UNIVERSITY OF EXETER

Risk Governance and Management Policy Framework (Updated April 2016)

Introduction

There are two major drivers for Universities adopting and implementing risk management policies. First, the effective understanding and management of risk is central to the delivery of our strategic objectives over all time frames. Second, there is a statutory requirement to manage risk to good practice standards, stipulated by HEFCE, and that full compliance with HEFCE's requirements must be attained.

More generally, it is worth restating that whilst there is often an emphasis on 'threats' when thinking about risk, an effective risk management policy should enable the University to seek and exploit opportunities, mindful of the risks therein.

The policy should not be only about fundamental or major risks, but should also operate at all levels, guiding good management across the University.

Purpose of this document

1. This risk management policy forms part of the University's internal control and corporate governance arrangements and exists to assist the University in achieving its strategic objectives.

2. The policy is not a process for avoiding risk. It is designed to allow the University to take on activities that may have a higher level of risk, because risks have been identified, understood and managed, within the University's overall risk appetite.

3. The policy explains the University's underlying approach to risk management, documents the roles and responsibilities of Council, Audit Committee, Dual Assurance, Vice-Chancellor's Executive Group (VCEG), Senior Management/Risk Owners and other key parties.

4. It outlines key aspects of the risk management process, and identifies the main reporting procedures. The overall approach identifies risk management as being integral to normal management processes, and in many areas the policy simply makes more explicit good practice.

Key principles

5. The University's fundamental principles to risk management are as follows:

    - The University should have a clear, effective and transparent framework for assessing, managing and reporting on risks that could affect its ability to deliver on strategic objectives.

    - The risk management systems should be incorporated within existing governance/management arrangements and reporting systems as far as possible.

    - The framework should address the taking of opportunities in the form of new and emerging risks, as well as effective management of existing risks or 'threats'.

- There should be a process in place for escalating risks for appropriate attention and action, i.e. where risks could threaten in a new way the University's strategic objectives.
- Risks at University and College/Professional Service level should be overseen and managed through a clear system of accountabilities and responsibilities.
- Risks at an operational level should form part of the overall system, as in some cases and circumstances they can impinge upon strategic objectives.
- Council should receive reports on risk alongside those on performance so that clarity of connections between them is achieved.

Summary of the systematic approach to risk management

6. The following key means outline how the University's approach to risk management and internal control is implemented:

- Council is responsible for overseeing risk management and internal control within the University as a whole.
- Council adopt an open and receptive approach to solving risk problems, and have an appetite for risk where there are potential benefits for the institution. Council will have the opportunity to discuss with Senior Management how best to address key risk problems, potential mitigating activities, and / or strategies to address a risk that has materialised.
- Audit Committee presents opinions on a regular basis, and summarised in its Annual Report, to inform Council's understanding of risks and internal controls. The internal audit programme, which Audit Committee directs, includes scrutiny of specific risks and their controls, and an annual audit of the Risk Management process – which provides an annual opinion regarding the process.
- VCEG, which reports to Council and Audit Committee, monitors the University's risk profile including emerging risks, together with the Corporate Risk Register.
- VCEG is responsible for ensuring that systems and processes are in place to establish, develop and revise the overall risk management system.
- VCEG oversees the regular reporting and monitoring of risks, controls and key risk indicators.
- VCEG oversees the management of individual risks, with a clear system of accountability and responsibility in place for major risks.
- The Vice-Chancellor, VCEG and the Senior Management Group support, advise and implement policies with the delegated authority of Council.
- VCEG and Senior Management Group ensure linkage between the operational and strategic risks of the institution to ensure fluidity between the two areas of risk management.
- The University makes prudent recognition and disclosure of the financial and non-financial implications of risks;
- College Registrars/Directors of Services are responsible for ensuring good risk management practice within their areas;
- Project Managers are responsible for ensuring risk management is fully embedded in their approach to project management;
- All staff are expected to contribute to mitigating those risks that are relevant to them and their role.

Role of Council

7. Council has a major role to play in the governance of risk. Its role is to:
   a. Set the tone and influence the culture of risk management within the University. This includes:

      - Determining whether the University is 'risk taking' or 'risk averse' as a whole or on any relevant individual issue or activity
      - Determining, broadly, what types of risk are acceptable and which are not
      - Setting the standards and expectations of staff with respect to conduct and probity

   b. Determine the appropriate risk appetite or level of exposure for the University.

   c. Approve the major decisions affecting the University's risk profile or exposure.

   d. Periodically review the University's approach to risk management and approve changes or improvements to key elements of its processes and procedures.

Role of Audit Committee

8. To keep under review the effectiveness of the risk management, control and governance arrangements with such reviews being informed by the assessment of risks, which are assessed and monitored by VCEG.

9. To advise Council on Risk Management by:

   - becoming familiar with the concepts and requirements of risk management
   - ensuring appropriate audit work in risk management

10. To receive regular detailed updates on the work of the VCEG, receive copies of relevant VCEG minutes and to meet annually with representatives of the VCEG in order to review risk management activity across the institution and the information collected on risks and risk management.

Role of Vice-Chancellor's Executive Group (VCEG)

11. VCEG's role includes:

    a) To consider, manage and monitor the University's risk profile overall, including current, projected and potential risks. This involves ensuring that planned and existing actions / controls are implemented and that risks are mitigated as planned;

    b) To review, at a high level, the strategic risks facing the University, and the application of controls against those strategic risks;

    c) To analyse in depth specific major risks, on an exception basis as determined by VCEG itself and/or Council;

    d) To monitor, at a high level, the current and potential risks in Colleges and central Professional Services and how they relate to University-level risks;

    e) To provide Audit Committee with sources of information and assurance on the institution's strategic and key operational risks;

    f) To consider such matters as may be referred to it by Council or Audit Committee;

    g) 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 HEFCE requirements.

    VCEG discuss Risk Management three times a year.

Role of Dual Assurance

12. The concept of dual assurance was introduced at the University to provide for more executive decision making in place of committees without compromising on sound governance and the accountability and transparency required by Council. The business areas covered by dual assurance are:

• Finance and Investment	• Education
• Research and Impact	• Global Engagement and Development
• Human Resources and Health and Safety	• Risk
• Equality and Diversity	• Communication and Reputation
• Infrastructure and Environmental Sustainability	• Sport
• Information Technology	• Ethics

13. Each dual assurance group includes a Lay Lead (member of Council), Management Lead (VCEG member with oversight of the business area) and Coordinator. The role of the Lay Lead is **not** to manage the business area, but to ensure that it is well-managed, and that the Management Lead and other University colleagues have followed appropriate processes in reaching decisions. In particular the Lay Lead should consider three questions:

    a. Are the objectives in the strategy/plans relating to the business area being delivered? To what extent – fully, partially, nearly, not at all?
    b. Are the risks relating to activity in the business area being well-managed?
    c. Is communication sufficient?

14. The Lay Lead should also feel able to participate in debate, stimulate thought and challenge received wisdom in their business area.

15. For dual assurance the Lay Lead, as a member of Council, will be expected to develop an in depth understanding and knowledge of the business area in order to give guidance to the Chair of Council on whether there is cause for concern in its management. It is emphasised, however, that dual assurance does not interfere with line management and its processes for objective setting and performance monitoring.

16. Dual assurance is integral to risk management in two ways – individual areas of activity involve their Dual Assurance Lead in assessing and managing their risks, and Risk Management as a whole has a Dual assurance Lead.

17. The involvement of Dual Assurance Leads for specific areas in relation to Risk Management includes agreeing the Corporate Risk(s) owned by that area (i.e. assessing the scoring, current / planned mitigations, and nature of the risks included).

18. There is also Dual Assurance of the Risk Management process, which aims to:

    a) Look across the Corporate Risk Register as a whole to ensure that when the individual risks are brought together, the overarching Register gives a coherent and true picture of the strategic risks faced by the University.
    b) Discuss and monitor planned improvements to the Risk Management Process (e.g. arising from Internal Audit; Council requests; VCEG requests; response to good practice guidance)

c) Ensure that the information being provided to Council regarding Risk Management meets their needs
d) Consider the University's appetite for risk in different areas, recommend what the risk appetite should be, and ensure that it is embedded in practice.
e) Take account of Council's view of risk when carrying out the above.

Role of Senior Management and Risk Owners

19. Key roles of Senior Management and Risk Owners are to:

a. Implement policies on risk management and internal control (directed by VCEG) to manage the key risks of the University.

b. Identify and evaluate the corporate risks faced by the University for consideration by Council through VCEG.

c. Provide adequate information in a timely manner to VCEG and Council on the status of risks, controls and key risk indicators/early warning mechanisms, including submitting updated risk register to the Governance and Compliance Office in accordance with the risk management reporting cycle.

d. Assist with the annual review of risk management by the internal auditors.

e. Promote risk management to managers to deploy on a day-to-day basis as an important tool of good management.

f. Ensure that the connections between strategic and operational risks are understood and managed, so that fluidity and actions are maintained between these two levels of risk management.

g. Ensure that the risks they oversee are properly managed.

20. Not all Risk Owners or facilitators will have direct responsibility for, or the ability to manage, particular risk elements within their register. For example, 'Delivering Student Expectations' is owned by a Professional Service, but many of the elements affecting the risk will be delivered directly by Colleges. In instances such as these, the responsibility of risk owners / facilitators is to obtain assurance that the risk is being addressed effectively. 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.

Role of the Governance and Compliance Office

21. The Governance and Compliance office is responsible for the oversight and co-ordination of the risk management process (i.e. the process by which strategic and high-level operational risks are reported by Colleges and Services to senior management). Specifically it supports VCEG and the annual risk management review and reporting cycle; supports Dual Assurance for Risk Management; provides support for Risk owners / facilitators; and formulates policies, procedures and guidance.

Risk management as part of the System of Internal Control

22. The risk management framework incorporates the internal control system. This framework encompasses a number of elements that together facilitate an effective and efficient operation, enabling the University to respond to a variety of governance, staff, student experience, teaching, research, reputational, estate, operational, financial, and commercial risks. These elements include:

a. *Policies and procedures*

Attached to corporate risks are a series of policies that underpin the internal control process. The policies are set by Council and implemented and communicated by senior management to staff. Written procedures support the policies where appropriate.

b. *Regular risk reporting*

Comprehensive and regular reporting is designed to monitor key risks, controls and key risk indicators. Decisions to take proactive action will be made by risk owners, VCEG, senior management and Council if appropriate.

c. *Business planning and budgeting*

The business planning and budgeting process is used to set objectives, agree action plans, and allocate resources. Progress towards meeting business plan objectives is monitored regularly. Risk assessment is incorporated into the business planning process.

d. *Risk owners*

VCEG delegates the responsibility for managing specific risks to different senior managers who are risk owners. They are responsible for monitoring and reporting on the performance of risks, controls and key risk indicators/early warning mechanisms.

e. *Corporate risk framework*

This framework is compiled by VCEG and helps to facilitate the identification, assessment and ongoing monitoring of risks, which were they to crystallise would have a fundamental effect on the University's ability to achieve its objectives. The Corporate Risk Register is reviewed three times a year by VCEG but emerging risks are added as required, and improvement actions and key risk indicators monitored regularly by risk owners.

f. *College / Professional Service Risk Registers*

College Registrars and Directors of Services develop and use this framework to ensure that risks in their operating environments, which would stop them achieving their objectives, are identified, assessed and monitored. The Registers are reviewed twice a year but emerging risks are added as required, and improvement actions and key risk indicators are monitored regularly by risk owners. Risks which are considered to be of a fundamental nature are escalated through to VCEG for potential inclusion in the Corporate Risk Register.

g. *Audit Committee*

The Audit Committee is required to report to Council on internal controls and alert Council to any emerging issues. In addition, the Committee oversees internal audit, external audit and management as required in its review of internal controls. VCEG has an accountability with regard to the proper management of risk to Council and Audit Committee.

h. *Internal audit programme*

Internal audit is an important element of the risk management framework. The Internal Audit Strategy is linked to the University objectives and Corporate Risk Register as a primary resource. Apart from its normal programme of work, internal audit will report on risks, controls and key risk indicators to risk owners and Audit Committee. Audit Committee in turn will provide VCEG with reports on specific risks where significant concerns are being raised by auditors.

i. *External audit*

External audit provides feedback to the Audit Committee on the operation of the internal financial controls reviewed as part of the annual audit.

j. *Risk based decision-making*

The University embeds risk thinking in taking all major decisions. Financial and non-financial risks are identified as well as ways of managing them down to levels within the University's appetite range for taking differing types of risk.

k. *Risk education*

As part of the Risk Management process, training / information is provided on key risk concepts, risk based decision-making and the managing and monitoring of risk. Training is offered to facilitators on a one-to-one basis. Detailed guidance is also provided and links to other sources of information with the risk templates are available to address queries that facilitators may have. In addition, the University's Legal and Insurance Services also provide training around risk for staff at an operational level.

l. *Business Continuity*

Business Continuity plan forms an important element within the system of internal controls.

m. *Third party reports*

From time to time, the use of external consultants may prove necessary. The use of specialist third parties for consulting and reporting can increase the reliability of the internal control system.

Annual Assessment of Risk

23. Internal Auditors, advised by Audit Committee, should undertake an annual review to consider the Risk Management process, covering issues as appropriate such as:

- whether risk management continues to be linked to the achievement of the University's objectives
- the appropriate risk appetite or level of exposure for the University as a whole
- whether risk review procedures cover fundamental reputational, governance, staff, research, teaching, operational, compliance, student experience, estates, financial and other risks to achieve the University's objectives
- whether risk assessment and risk-based internal control are embedded in ongoing operations and form part of its culture
- changes in the nature and extent of fundamental risks and the University's ability to respond to changes in its internal and external environment since the last assessment
- the effectiveness of the overall approach and policy to risk management and whether changes or improvements to processes and procedures are necessary.

Definitions

a. Gross likelihood – the probability/likelihood of the level of risk being realised **before** internal controls/mitigating actions have been applied/implemented, i.e. how likely is it that the risk will happen (Scale of 1-6)

b. Gross impact – the severity/impact/consequences of the risk if it were to be realised **before** internal controls/mitigating actions have been applied/implemented, i.e. if the risk happens how would you rate the impact/consequences (Scale of 1-6)

c. Net likelihood – the probability/likelihood of the level of risk being realised **after** any internal controls/mitigating actions have been applied/implemented, i.e. how likely is it that the risk will happen (Scale of 1-6)

d. Net impact – the severity/impact/consequences of the risk if it were to be realised **after** internal controls/mitigating actions have been applied/implemented, i.e. if the risk happens how would you rate the impact/consequences (Scale of 1-6)

The University has set criteria for likelihood and impact to aid risk owners / facilitators in scoring their risks. These are attached at Annex A.

Revised March 2015

Annex A: Criteria for scoring Risks

Score	1	2	3	4	5	6
Impact	**Insignificant**	**Minor**	**Moderate**	**Significant**	**Major**	**Catastrophic**
General Description	Negligible impact upon achieving objective. The consequences are dealt with by routine operations.	Minor impact on objective. Consequences threaten the efficiency or effectiveness of some services. This will be dealt with internally.	Moderate impact on objective. The consequences would not threaten the provision of key services, but would have a medium term impact meaning the organisation could be subject to a significant review or change in operating procedures.	Significant impact upon objective. Threat to meeting external standards. The consequences may threaten continued effective provision of services and require top-level management intervention.	Major impact upon objective. No longer meets external standards. The consequences would threaten continued effective provision of services and require top-level management intervention.	Catastrophic impact on objectives. The consequences would affect the long term provision of key services, causing major problems for the organisation, and threatening its existence.
Finance	< £10,000	Loss of more than 1% Turnover £3m loss for University; £0.3m for a College	Loss of more than 2.5% Turnover £7.5m loss for University; 750k for a College	Loss of more than 6% Turnover £18m loss for University; £1.5m for a College	Loss of more than 15% Turnover. £30m loss for University; £6.5m for a College	Loss of more than 20% Turnover £60m loss for University; £10m for a College
Services	Some service interruption but can be made up without students becoming aware. No supply chain disruption.	Small fall in service levels, some minor quality standards not met. Or minor disruption to supply chain.	Moderate fall in service levels. Student and/or supplier relationships strained. Project & grant delays. Quality requirements partly met. Or limited disruption to key supply chain.	Significant fall in service levels. Project & grant requirements not achieved. Quality specifications not met. Students go elsewhere. Or significant disruption to key supply chain	Major fall in service levels. Major loss or reduction in quality of: research outputs & grant values, achievement of 1st degrees, student satisfaction & employability, international students. Or major failure of key supplier.	Catastrophic fall in service levels. Catastrophic loss or reduction in quality of: research outputs & grant values, achievement of 1st degrees, student satisfaction & employability, international students. Or catastrophic failure of key supplier.

Health and Safety	Minor injury or illness, first aid treatment needed.	Major injury requiring medical attention and/or causing >3days absence (i.e. RIDDOR reportable)	Single major injury, or long term incapacity / disability	A number of major injuries, or long term incapacity / disability, localised disease outbreak.	Incidents of death or major permanent incapacity, widespread disease outbreak.	Negligence resulting in multiple incidents of death or major permanent incapacity, regional/national disease/chemical outbreak.
Reputation	No community response. No media interest. No Reputational impact	Low consequence politically. Local short term media interest. Isolated community complaints. Reputation contained.	Some community complaints. Possible local long term media interest and / or correspondence with VC's office. Some reputational damage.	Significant complaints. National short term media interest and/or VC has been questioned. Loss of credibility- Real reputational damage.	Major complaints. National short term media interest and/or Ministry Office have been questioned. Major loss of credibility- Major reputational damage	Parliamentary questions with National long term media interest. Catastrophic reputational damage

Likelihood Rating	Definition	Guidance
1	Remote	Remote probability (<1%) the risk will occur in the next 5 Years. It may occur only in exceptional circumstances.
2	Rare	Very low probability (1-10%) the risk will occur in the next 5 Years
3	Unlikely to happen	Low probability (10-30%) the risks will occur in the next 5 Years
4	Possible to happen	Moderate probability (31-60%) the risk will occur in the next 5 Years. Might occur at some time.
5	Likely to happen	High probability (61-90%) the risk will occur in the next 5 Years. It will occur in most circumstances
6	Almost Certain to happen	Very high probability (>90%) the risk will occur in the next 5 Years. It is expected to occur.