. They monitor key new and emerging risks and ensure that risks are being managed and controlled effectively with a clear system of accountability and responsibility in place. UEB reports the status of risk management to Council, via a termly Risk Report. UEB discuss and agree the processes for managing risk and bring forward proposals to Council for final sign off. UEB, approve and support the implementation of corporate policies, which set out how risks will be managed.

c) The Audit and Risk Committee, provides a pivotal role as a Committee of Council in taking assurance on the risk management processes in place. Audit and Risk Committee reviews the risk report each term, presents its opinion to Council and summarises this in its Annual

Report, to inform Council's understanding of risks and internal controls. Audit and Risk Committee directs the internal audit programme, which incorporates scrutiny of specific risks and their controls. This also includes an annual audit of the Risk Management process.

d) Council is the accountable body for risk management at the University. Council seeks assurance that associated policy and processes remain effective. Council takes an opportunity during each risk cycle, to review the risk report and feedback to UEB on any amendments to direction of travel for specific risks, or with the risk management process itself. Council also receives a report from the Chair of the Audit and Risk Committee on its view of the management of risk.

5. Roles and Responsibilities

5.1 Role of University Executive Board (UEB)

a) To have institutional management oversight and operationalisation of the University Risk Management process and reporting system, including the Risk Management Policy, Risk Register and all other supporting tools. UEB is accountable to Council for their oversight.
b) To identify and review the corporate risks, with ownership of these being allocated to relevant members of the board.
c) To monitor, at a high level, the Operational risks in Faculties and Professional Services and consider how they may relate to corporate risks.
d) To review the Amber and Red corporate risks and identify if these risks are within tolerance or agree where any additional action is required to manage the risk.
e) To consider, monitor and manage the University's risk profile. This involves ensuring that planned and existing actions / controls are implemented, and that their effectiveness is validated to ensure that risks are mitigated as planned.
f) To analyze in depth specific significant risks, on an exception basis as determined by UEB itself and/or Council.
g) To provide Audit and Risk Committee with sources of information and assurance on the institution's Corporate and key Operational risks.
h) To consider such matters as may be referred to it by Council or Audit and Risk Committee.
i) To ensure that the University's risk management policy is appropriate at all levels of the University to deliver good practice and to comply with relevant regulatory requirements.
j) UEB discussion and decision making is informed by the risk management principles at each meeting, and UEB reviews the formal risk report three times a year.

5.2 Role of Council

a) Take assurance, via reports from UEB and Audit and Risk Committee that risks are being managed effectively.
b) Periodically review the University's approach to risk management and approve changes or improvements to key elements of its processes and procedures.
c) Appoint Internal and External Auditors.
d) On an annual basis (or as required if within the annual cycle), using the specialist knowledge of its members, consider whether additional risks should be reviewed against the University's risk profile.

5.3 Role of Audit and Risk Committee

a) To keep under review the effectiveness of the management of risk, the control and governance arrangements in place.
b) Report to Council on findings with regards the effectiveness of the University in identifying, assessing and managing risk, taking into account the Internal Auditor opinion on the risk management process and risks identified in the annual audit plan.
c) To receive regular detailed updates on the work of the UEB and the senior management team and to receive copies of relevant UEB and other key committee minutes.
d) To meet annually with representatives of the UEB and the senior management team in order to take assurance on the risk management activity across the institution and the information collected on risks and risk management.
e) Seek updates from appointed Auditors on the risks facing the sector to ensure the University has an up-to-date risk profile.

5.4 Role of Dual Assurance

Dual assurance supports risk management by combining the expert knowledge of a management lead and an independent external lead to seek assurance on processes and risks in key strategic business areas.

a) Dual Assurance meetings include, at planned intervals, the review of registered corporate risks within its area of expertise and focus.
b) Assurance is sought by the Independent and Executive Leads that these risks are scored and managed effectively, including seeking evidence that controls in place are effective and that if a risk is scored at amber or red, that an appropriate action plan is in place, owned, and progressing.
c) The specialist knowledge of the Dual Assurance Leads is utilized to consider whether additional risks or impacts should be considered and reviewed by the relevant corporate risk owner.

5.5 The Role of Other Key Committees

There are a number of key committees of UEB that provide an important role in the direct management of risk. These Committees are committees of UEB:

1. Capital Investment Group
2. Business Engagement and Innovation Committee
3. Research and Impact Executive Committee
4. Global Engagement Committee
5. Wellbeing, Inclusion and Culture Committee
6. Compliance Committee

There are a number of other committees and groups, which have a role in the management of risk at the University such as the University Consultative Health and Safety Committee and the Information Steering Group. The Chairperson is responsible for ensuring there is sufficient time allocated to the agenda to consider any existing, changed, and new risks and consider how new risks identified are added to the risk register.

All persons appointed as chair to University Committees should be fully conversant with the risk management policy and take steps to ensure that any risks identified are managed in accordance with this policy and associated procedure. Strategic decision making should be informed by a review of associated risks.

5.6 The Role of Risk Owners

UEB devolves the responsibility for managing specific risks to Risk Owners who either are subject matter expert senior managers or are senior leaders of Faculties and Professional Services.

Key responsibilities of the Risk Owners are to:

a) Implement policies and internal controls (directed by UEB) to manage the key risks of the University, taking action when it is identified that there are gaps in policy compliance.
b) Identify, evaluate and record risks on the risk register and keep the risk register up to date.
c) Provide adequate information in a timely manner to UEB and Council on the status of risks and controls including submitting an updated risk register to the Risk Management Lead in accordance with the risk management reporting cycle.
d) Identify where risk or control ownership is shared across different areas of the University, and ensure that a holistic approach is taken, with information on risk profile, controls and their effectiveness shared with relevant parties. See note below*
e) Attend relevant committees, such as Audit and Risk Committee, when in-depth reviews of their risk(s) are being carried out, and to represent on their own risks and mitigations.
f) Assist with the annual review of risk management by the internal auditors where requested.
g) Promote effective risk management practices to managers to deploy on a day-to-day basis as an important tool of good management.
h) Allow time to discuss risks in meetings, promoting and encouraging the identification, reporting, and ongoing control of risk.
i) Ensure that the connections between Corporate and Operational risks are understood and managed, so that fluidity and actions are maintained between these two levels of risk management.
j) Ensure that the risks they oversee are properly managed, and that identified actions and mitigations are effective in controlling risk.
k) Seek advice on risk scoring from the Compliance and Risk Team, where required.

*Not all Risk Owners or facilitators will have direct responsibility for, or the ability to manage, particular risk elements within their register. For example, the 'Delivering Student Expectations' risk entry is owned by a Professional Service, but many of the elements affecting the risk will be delivered directly by the Faculties. In instances such as these, the responsibility of Risk Owners is to obtain assurance that the risk is being addressed effectively by all areas responsible for associated controls. If it is not clear that this is the case, then the scoring of the risk may be affected, and any significant issues can be noted in the narrative for follow-up by Senior Management.

5.7 The Role of University Corporate Services (UCS) Directorate

The UCS Directorate, specifically the Compliance and Risk Team is responsible for;

- Ensuring there is central competency to support the implementation of the risk management policy, tools and systems. Keeping the risk management policy up to date.
- Developing, supporting and advising risk owners, managers and committee chairs on effective risk management.
- Providing training, workshops and toolkits to develop risk owner skill in the reporting and management of risk.
- Have oversight and co-ordination of the risk management process (i.e. the process by which corporate and high-level operational risks are reported by Faculties and professional Services to senior management).
- Support UEB by coordinating the risk management reporting cycle and preparation of risk reports.
- Horizon scanning, assisting with the identification of emerging key risks and facilitating risk identification and assessment where required.

6. System of Internal Control

The Risk Management Process is part of the University's internal control system, which can be considered under the "Three Lines of Defence" framework. Three lines of defence model sets out how the different parts and levels of the University play important roles in effectively managing risk.

6.1 The First Line of Defence

In the first line of defence are managers and those who are responsible for operationally identifying, owning and managing risks, following approved policies, procedures and guidelines set by UoE to manage risk. In the first line of defence, they are responsible for:

- **Compliance with all relevant policies and procedures -** those who manage risk should be fully conversant with policy requirements that are required within their area of responsibility, implementing those requirements, monitoring that policy requirements are being fulfilled.
- **Risk Assessment -** ensuring that risks are identified and assessed within their management areas.
- **Implementing risk treatment –** including deciding whether to:
    - **Avoid –** stop the activity that introduces the risk
    - **Reduce –** take actions to directly the limit the likelihood or impact of the risk
    - **Transfer** – via outsourcing or insurance (note that these do not completely mitigate the risk, e.g. insurance has a premium cost attached, and likely excess payable. Insurers will require reasonable risk controls to be in place against the addition protection being purchased).
    - **Share** – agreed liability sharing with partners for known joint risks
- **Risk monitoring** - comprehensive and regular monitoring of risks and controls via the risk register. The updates provided by risk owners to the formal risk reporting cycle should evidence that risks have continued to be managed between the reports within the cycle and highlight any changes in score and/or actions. Action plans to improve existing or implement additional controls should be monitored to completion by the risk owner, with any resulting impact on the risk profile reflected in the scoring. Risk monitoring should include an

assessment of new information that changes the risk profile, in addition to reviewing controls in place and action plans already in progress.

- **Risk based decision-making** -. Risk assessment is built into various committee-reporting templates to enable committees to consider the risks of any proposals being made.
- **Business Continuity planning** – sets out how the University (or departments thereof) would continue to manage key operations should a major event or situation occur.
- **Business planning and budgeting** - set objectives, agree action plans, and allocate resources considering risk. Progress towards meeting objectives is monitored regularly.

6.2 The Second Line of Defence

The provision of effective policies, frameworks, tools, techniques and support to enable risk and compliance to be managed in the first line. Second line of defence is interested in ensuring there is sufficient training and skill in the first line to identify risk, ensuring monitoring is carried out to judge how effectively policies are being implemented in practice, and ensuring effective tools are in place enabling risks are being assessed and managed.

The types of controls within this defence line are (not exhaustive):

- **Communication and training on internal controls** – All new staff are required to carry out mandatory training which includes details of how risks are managed at the University. Local inductions are in place to appraise staff of the risks in the work environment. Training and development in the management of risk topics, policies and procedures is widely available.
- **Competent Advisors** – the University employs a number of competent advisors across various subject matter, who set policy, give advice, support and training to those in the first line, on the management of risk. From time to time, the use of external consultants to review risk controls in specific areas may prove necessary, the engagement from specialist third parties for consulting and evaluating may be required.
- **University policies and procedures** – University policies set out how core and regulated activities of the University must be carried out. Written procedures support the policies where appropriate.
- **University Compliance Framework and Monitoring**- The Compliance Framework is the University register of all legislative, regulatory and policy requirements that the University is obligated to, or has chosen to, comply with. The Compliance Committee, a committee of UEB, is responsible for seeking assurance that the University is meeting those requirements. Policies are monitored to assess the rate of compliance in practice. Where any matters identified pose a risk, the Compliance Committee will seek evidence that steps are taken to assess and manage the risk and that it is recorded on the relevant risk register.

6.3 The Third Line of Defence

The third line of defence is in place to assess and evaluate, on behalf of the governing body and UEB that the controls in place within the first and second lines of defence are working effectively and provide recommendations on any areas that can be improved. The third level can also be used to give assurance to regulators that appropriate controls and processes are in place and operating effectively.

- **Internal Audit** – appointed by Council, the Internal Auditor will review key processes, evaluating risk controls and report findings to the Audit and Risk Committee. This includes

highlighting where findings indicate an increased level of risk. Audit and Risk Committee provide UEB with the final audit reports and its opinion on the management of the risks identified.

- **External audit** – appointed by Council, this focuses specifically on the effectiveness and accuracy of financial controls and provides feedback to the Audit and Risk Committee as part of the annual audit review. The External Auditor also provides sector benchmarking information to inform Audit and Risk Committee's assurance that the University has identified the relevant risks.

7. Policy Monitoring

To supplement the annual Internal Audit of Risk Management, the Senior Risk and Compliance Advisor will monitor the Risk Management Policy annually. The following areas will be investigated to support the ongoing improvement of the positive risk management culture:

1. **Risk Management training and development is in place and staff are attending as appropriate:**
    a. All staff with formal risk management responsibilities have received targeted training from the Compliance and Risk Team
    b. Mandatory training for all staff

2. **Risks are being considered and managed in key meetings (from a sample)**
    a. Other Committees of Council or UEB as set out at section 5.5
    b. Dual Assurance Groups
    c. Meetings of Faculty and Division Senior Management Teams
    d. Specialist meetings such as Fire Safety, Information Steering Group etc.

3. **The quality of risk reporting will be assessed (from a sample)**
    a. The risk descriptions follow the cause, event and consequence model and clearly define the risk to any audience.
    b. Risk scores can be justified using the University scoring matrix impact statements.
    c. Controls are assessed for effectiveness and are reflected in the residual risk score.
    d. Action plans (where relevant) are targeted at improving existing or implementing new controls that will positively impact the likelihood and/or impact of the risk.

4. **There is evidence of constructive challenge on risks and risk scoring**
    a. Minutes from meetings set out at monitoring point 2 above.
    b. Minutes from the meetings conducting the scheduled review of the risk report.

The findings of the Policy Monitoring will be reported to the Compliance Committee and any action required to address any issues identified will be monitored by the Compliance Committee.

Document Revision History

Initiation Date	14/07/2016		
Author	Kate Lindsell, Assistant Director UCS (Compliance and Risk)		
Key contributors	Tracey Tuffin, Senior Risk and Compliance Advisor		
Approver	Council		
Last review date	March 2023	Next review date	Jan 2025 or sooner where audit or monitoring identifies a need
Consultation Plan	• Divisional Director UCS - Completed 16/02/2023 • Compliance Committee – Completed 14/02/2023 • PDSLT - Completed 20/02/2023 • UEB – Completed, revisions included 24/02/2023 • Audit and Risk Committee - Completed, revisions included 07/03/2023 • Council - Completed, revisions included 18/05/2023		
Communication plan	On approval: • Final document uploaded to Risk webpages • Email to all risk owners / those with responsibility advising of the updated policy		

Version	Revision Date	Modified by	Description of Revision	Approved by
2	January 2023	Assistant Director UCS (Compliance and Risk)	Full review to refresh roles and responsibilities in line with University organisational design changes To incorporate feedback received in the PWC risk management audit. To incorporate best practice as identified by the Institute of Risk Management.	Council, May 2023
1	July 2016	Director of Compliance Governance and Risk	First publication of policy	Council, July 2016