University of Edinburgh

Risk Management Guidance Manual

What is the purpose of this guide?

The risk management guidance manual is a reference document for use by managers to help them understand how the University deals with risk in its governance process, and to provide guidance on how they should be addressing risk within their own areas of responsibility.

Who should read this Guide?

This Guide is intended to be helpful to Heads of College and Support Groups, Heads of School, School Administrators, Senior College and Support Group managers and the heads of key administrative functions. The guide is a reference document to be referred to as need arises, for example when developing a new activity which will need analysis of the potential risks involved.

CONTENTS

1. Risk Management is easy – the concepts

Whenever an activity takes place, there will be an outcome that will either be a success or a failure. In undertaking the activity there will be a number of factors which have to be got right which will determine whether the activity is a success or not, and there are a number of risk factors which, if they are not managed properly, will result in failure rather than success.

Risk Management is fundamentally an approach designed to provide a methodical way for addressing risk.

It comprises:

- Identifying the objectives and what can go wrong – identifying the risk
- Acting to avoid it going wrong or to minimise the impact if it does – managing the risk

Risk Management operates at a number of levels.

1.1. Individual

Individuals in their day-to-day working and personal life take many decisions and undertake many activities. In the working environment, activities such as working in laboratories, with animals, on estates projects etc involve risks, particularly health and safety. Equally, control of funds in grant-funded projects must be done correctly, and research findings must be properly validated before publication otherwise personal reputations are at risk.

1.2. Operational Activity

Operational activities carry risks for the University if not undertaken properly. Policies and procedures in areas such as finance, procurement, HR, estates, communications and marketing, student services etc are designed to ensure statutory and professional compliance, as well as the avoidance of financial, staff and student mismanagement.

1.3 Change Activity

All change activities and projects have risks attached to them, whether introducing new teaching courses, changing the curriculum, implementing IT projects, changing organisational structures, developing partnerships with overseas institutions, building new facilities etc. The relevant team managing the activity or project should ensure that they understand both what key factors must be achieved to deliver success and also what could go wrong and what should be done to avoid this outcome.

1.4. Achievement of short/medium/long term organisational goals

Every organisation (University, Colleges, Schools or Support Groups) will be looking to achieve its short and longer term goals. There will be a number of key aspects that must be got right to achieve these goals, and also there will be a number of things that can go wrong. Identifying and understanding these factors will aid decision-making, resource allocation etc. which, in turn, will give the organisation a better chance of success in achieving its goals.

For risks identified there will normally be a number of actions that can be undertaken to manage, control or mitigate the risk, and there may well be contingency plans which could be invoked to manage the consequences of the risk occurring.

If risks are not properly identified and managed then for an individual or organisation the consequences can be:

- Not achieving goals and objectives
- Loss of reputation
- Financial loss
- Loss of competitiveness (e.g. against other Universities)
- Failure/take over/winding up of the organisation
- Injury, death, loss of job etc. for individual

In all organisations, risk management is now part of the governance structure. Governing bodies are expected to adopt a holistic approach to risk management that builds the simple concepts outlined above into the structures and processes of the organisation. The key elements of this best practice are:

1. The governing body establishes an overall risk policy that sets out the appetite for risk which the organisation is willing to accept and the roles and responsibilities for identifying and managing risk throughout the organisation.

2. The governing body will maintain an overall risk register, identifying the main risks to the organisation's goals and objectives. Substantial sub-organisations should also maintain a risk register.

3. Individuals will be assigned responsibility for ensuring that each key risk is being properly managed (both the risk itself, and that contingency/recovery plans are in place should the risk materialise).

4. The assessment of risks becomes a part of the decision-making process of the organisation.

5. The assessment of risk becomes an integral part of the planning and budgeting processes.

6. Risk assessment becomes part of the operational activities.

7. Managerial and internal control reflects the risks identified.

8. A Risk Management Committee is formed to inform the Governing Body of risk management issues, and to ensure the risk management processes in the organisation are operating satisfactorily and effectively.

9. Internal Audit programmes are determined by reference to the risk maturity of the organisation and the key areas of risk identified in the Risk Register(s).

10. The Governing Body establishes processes of reporting, review and audit which will enable them to satisfy themselves that throughout the organisation, key risks are being properly managed and that the internal control framework is effective.

The establishment of this holistic approach to Risk Management brings the following benefits:

- Facilitates better planning and prioritisation
- Enhances potential achievement of objectives and goals
- Reduces the chances of nasty surprises
- More informed and better decision-making
- Improved communication and knowledge sharing
- Improved allocation of resources
- Allows opportunities to be taken as risks are better understood
- Enhanced credibility in the organisation and people
- Increased responsiveness to internal and external change

Given the development of this approach over the past thirty years, initially in the private sector and now in the public sector, it is no surprise that risk management is a mandated requirement for listed companies, and is now a condition of grant funding from both HEFCE and the SFC.

The remainder of this guidance describes the risk management approach being established in the University.

2. Overview of Risk Management Processes in the University

The University wishes to achieve the benefits of a holistic risk management approach, and ensure compliance with SFC requirements. This latter requirement is that the University Court, as the duly constituted legal governing body, must make a statement in the annual published accounts to the effect that:

(a) There is an ongoing process for evaluating and managing significant risks faced by the University, and

(b) This process has been in place for the year under review and up to the date of approval of the annual report and accounts, and

(c) The University Court has satisfied itself that an effective system of internal control has been in place for the year under review.

The key elements in the overall University process for risk management are:

University level

i. The Risk Management Strategy is reviewed and confirmed by CMG, F&GPC, Audit Committee and Court each year.

ii. The University Risk Register is formally updated each year by the Risk Management Committee, then reviewed and confirmed by CMG, F&GPC, Audit Committee and Court. The University Risk Register recognises the major risks to the University as a whole, and tends to comprise the main strategic risks for the University.

iii. Any material changes to the overall risk profile of the University are notified by the Risk Management Committee to CMG, F&GPC, Audit Committee and Court as and when material changes occur.

iv. The Risk Management Committee reviews the procedures to control and manage each risk in the University Risk Register with each Lead Senior Manager on a rolling basis to confirm that processes are effective and to identify areas for improvement. The format of the review is shown in Appendix 1.

v. The Risk Management Committee will report on its activities to CMG, F&GPC, Audit Committee and Court at the end of the University's financial year. A year end risk questionnaire is completed by each College, Support Group and Subsidiary Company and a summary of the responses is incorporated into the Risk Management Committee's year end report. Similarly specific assurances on Procurement as required by the CUC Guidance manual, and assurances in support of the Letter of Representation provided by the Court to the External Auditors are also included in the RMC annual report.

vi. All papers being presented to formal committees of the University must include a section outlining the key risks related to achieving a successful outcome to the proposal where appropriate. The cover sheets include a section entitled 'Risk Assessment'.

vii. Submissions into the University's annual planning process must include a section outlining the key risks to delivery of the proposals and the medium term plans. The proposed plans should be cross-checked against the University/College/Support Group risk registers to ensure the planning proposals reflect the appropriate risk management activities, and resources are adequately allocated to key risk areas.

viii. Certain committees may also wish to develop a Risk Register identifying the key risks in delivering their role and objectives, which can then be used to assist agenda setting, decision-making or action priorities.

ix. Internal Audit will review the operation of risk management processes in the University and report findings to the Risk Management Committee and Audit Committee. In addition, Internal Audit assesses the risk maturity of the University and develop its work programmes to ensure areas of significant risk are audited. This supports the Audit Committee and Court in being able to provide the required statements and assurances in the published Annual Accounts.

College/Support Group level

x. Each College, Support Group, and Subsidiary Company will maintain a Risk Register which should be formally reviewed annually by the relevant College/Support Group Senior Management Team. Copies of the College/Support Group Risk Registers are reviewed by the University Risk Management Committee. Each College and Support Group should decide which organisational level is appropriate to identify risks, and manage them.

xi. The Senior Management Team should satisfy itself that all risks identified are being effectively and satisfactorily managed. This will involve identifying individuals to take overall responsibility for ensuring each risk is managed, and that contingency plans are established as appropriate. They should review the controls and improvement activities proposed.

xii. The Senior Management Team should be notified of any new or changing risk as and when it arises, and they should satisfy themselves that appropriate actions are taken to manage the new situation. The change in risk should be notified to the University Risk Management Committee.

xiii. A project risk register, reflecting the project's objectives, should be established for each project, development or change activity. This should be regularly reviewed by the relevant steering/management group throughout the project. Actions are to be taken to mitigate the risks identified and thereby improve the likelihood of success.

xiv. College/School/Support Group Annual Planning documents should identify key risks to the delivery of the proposed plans. They should also be cross-checked to the relevant Risk Register to ensure that plans, objectives and resource proposals reflect the actions required to ensure key risks are being appropriately managed.

xv. Each College/Support Group/Subsidiary Company is required to complete a Risk Questionnaire at the end of the University's financial year which includes a statement indicating that the College/Support Group is satisfied that risks are being appropriately identified and managed. This is required so that assurances can be given to the University Court in support of the statements it is required to make in the Annual Financial Statements.

3. University Risk Management Strategy

The University Risk Management strategy can be found at
http://www.docs.sasg.ed.ac.uk/GaSP/Governance/RiskManagement/RiskManagementStrategy.pdf

4. Risk Registers – University/College/School/Support Group/Subsidiary

A Risk Register provides an overview of

(a) The key risks to the organisation – those that put in jeopardy the delivery of its medium/long term objectives, or its ongoing survival.

(b) The consequences of the risks materialising.

(c) The impact and likelihood of the risk materialising.

(d) The management and control mechanisms to manage and mitigate the risk, and the contingency arrangements if applicable that would be invoked should the risk materialise.

(e) The nominated person who takes responsibility for ensuring that the management and control arrangements are in place, operating satisfactorily, and are being improved.

(f) A brief statement of the further action necessary to minimise risk event occurring and/or to mitigate its effects.

The Risk Register should be put together by members of relevant organisations, but must be owned and agreed by the Senior Management Team. In the case of the University, this is Court, with prior approval of CMG, the Audit Committee and the Finance and General Purposes Committee. In the case of Colleges and Support Groups, it will be the Senior Management Team. For subsidiary companies it will be the directors of the company.

The processes for developing and updating the risk register are

(i) Identify the objectives for the organisation or operational area.

(ii) Identify risks and consequences, likelihood and impact – brainstorming, discussion etc.

(iii) Identify the management control mechanisms, other potential mitigating strategies and the nominated manager (risk owner).

Following development of the Risk Register

(a) Each nominated manager should review the management and control mechanisms for the relevant risk and satisfy themselves that the mechanisms are operating effectively, and identify any areas where new mechanisms or improvements need to be implemented. This will need to be reported back to the Senior Management Team, and will be an annual requirement. The format used for risk reviews in Risk Management Committee is at Appendix 1.

(b) Any new risks which arise over the course of time or any change to existing risks should be notified to the Senior Management Team who should decide whether the Risk Register should be amended. At University level, the Risk Management Committee maintain a log of emerging risks throughout the year, and incorporate them if and as appropriate in the next update of the Risk Register.

(c) The Risk Register should be reviewed by the Senior Management Team at least once each year.

5. Risk Assessment in Committee Papers

Presentation of papers to formal committees of the University must now include a reference to risk assessment and state the main risks pertaining to each particular project or proposal, together with details of the actions taken or proposed in order to minimise the risks.

The Committee Cover Sheet includes information relating to risk assessment. The following is a quote taken from the relevant paragraph:

"Risk Assessment

[Where relevant, summarise the main risk associated with the proposals and the actions which would be taken to minimise them.]"

6. Risk Assessment in the Annual Planning Round

In the process of preparing the planning submissions and proposed budgets, there are inevitably a number of assumptions and judgements made, and consequently inherent risks and uncertainties in the outcome. Whilst these are undoubtedly considered in preparing planning submissions, it is important that all those involved in preparing and reviewing the submissions are aware of these uncertainties.

Colleges and Support Groups are, therefore, asked in the planning submissions to provide a brief commentary (and where practicable, a financial evaluation) of the key risks and uncertainties which might cause failure to achieve the medium term plans, and in particular the proposed budgets and plans for the year in question, together with an indication of the specific plans to be taken to reduce or eliminate the major risks faced.

7. Risk Assessment in Change and Development Activities or Projects

Whenever change or development activities take place, whether organised as projects or managed in other ways, there are a set of "issues that have to be got right" in order for the project to be successful, and a set of "things that could go wrong".

Examples of activities where such an approach should be used include: new degree programmes, new business development or alliances, research programmes, IT system changes, organisational changes, major expansion in student numbers, estates projects, etc.

It is good practice to capture the risks in a project risk register showing the risk, its importance to the project (High, Medium, Low) and how it is to be managed. An example of such a risk register is shown below.

The objective is to review the list in the appropriate project group/steering group/ committee etc. throughout the project, and for the group at each review to:

- Add/amend the risks
- Amend the importance of the risk (in the early stages of a project, the risks are often 'High' but as the activity progresses, the risks become lower as they are resolved or managed).
- Initiate actions to manage the risks, and monitor their progress.

In this way the steering group is aware of the key issues throughout the project, and particularly at critical decision points or implementation points.

Project/Change/Development Activity Risk Assessment: Risk Summary

Risk	Importance H/M/L	Actions to Manage and Responsibility (Risk Owner)	Timescale
1.			
2.			
Etc.			

8. Reporting on the Effectiveness of Risk Management Processes

During each year the Risk Management Committee reviews the procedures to control and manage each risk in the University Risk Register prepared by the relevant Lead Senior Manager to confirm that processes are effective and to identify areas for improvement. The format of the review is shown in Appendix 1

At the end of the financial year, Heads of Colleges (and the Management Teams), the Heads of Support Groups, and Subsidiary Companies (with their Management Teams, are required to complete a Risk Questionnaire and provide an assurance to the University Risk Management Committee, and through them to Court, that the risks to the delivery of College/Support Group objectives and their ongoing survival, have been properly identified and that they are being managed effectively.

In addition a year end report is obtained on IS, Procurement, and Health and Safety risks. Also, Finance Department report on outcomes of the Internal Control Questionnaire completed for the External Auditors.

At the end of the year, the Risk Management Committee prepares a report of its activities, and summarises the responses to the Risk Questionnaire. This report is taken to CMG, Finance and General Purposes Committee, Audit Committee and to the University Court, It provides assurances that enable Court to make statements in the annual published accounts to the effect that:

(a) There is an ongoing process for evaluating and managing significant risks faced by the University, and

(b) This process has been in place for the year under review and up to the date of approval of the annual report and accounts, and

(c) The University Court has satisfied itself that an effective system of internal control has been in place for the year under review.

In addition it provides specific assurances on procurement as required by the Committee of University Chairmen's Guidance manual, and also assurances in support of the Letter of Representation that Court is required to provide to the External Auditors.

9. Useful Risk Management Links

- Scottish Funding Council Code of Audit Practice http://archive.sfc.ac.uk/publications/pubs_other_shefcarchive/code_of_audit_practice.pdf
- Scottish Government guidance on risk management: http://www.scotland.gov.uk/Topics/Government/Finance/spfm/risk
- British Standards on Risk Management
  - BS 31100:2008 Risk management, Code of practice
  - BS ISO 31000:2009 Risk management, Principles and guidelines
- UK Treasury Orange Book: Management of Risk – Principles and Concepts
  - http://www.hm-treasury.gov.uk/d/orange_book.pdf

Appendix 1: Template for Risk Reviews

RISK REVIEW

The aims of the Risk Review are twofold

- *to enable the Lead Manager of the particular risk to review and assess whether the risk is being adequately managed, and what further actions should be undertaken to ensure required or desirable improvements in the management of the risk are undertaken*
- *to provide the Risk Management Committee, and through them, the University Court, assurance that the Risk is being adequately managed*

Risk:

Inherent risk: *(in the absence of any mitigation)*	**Senior Manager:** *(taking lead responsibility for management of Risk)*
Residual risk: *(with current mitigating actions in place)*	**Risk Review prepared by:**
Likelihood of risk event occurring *(as assessed with current mitigating actions in place)*	**Date:**

Threats: *(if risk event occurs or risk is not managed)*

Opportunities: *(other benefits that might accrue on successful management of risk)*

Current management processes or mitigating actions: *(Identify the major elements in managing the risk and how you ensure those elements are operating properly. For some risks, if it is possible to identify actions that would be taken in the event of the risk event occurring that would mitigate its impact, please also identify these.)*

Monitoring of Risk / Performance Indicators: *(Identify how you would know that the risk is not being adequately managed; and identify relevant key performance indicators that provide an indication of the adequacy of risk management/mitigation. Attach tables or graphs of those indicators.)*

Senior Manager's assessment of current management of risk:	**Yes/No**	**If no, please explain**
Are the current management processes and mitigating actions operating satisfactorily? Do the current management processes and mitigating actions, coupled with the evidence from the Performance Indicators provide you with assurance that the risk is being adequately managed? Is the Residual Risk "rating" above acceptable given the nature of the risk? *(If no, please state what "rating" the University should be regarding as acceptable, and identify below the actions that are to be put in place to achieve an acceptable level of management/mitigation)*		

Further actions *(either required to achieve an acceptable level of adequacy of management/mitigation, or planned to enhance the existing management /mitigation processes)*	**Responsibility**	**To be completed by**
1. 2. etc		

Note – where actions above are to be shown as the responsibility of an individual, then those individuals must agree to the action and the timescale. Any actions not yet agreed with the individual, or potential areas for action that require to be discussed, to be included in the table below.

Proposed additional actions *(either required to achieve an acceptable level of adequacy of management/mitigation, or planned to enhance the existing management /mitigation processes)*	**Proposed Responsibility**
1. 2. etc	