UNIVERSITY of York

Risk Management Policy, Strategy and Assurance Framework

Version 3 June 2014

Contents

1. Introduction 3
Risk Management Overview 3
Benefits of Risk Management 3
2. Risk Management Policy Statement 3
3. Approach to Risk Management 4
Risk Management Objectives 4
Risk Management Vision 4
Risk Management Culture 5
Risk Management Structure 5
4. Risk Assessment – Definitions 5
Likelihood and impact 5
Mitigating actions 6
Residual Risk 6
Risk Appetite 6
5. Scoring Risk Assessment 7
6. Assurance Strategy 7
Corporate risk 7
Departmental risk 8
Project risk 8
Governance statement 8
Appendix 1- Definition of impact and likelihood 9
Appendix 2 – Annual Cycle of Reporting (updated March 2014) 10

1. Introduction

1.1 This document sets out the University of York's approach to risk management.

Risk Management Overview

1.2 The University is committed to achieving its aims as defined in the University Plan and associated documents. In doing so, the University realises that it will face a variety of risks.

1.3 Risk is regarded as a quantifiable level of exposure to the threat of an event or action that will adversely affect the University's ability to achieve its business objectives successfully. In simple terms, risk is 'uncertainty'. The task of management is to respond to these risks effectively so as to maximise the likelihood of the University achieving its purposes and ensure the best use of finance and resources.

Benefits of Risk Management

1.4 Some risk taking will always be necessary. To inform the risk taking, the University will take a measured approach to risk management that enables:

- an understanding of the level of risk exposure that can be tolerated
- an understanding of the type of risks faced and how to measure them
- where the level of risk exposure is too high that a suitable level of mitigation exists
- the on-going assessment of the effectiveness of mitigation
- prompt action where existing arrangements are found to be inadequate or ineffective
- an awareness of risk at all levels of the University to ensure that risks can be escalated to a level of management that can effectively respond to them.

1.5 The establishment of effective risk management is recognised as being fundamental in ensuring good corporate governance. Thus, these arrangements are endorsed and upheld by the Council through the implementation of cyclical risk management reporting and monitoring regimes. These arrangements are intended to be both robust and transparent, underpinning the production of the annual Governance Statement (see para. 6.10).

1.6 The University internal auditors utilise the information contained in the risk registers to formulate an effective annual audit plan.

2. Risk Management Policy Statement

2.1 The Council is committed to ensuring that the management of risk underpins all business activities of the organisation and that thorough risk management procedures are in place throughout the University.

2.2 The application of this policy and strategy will enable the University to obtain, maintain and respond to a changing risk profile.

2.3 Notwithstanding the above, the Council recognises that the application of risk management practices should not and will not eliminate all risk exposure. Moreover, through the application of the risk management approach identified in this policy and strategy we aim to achieve a better understanding of the risks being faced and their implications for the business, thus informing decision-making.

2.4 Because risk can never be eliminated fully it is vital that the University has in place plans to ensure business recovery and continuity in the event that serious risks do occur. As such the University's business continuity management process forms an integrated part of its risk management process.

2.5 The Council expects management to take action to avoid or, where appropriate, mitigate the effects of those risks that are considered to be in excess of the University's risk appetite. Where a risk is deemed to be in excess of the University's risk appetite this will be captured on the University's corporate risk register, along with the actions being undertaken to address the risk.

2.6 The active, ongoing commitment and full support of the Vice-Chancellor and the senior management group is a necessary and essential part of this policy. The Council, management and other staff will establish, maintain and support the Risk Management Strategy and ensure that effective mechanisms are in place for assessing and responding to any issues arising.

2.7 All employees are expected to have an understanding of the nature of risk within the University and those acting on behalf of the University must further accept responsibility for risks associated with their activities.

3. Approach to Risk Management

Risk Management Objectives

3.1 To assist in the management of business risk the following objectives have been identified. These form the basis of the University's Risk Management Strategy:

- Promote awareness of business risk and embed the approach to its management throughout the organisation

- Seek to identify, measure, control and report on any business risk that will undermine the achievement of the University's business priorities, both strategically and operationally, through appropriate assessment criteria

Risk Management Vision

3.2 The University will seek to identify the risk and its cause at the earliest opportunity and measure the risk effect on the institution. Wherever practicable, it will seek to apply a proportionate level of resources to control the risks in order to maximise the quality of its service provision and avoid reputational damage.

3.3 Furthermore, the University will seek to obtain assurance that the controls relied on relied on to mitigate the key risks are effective. An assurance framework has been developed to support the ongoing monitoring of controls (see Section 6).

Risk Management Culture

3.4 The Council recognises the value of adopting a risk management culture. Consequently, it will:

- review the Corporate Strategy and Corporate risk register on an annual basis;
- nominate the Registrar & Secretary and the Director of Finance jointly to promote the risk management function and ensure its effectiveness across the organisation;

Require the Vice-Chancellor and Senior Management to:

- implement and monitor risk management arrangements across the organisation at all levels;
- establish a rolling programme of risk assessment and incorporate risk management in the business planning process at all levels;
- encourage all senior managers, staff, partners, suppliers, and other stakeholders to develop and maintain a risk management ethic and to report concerns accordingly.
- ensure that designated individuals receive the necessary training, ongoing support and advice in connection with risk management

Risk Management Structure

3.5 To ensure that the University has a full understanding of the risks being faced and the implications for the business, risks will be identified and assessed at three levels, Corporate, Departmental and Project.

3.6 To ensure a consistent understanding across the organisation the definitions for the levels of risk being captured at the University are:

Corporate: Those business risks that, if realised, could have a significant detrimental effect on the University's key business processes, activities, governance or reputation. The risk realisation may lead to inefficiency, ineffectiveness, loss of opportunity, compliance issues arising from legal/ regulatory environment or harm to institutional reputation.

Departmental: Those business risks that, if realised, could have a significant detrimental effect on a department or directorate's key business processes, activities or reputation. The risk realisation may lead to inefficiency, ineffectiveness, loss of opportunity or harm to reputation

Project: Those business risks that, if realised, could have a significant detrimental effect on the outcome of a project.

4. Risk Assessment – Definitions

Likelihood and impact

4.1 Likelihood is defined as the probability of the realisation of a risk.

4.2 Impact is defined as the effect of a risk if it is realised.

Mitigating actions

4.3 These are the mechanisms and arrangements that are in place within the University to either reduce the likelihood of occurrence of the risk or minimise the impact of the risk if it does occur. An internal control system encompasses the policies, processes, tasks, behaviours and other aspects of the University that, taken together:

- facilitate its effective and efficient operation by enabling it to respond appropriately to significant business risks. This includes the safeguarding of assets from inappropriate use or from loss and fraud, and ensuring that liabilities are identified and managed;

- help to ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information; and

- help to ensure compliance with applicable laws and regulations, and also with internal policies.

Residual Risk

4.4 The residual risk is defined as the risk that remains even taking account of the relevant mitigations.

Risk Appetite

4.5 The University recognises that its risk appetite will change continuously over time as a response to changing circumstances. Moreover it is not possible to quantify a single, overall risk appetite. Rather at a given point in time the University will be willing to accept additional risk in some areas (in order to achieve additional returns) and will be seeking to reduce risk in other areas. Therefore the risk appetite of the University will be described by specifying the different key areas in which it is desirable to increase or decrease risk. The statement of risk appetite will be kept under review and updated as necessary.

The University's whole-of-institution appetite for risk in the following areas is:

- Reputation, quality, integrity, stakeholder and student responsibilities

The University's appetite for risks affecting its academic quality and integrity, research, students, stakeholders and reputation is **limited** (low) - it will not compromise its reputation and values by either short term or long term expediency.

- Physical and electronic resources, infrastructure and business disruption

The University's risk appetite is **limited** (low) with respect to the operation of key university systems and services. These systems are understood to underpin the ongoing delivery of critical services to a scale, scope and quality necessary for the University to compete in a rapidly changing environment.

- Strategic, financial viability and safeguards

The University's appetite for financial and strategic risk is **modest** (medium) - it recognises its financial viability as being critical to its future. Financial viability risks and rewards are to be weighed against both short and long term strategic and operational priorities.

- Corporate and academic governance issues

Within these risk categories, the University's risk appetite is **limited** (low). The University seeks to comply with relevant statutory requirements and contractual obligations to the best of its endeavours. This statement is made with the understanding that the seriousness of particular compliance requirements may vary depending upon the relationship of the requirement with the risk areas listed above. The University will look to satisfy compliance requirements in the simplest and most effective way possible.

Whilst the overall University risk appetite is limited, the risk levels adopted in individual departments may be higher to support the institutional strategic objectives. It is recognised that the University also expects academic departments to be innovative and to take calculated risks, for example in experimental research.

5. Scoring Risk Assessment

5.1 The University of York will adopt a scale of 1 to 3 to measure likelihood and impact. The most significant risks will be identified by multiplying likelihood by impact.

Likelihood		**Impact**		**Overall Rating**	
High	3	High	3	Red risks:	5-9
Medium	2	Medium	2	Amber risks:	3-4
Low	1	Low	1	Green risks:	1-2

Appendix 1 contains more details on the definitions of impact and likelihood

6. Assurance Strategy

6.1 The purpose of the Assurance Strategy is to ensure that key risks and their owners are clearly identified, that mitigation and specified actions are appropriate and that the actions are being carried out.

Corporate risk

6.2 The University of York will maintain and regularly review and update a corporate register of key risks facing the University. This will be recorded in both a Detailed and Summary format.

6.3 Responsibility for updating the corporate risk register will lie with the Registrar & Secretary. The Director of Finance will take lead responsibility for monitoring financial risks and ensuring that associated actions are implemented.

6.4 SMG will receive the summarised version of the corporate risk register on a monthly basis. Operations Group will receive the detailed version of the register on a termly basis. The Operations Group discussions will provide an opportunity for identification and assessment of possible new risks. The Operations Group will also keep the statement of risk appetite under review.

6.5 The Audit Committee will review the summary and detailed corporate risk registers twice a year and will receive an annual report on risk from the internal auditors. The Audit Committee will also consider input from other sources of assurance, including the external audit.

6.6 The Audit Committee will submit a written report to the Council, including an updated version of the corporate risk register.

Departmental risk

6.7 Academic departments and support services will review risks and actions in mitigation of risk on a termly basis as an integrated part of the Medium-Term Planning process.

6.8 The Director of Corporate Planning will ensure that risks identified at departmental level which may have a wider impact are considered in the course of reviews of the corporate risk register by Operations Group.

Project risk

6.9 Risks associated with projects will be reviewed by the Planning Committee or other committee depending on the nature of the project. The Registrar & Secretary and Director of Corporate Planning will ensure that risks identified at the project approval stages which may have wider impact are considered in the course of reviews of the corporate risk register.

Governance statement

6.10 These processes will underpin the production of the annual Governance Statement. The Governance Statement forms part of the Annual Report of the Council and is included in the University of York's Financial Statements. The Governance Statement is a public report that confirms the on-going effectiveness of the internal control environment in the management of risk, both financial and non-financial. The production of a "fair and representative" Governance Statement is an essential part of the University of York's corporate governance framework.

Appendix 1- Definition of impact and likelihood

Impact area	Low	Medium	High
Financial*	£50k to £250k impact on bottom line	£250k to £500k impact on bottom line	£500k or greater impact on bottom line
Health & Safety	HSE Reportable injury, disease or dangerous occurrence.	Serious injury (loss of limbs, sight etc) with long term consequences for those injured	Fatalities and/or prosecution by the HSE.
Reputation	Significant adverse publicity in local/national media	Sustained adverse publicity in national media. Long and short term damage to reputation.	Sustained adverse media coverage at various levels. Long term damage to reputation and widespread loss of confidence in the University.
Legislative	Potentially serious legal or regulatory implications.	Very serious legal or regulatory concerns.	Legal or regulatory issue leading to inability to continue significant area of operations.
Ability to deliver services	Major disruption (typically 1 to 4 weeks). Significant management action and/or outside assistance needed to recover.	Disruption causing inability to deliver majority of services at University wide level or services of an entire department. Significant senior management involvement needed.	Immediate impact on University's ability to provide services causing total shut down of operations. Senior management involvement needed.

*These financial thresholds apply at the corporate level. Individual departments will scale down these figures in line with the size of the department when completing departmental registers.

	Low	Medium	High
Likelihood	Unlikely to occur given current circumstances (including mitigations). Approx 0% to 20% chance of occurring in the next 2 years	Reasonable chance of occurring given current circumstances (including mitigations). Approx. 20% to 50% chance of occurring in the next 2 years	More likely to occur than not in the next 2 years. i.e. probable to certain.

Appendix 2 – Annual Cycle of Reporting (updated March 2014)

Month/ Activity

October

- Audit Committee receives Internal Audit risk management report
- Audit Committee reviews the Corporate risk register
- Corporate register on SMG Agenda

November

- First review of Departmental registers by departments as part of LTP/MTP process
- Review of Corporate register by Operations Group
- Corporate register on SMG Agenda
- Audit Committee receives Internal Audit Annual Report
- Council receives Audit Committee Annual Report including risk management audit report
- Review of Corporate Register by Council

December

- Corporate register on SMG Agenda

January

- Review of Corporate register by Operations Group including report by Director of Planning on departmental risks (based on first departmental review)
- Corporate register on SMG Agenda

February

- Audit Committee receives report on Risk Management including review of departmental registers, review of Corporate Register and details of reviews by SMG and Operations Group since October
- Corporate register on SMG Agenda
- Internal Audit conduct field work for risk management audit
- Second review of departmental registers by departments, in conjunction with Medium Term Planning sign off (will occur in March for some departments)

March

- Corporate register on SMG Agenda

April

- Review of Corporate register by Operations Group including report by Director of Planning on departmental risks (based on second departmental review)
- Corporate register on SMG Agenda

May

- Review of Corporate risks by Operations Group
- Internal Audit issue Risk Management report to Registrar and it is reviewed by Operations Group
- Corporate register on SMG Agenda

June

- Corporate register on SMG Agenda

July

- Third review of departmental registers by departments incorporating up to date student recruitment information
- Corporate register on SMG Agenda

August

- Corporate register on SMG Agenda

September

- Review of Corporate register by Operations Group including report by Director of Planning on departmental risks (based on third departmental review)
- Corporate register on SMG Agenda