RISK MANAGEMENT POLICY

Introduction

This Policy sets out the University's objectives and strategy for risk management, and the arrangements it has adopted to enable it to manage its risks.

Objectives

The University's objectives for risk management are:

a) to align risk management with the University's objectives (as set out in the Strategic Plan and elsewhere);

b) to appraise and manage risks and opportunities in a systematic, structured and timely manner, in accordance with best practice;

c) to strengthen decision-making, prioritisation and planning;

d) to achieve the appropriate balance between stability and innovation; and

e) to assign accountability and responsibility for risk within the University.

Scope

This Policy and associated explanatory guidance has been adopted by Council and applies throughout the University apart from Oxford University Press, which has its own policy and procedures for risk management. This policy also applies in full to wholly-owned subsidiary companies unless separate policies have been formally approved and adopted by the Boards of those companies and endorsed by the Council's General Purposes Committee.

Standards

The University follows best practice in the management of risk. The University is mindful of both international standards on risk management, and guidance from HEFCE and other relevant sector bodies[1].

[1] ISO 31000 and guidance from HEFCE, www.hefce.ac.uk/reg/

Definitions

Risk is defined as 'the effect of uncertainty on objectives'. This may also be expressed as a deviation from expected outcomes that could be positive (opportunity) or negative (threat).

Risk management is defined as 'co-ordinated activities to direct and control an organisation with regard to risk'.

Risk appetite is defined as 'the amount of risk that an organisation is willing to pursue or retain'.

A ***risk management framework*** is defined as 'a set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation'. The standards also note[2]: that a risk management framework would be expected to include policy, objectives, mandate and commitment to manage risk; together with plans, accountabilities, resources, processes and activities for risk management.

These definitions are specified in international standards ISO Guide 73:2009 and reflected in ISO 31000:2009. Further definition of terms, together with explanatory guidance on their interpretation and application, is provided separately on the University web-site[3].

[2] Specifically, notes 1 – 3 of the ISO Guide 73 definition of 'risk management framework'.
[3] www.admin.ox.ac.uk/councilsec/

Risk appetite

The University's statement of risk appetite sets out the overarching principles that define its appetite for risk, and guides the University's approach to the acceptance of risk.

University statement of risk appetite

In pursuing its objectives, as expressed in its Strategic Plan and elsewhere, the University will generally accept a level of risk proportionate to the expected benefits to be gained, and the scale or likelihood of damage.

The University has a high appetite for risk in the context of encouraging and promoting critical enquiry, academic freedom, freedom of expression, and open debate.

The University has a very low appetite for risk where there is a likelihood of significant and lasting reputational damage; significant and lasting damage to its provision of world-class research or teaching; significant financial loss or significant negative variations to financial plans; loss of life or harm to students, staff, collaborators, partners or visitors; or illegal or unethical activity.

Risk registers and risk management reports

It is acknowledged that risks will vary widely across the University, and that divisions, departments, faculties and other units will expect to retain the flexibility to manage risk in a manner appropriate to each unit. The University's risk management approach therefore allows risk management tools and techniques to be adapted to suit the needs of different parts of the University. Template risk registers and risk management reports will be provided to encourage consistency in the treatment of risk; facilitate the comparison of risk across different parts of the University; and, where appropriate, enable aggregation of operational assessments of risk into a single University-wide view.

Risk registers – a structured means of identifying and classifying risk in a consistent and coherent manner, and for assigning risk ownership. Risk registers are held by committees, faculties, departments, divisions and other academic and service units of the University. The University's Strategic Risk Register is a summary of the key risks facing the University as a whole, and is the document used by Council to manage risk.

Risk management reports – a structured approach to managing risk, considering risk appetite, and recording controls, mitigation and the current and future status of the risk. Risk management reports provide a means by which to monitor the management of risks in the Strategic Risk Register and other risk registers, setting out detail of the particular risk and the controls that are in place to mitigate the risk. Risk management reports also contain commentary from the owners of each risk, thereby providing a means by which the body responsible for risk management can ensure the risk owners are taking appropriate action to manage the risk.

Template risk registers and risk management reports will be published on the University's website[4].

[4] www.admin.ox.ac.uk/councilsec/

Responsibilities

Council is responsible, under Statutes and Regulations, for the advancement of the University's objects, for its administration, and for the management of its finances and property[5]. It will receive regular reports on strategic risks, and will seek assurances over risk management and controls from individuals identified as accountable for risks. It will make an active contribution to management by challenging accountable individuals. It will define and keep under review the University's risk appetite.

Council delegates to the **General Purposes Committee** ('GPC') responsibility to keep under review procedures for identifying and managing risks across the University's activities[6]. In discharging these responsibilities GPC will also advise Council on any recommendations to amend this Policy. GPC is also the forum in which matters relating to risk that cannot be adequately resolved elsewhere are determined. In order to discharge its responsibility for procedures for identifying risks across the University's activities, GPC will review and update regularly the University's strategic risk register. GPC will consider the strategic risks identified by the academic and service divisions, the major Committees of Council, and other bodies, as appropriate. These divisional and Committee risk registers will have been informed by the risk registers of departments, faculties and other academic and service units of the University. In order to discharge its responsibility for managing risks, GPC will review risk management reports relating to each of the key risks on the University's Strategic Risk Register.

The **Vice-Chancellor** is accountable to HEFCE for discharging the University's responsibilities for effective risk management, as set out in the annual Accounts Direction to Higher Education Institutions[7].

The **Audit and Scrutiny Committee** provides an annual opinion to Council on the adequacy and effectiveness of the University's arrangements for risk management.

The **internal auditors** undertake audit work sufficient to allow them to provide an annual opinion to the Audit and Scrutiny Committee on the adequacy and effectiveness of the University's arrangements for risk management.

The **Risk Advisory Group** is responsible for advising GPC on the University's risk management process, being the procedures, guidance and training provided to staff to facilitate the embedding of risk management into the culture of the University.

The **Registrar** is responsible for:

a) ensuring that this Policy is implemented and maintained;

b) providing appropriate levels of explanatory guidance and training to support this Policy;

c) defining and implementing procedures for the reporting and escalation of risk to GPC, Council and other University bodies as required;

d) raising awareness of this Policy and its objectives, standards and statements amongst staff and all others to whom it is relevant.

---

[5] Statute VI: www.admin.ox.ac.uk/statutes/783-121.shtml

[6] Part 3 of Council Regulation 15, 2002.

[7] www.hefce.ac.uk/pubs/year/2014/CL,252014/

Heads of Division, Heads of Department, Faculty Board Chairs and Heads of University Services (ASUC and UAS) are responsible for:

a) ensuring that this Policy is implemented and followed in their respective divisions, departments, faculties and sections (as appropriate);

b) ensuring that staff within these areas are made aware of this Policy, associated explanatory guidance, and any requirements that the Policy places upon them or their activities.

The **Boards of Directors** of wholly-owned subsidiary companies of the University are deemed to have responsibilities equivalent to Heads of Division as set out above unless alternate arrangements have been agreed and approved by GPC.

Every member of staff is responsible for familiarising themselves with this Policy, in particular any aspects that have a direct bearing upon the role that they perform for the University.

Interaction with other policies, procedures and regulation

This Policy interacts and overlaps with a number of other University policies and procedures, including but not limited to:

- Financial Regulations and supporting Financial Processes including, in particular; insurance;
- Health and Safety Policy and associated Regulations and Codes;
- Research Integrity and Ethics;
- Bribery and Fraud Policy;
- Information Security Policy and associated controls relating to IT risk.

This Policy also takes account of the University's wider legislative obligations as they relate to risk management, including the Financial Memorandum with HEFCE and the Audit Code of Practice[8].

Interaction with third parties

In order to achieve its objectives, the University works closely with a number of third parties, including the colleges, the PPHs and the NHS. Some risks, therefore, are shared with these third parties.

Whilst GPC will retain an overview of the University's strategic relationships, where divisions and departments have significant interaction with third parties, it is the responsibility of the Head of Division or Head of Department (as appropriate) to ensure that adequate steps are taken to manage shared risks effectively.

[8] www.admin.ox.ac.uk/councilsec/

Further guidance

Further guidance, including explanation, interpretation and definition of terminology used is provided separately on the University web-site[9].

[9] www.admin.ox.ac.uk/councilsec /