



UNIVERSITY OF STIRLING

RISK MANAGEMENT POLICY

June 2015

Contents

1. Introduction
2. Purpose
3. What is risk?
4. What is risk management?
5. The University's approach
6. Responsibilities
7. Defining the risk appetite
8. Management of risk
9. Annual review of effectiveness

1. Introduction

The University faces numerous risks that could affect any aspect of its academic, administrative or commercial business activities. Sound risk management is therefore required to ensure the University is able to achieve its operational aims and strategic objectives.

The University considers risk management to be fundamental to good management practice and a significant aspect of corporate governance. Risks include not only threats facing the University, but also a failure to seize opportunities. An assessment of risk must therefore be conducted to identify, analyse and report to the most appropriate management level within the University.

It should be noted that risk management is the responsibility of everyone at the University, not just a small number of named individuals. The University maintains a register of strategic risks, and all academic schools and service areas maintain operational risk registers that are integrated into the planning and budgeting process.

2. Purpose

This risk management policy identifies the underlying approach to risk management across the University. It defines the roles and responsibilities of senior managers and governing bodies together with the annual mechanism for reviewing risk management processes. The policy is informed by the good practice guide for higher education institutions published by the Higher Education Funding Council for England¹.

The purpose of this policy is a formal acknowledgement of the commitment made by the University to risk management. The University considers that taking well-managed risks is essential to the success of higher education, in the management of its core activities of research and teaching, as well as its supporting activities. The aim of the policy is not eliminate risk from the University's activities, but rather to manage risk appropriately.

This document is supported by a concise risk management policy statement that is published online as a quick reference guide for all staff (Appendix 1).

3. What is risk?

Risk is commonly defined as the possibility that an action, event or set of circumstances will adversely or beneficially affect an organisation's ability to achieve its objectives.

Risk exists as a consequence of uncertainty and is present in all University activities. The exposure is normally expressed in terms of the failure to reach an objective and the operational, reputational and financial damage that may be incurred as a result.

4. What is risk management?

Risk management is the planned and systematic approach to identifying, evaluating and controlling risks at all levels of the organisation.

5. The University's approach

The University's approach to risk management is guided by the following principles:

- the University Court has responsibility for the effectiveness of internal controls based on information provided by Audit Committee
- risk management is implemented as an integral part of University activities at all levels and is monitored by the Audit Committee

¹ *Risk Management: A guide to good practice for higher education institutions, HEFCE, May01/28*

- risks are identified, analysed and recorded as appropriate, normally within a risk register that scores the likelihood and impact of risks
- the management of risk will involve user-friendly language and University processes will be kept as simple and effective as possible
- the financial and non-financial implications arising from risks and associated controls will be estimated as accurately as possible
- the University Strategy and Policy Group (USPG) will support, advise and implement risk management processes and will act as a risk management committee when required
- risk will be a standing item at meetings of the Senior Management Team (SMT), and heads of academic schools and service directors will be responsible for embedding good risk management practice within their school or service area.

The University uses five steps to manage risks, and a common template to record and report strategic and operational risks:

Step 1 – Identifying risks

The identification and review of risks takes place throughout the year and is a formal part of the planning and budgeting cycle. Each management group is encouraged to carry out ongoing reviews and updates of the linkages between strategic objectives and risks to ensure that focus is maintained on priority activities.

Strategic risks typically affect the whole of an organisation and not just one or more of its parts. Because of this, strategic risks are recorded and monitored at an institutional level and form a key part of strategic management. Operational risks refer to issues arising from the normal business operations. Accordingly, they affect the day-to-day running of the University in contrast to strategic risks that arise from the organisation's strategic positioning. Operational risks are typically managed at school or service level and can be managed and mitigated by internal control systems.

Step 2 – Analysing the risk

The University uses a risk model to measure the likelihood and impact of individual risks identified in operational or strategic registers. Impact is the potential severity or effect of the risk. Likelihood is the frequency or probability of a risk occurring. The risk score is calculated using the impact and likelihood to produce an evaluation of net risk that can be translated into a traffic light system.

Step 3 – Determining the risk owner

Strategic and operational risks should be assigned to a risk owner, who is responsible for managing the risk and associated control measures.

Step 4 – Identifying control measures

The identification of control measures will depend on the treatment category of the risk at residual level. The University uses the 4Ts to categorise risk:

- Tolerate – risks are accepted and built into operational or project management
- Treat – risks are reduced by management action (e.g. putting in place a business continuity plan)

- Transfer – risks are passed on to another organisation or body (e.g. outsourcing, insurance or subcontracting)
- Terminate – risks are avoided by doing something else

Actions to mitigate or control a risk will have a direct cost or an opportunity cost that should be recorded in the risk register. The risk should be reassessed to identify the impact of any action on the net risk. The result of any control measure is known as the residual risk.

Step 5 – Reviewing the risk

Risks should be reviewed on a regular basis to ensure that strategic and operational registers are kept up-to-date. At a University level, the register of strategic risk is reviewed and discussed at each meeting of Audit Committee.

6. Risk responsibilities

It is essential that all participants in risk management are aware of their roles in the overall process and their own responsibilities. The key responsibilities are outlined below:

University Court

The Court has a fundamental role to play in the management of risk and in setting an overall culture of risk management within the University. This includes:

- determining and reviewing the risk appetite of the University as a whole, and agreeing a risk appetite statement that is reviewed annually
- approving major decisions affecting the University's risk profile or exposure
- determining what types of risk are acceptable or not acceptable

Audit Committee

Acting on behalf of Court, Audit Committee will:

- monitor the management of key strategic risks
- satisfy itself that less significant risks are being actively managed, with the appropriate controls in place and working effectively
- annually review the University's approach to risk management, and approve changes or improvements to key elements of its processes and procedures
- approve the internal audit plan which is linked to the Strategic Risk Register
- report to Court on the effectiveness of risk management processes as appropriate

Executive Group

The University Strategy and Policy Group (USPG) is responsible for strategic risks by:

- identifying and evaluating significant risks faced by the University for consideration by Court, via Audit Committee
- implementing policies on risk management and internal control

- providing adequate information in a timely manner to Court, via Audit Committee, on the status of risks and control measures
- regularly reviewing the effectiveness of internal controls
- identifying and acting as risk owner for appropriate strategic risks

Senior Management Team (SMT)

Heads of school and service directors are responsible for identifying, assessing and monitoring risks at school and service level. They will:

- disseminate good and appropriate risk practice within their school/service
- identify, monitor and assess risk issues within their school/service
- monitor and discuss risk as a standing item on the agenda of SMT
- report on risk and control issues in their annual Planning Statement, and review regularly as appropriate
- alert the risk management committee (USPG) to risks which may have strategic importance

Staff and students

Effective risk management depends on the commitment and co-operation of all staff and students. All staff have a significant role in the management of risk, particularly within their own areas of control. Project managers and project teams are responsible for managing project-specific risk and will complete a project risk register to demonstrate that this is being done.

7. Defining the risk appetite

The University Court determines the extent to which the University is “risk-taking” or “risk-averse”. The evaluation of the University’s strategic risks via Audit Committee provides a regular review of the University’s risk tolerance line.

8. Management of risk

The management of risk is supported by a system of internal control, and is closely related to the planning and budgeting process and institutional performance management. This enables the University to respond to a variety of operational, financial, reputational and commercial risks. The elements of this system include:

Policies and procedures

Attached to significant risks are a series of policies that underpin the internal control process. These policies are approved by Court and are supported by written procedures where appropriate.

Reporting

Strategic risks are reported regularly to Audit Committee via the risk register or on an ‘exception’ basis as required, for example, on risks associated with new projects, or on emergent external risks.

Planning and Budgeting

The annual planning and budgeting process is used to set objectives, agree action plans and allocate resources. Schools and service areas are responsible for updating their planning

statements and associated risk registers and performance measures as part of this process. Progress towards meeting planned objectives is monitored regularly by the senior management team.

Risk Framework

The register of strategic risks is reviewed by the risk management committee (USPG) and is used to identify, assess and monitor risks significant to the University. Improvement actions and risk indicators are monitored regularly.

Audit Committee

Audit Committee is required to report to Court on internal controls and inform Court about any emerging issues. In addition, Audit Committee oversees internal audit, external audit and management as required in its review of internal controls. Audit Committee will advise Court on the effectiveness of the risk management and internal control systems.

Internal audit

Internal audit is responsible for aspects of the annual review of the effectiveness of the internal control system within the University. The internal audit strategy will be developed around the University's strategic objectives and is informed by the register of strategic risk.

External audit

External audit informs the Audit Committee on the operation of internal financial controls reviewed as part of the annual audit. *However, external audit is not part of the risk management process.*

Third Party Reports

From time to time, the use of external consultants may be appropriate in areas such as health and safety (e.g. radiation protection adviser), and human resources. The use of specialist third parties for consulting and reporting can, in some cases, increase the reliability of the internal control system.

Operational Risk and Environmental Sustainability (OR & ES)

The University has access to competent safety advice through the Head of OR & ES, who advises the University on aspects of health and safety management and business continuity. The Head of OR & ES reports operationally to the Director of Estates and Campus Services, but also has a reporting line to the University Secretary. Overall responsibility for ensuring that the University complies with health and safety legislation lies with the University Court.

Policy and Planning

The Policy and Planning team compiles risk issues, supports University staff in the assessment and management of risk, and reports emergent strategic risks as appropriate. The team also reviews operational risk registers from schools and service areas, identifies training needs and identifies emergent risks to be included within the register of strategic risk.

9. Annual Review of Effectiveness

The University Court is responsible for reviewing the effectiveness of internal control of the University, based on information provided by Audit Committee. In doing this, Court will consider the following:

- The University's objectives and its financial and non-financial targets
- The University's performance in identifying, assessing and reporting risks
- Prioritisation of risks and the allocation of resources to areas of high exposure

- Effectiveness of control measures

Audit Committee, on behalf of University Court, will review the risk register and this policy document to ensure on-going effectiveness in the management of risk.

Policy and Planning

May 2015