



UNIVERSITY OF LONDON

GUIDE TO RISK MANAGEMENT

Purpose of the guide..... 2

Risk Management – The Basics 2

 What is Risk Management? 2

 Applying Risk Management 2

 The Use of Risk Registers in Risk Management..... 4

 What is the Purpose of Risk Management? 4

Risk Management in the University of London 5

 Components of Risk Management in the University 5

 Risk Management Roles and Responsibilities 5

 Risk Management Responsibilities – Quick Reference Guide 6

 Reporting Risk Management and Escalating Risks 7

Preparing a Departmental Risk Register – what to do 8

Conducting a Peer Review – what to do 12

 Guide to the Suggested Format..... 12

Risk Management in Major Projects – what to do 15

Preparing the Strategic Risk Register – what to do 15

Glossary of Risk Management Terms 17

Risk Management Prompt List..... 18

PURPOSE OF THE GUIDE

This document supplements the Risk Management Policy, explaining how the various management groups, committees and individuals who have Risk Management responsibilities under that Policy should consider carrying these out.

The Risk Management Policy is available [here](#).

This Guide is largely concerned with recommending best practice and efficient methods, but those involved in Risk Management may choose to use different methods to achieve the same ends. The recommendations within it will be updated from time to time based on effective practice within the University and the sector generally.

RISK MANAGEMENT – THE BASICS

Risk Management is not the same as risk assessments in terms of the health and safety of staff, student and visitors (if this is what you are looking for, the University's Health and Safety policies and procedures can be accessed [here](#)).

What is Risk Management?

In its simplest definition, Risk Management is answering one simple question:

What could go wrong and what are we going to do about it?

Several sub-questions make up this premise:

- What could go wrong in the achievement of our objectives?
- What could go wrong with our operations?
- How likely is it that they will go wrong?
- How bad (i.e. what impact) would it be if they did go wrong?
- What can we do to prevent them from going wrong?
- Are we doing enough regarding what could go wrong?
- Who is responsible for ensuring that we have good answers to these questions?

Applying Risk Management

In a higher education setting, we are required by HEFCE¹, the Colleges that constitute the University, and other stakeholders and funders, to demonstrate that we have considered what might go wrong with our plans, that we have analysed the consequences of things going wrong, and that we have thought through the actions and controls we need to prevent or limit these consequences.

¹ The Higher Education Funding Council for England.

Risks for the University (and other Higher Education Institutions) might include the following:

- Withdrawal of funding (from HEFCE or other sources);
- Collapse of key markets leads to a dramatic loss of income;
- College dissatisfaction with our services leads to withdrawal from that service or from the federal University (customer service, cost-effectiveness, relevance to College’s mission etc.);
- Inability to operate Halls of Residence (power failure, fire etc); or
- Damage to reputation through negative media coverage.

The logic to managing these risks can be broken-down as follows:

If...	... then	We don't want ...	So let's...
... we are unable to operate Halls of Residence because of a fire we'll lose income and our reputation will be adversely affected.	... to lose income from Halls and suffer reputational damage...	... create strict rules for naked flames, test fire alarms regularly, have well-rehearsed evacuation procedures.

... Or...

If...	... then	We don't want ...	So let's...
... Colleges are dissatisfied with the services we provide,	... they might withdraw from that service and stop funding it.	... Colleges to withdraw from our services,	... survey the Colleges every quarter to find out what they think and change what we do to meet their expectations.

This is a basic example – simplistic even – but it demonstrates the basic key principle of Risk Management, namely:

Risk Management is about identifying what we should be doing in order to get the results that we want and to stop things going wrong.

The Use of Risk Registers in Risk Management

In a professional capacity, especially in dispensing public funds, where we have to prove our planning and decision-making to outside organisations, it is not sufficient to make decisions only verbally, and carry the risks and resulting actions 'in your head'.

Instead, we use Risk Registers to document and record our consideration of risk and what we intend to do about risks. Doing this demonstrates the professional management of risk within the University and also, by setting out everything we do and submitting it to scrutiny, allows us to consider if we are doing enough to control each risk or whether our resources would be better used elsewhere.

Risk Registers are prepared:

- by each Department, at least twice per year, however the register should be thought of as 'live' and updated as necessary;
- by the Project Manager and Project Board of major capital investment projects (in accordance with established project management methodology such as PRINCE2); and
- by the Operational Development Group, documenting the risks faced by the University at a corporate / strategic level (the Strategic Risk Register).

What is the Purpose of Risk Management?

Given the example above, it becomes evident that Risk Management serves a number of purposes:

- It documents to HEFCE, Colleges and other funders that we take seriously the achievement of our objectives and can demonstrate what we are doing to prevent things going wrong in their achievement;
- It informs our actions and decisions about what we need to do in order to achieve objectives, how to allocate resources; and
- It is part of a comprehensive and professional approach to planning, and the monitoring of performance against plans.

RISK MANAGEMENT IN THE UNIVERSITY OF LONDON

The above principles are realised in the University through: (i) the Components of Risk Management; and (ii) Roles and Responsibilities in Risk Management.

Components of Risk Management in the University

The Risk Management Policy is part of the Ordinances under which the University is governed. The Risk Management Policy states that:

Risk Management in the University shall consist of the following elements:

- The Strategic Risk Register;
- Departmental Risk Registers;
- Peer Reviews of Departmental Risk Registers;
- Risk Registers for major Capital Investment Projects; and
- Urgent Action taken by the Vice-Chancellor.

Risk Management Roles and Responsibilities

The Board of Trustees, the Audit and Risk Committee, the Operational Development Group, Heads of Departments, the Risk Management Co-ordinator, and Project Managers of major capital investment projects each have various responsibilities for Risk Management as an integral part of their professional responsibilities.

The ways in which responsibility for the various components of Risk Management breaks down across different roles and Committees/management groups is summarised overleaf.

Risk Management Responsibilities – Quick Reference Guide

	Departmental Risk Registers	Peer Review of Risk Registers	Risk Registers for Major Capital Investment Projects	Strategic Risk Register
All Employees	To identify and report risks for Departmental Risk Registers.	N/A	To contribute to the risks registers for major projects through project management structures and governance.	N/A
Risk Management Co-ordinator	To provide guidance and support to Heads of Departments as appropriate.	To provide guidance and support to Heads of Departments as appropriate.	To ensure that Risk Management of major capital investment projects is reported to the Audit and Risk Committee on behalf of the Chief Operating Officer.	To support and assist the Operational Development Group in its bi-annual preparation of the Strategic Risk Register.
Heads of Departments	To prepare, at least twice per year and in consultation with appropriate colleagues, a 'local' Risk Register for their Department	To participate in a Peer Review once per year.	To ensure that major capital investment projects within their Department are subject to rigorous Risk Management controls.	To highlight risks within Department (through the 'local' Risk Register) for the attention of the Operational Development Group in preparing the Strategic Risk Register.
Operational Development Group	N/A	To review the progress and effectiveness of the Peer Review process.	To be satisfied that appropriate Risk Management arrangements are in place for Major Capital Investment Projects.	To prepare the Strategic Risk Register twice per year.
Audit and Risk Committee	N/A	To receive regular reports on the Peer Review process and the significant risks identified therein.	To receive regular reports on Risk Management arrangements for major projects.	To consider the Strategic Risk Register twice per year and recommend it for approval to the Board of Trustees.
Board of Trustees	N/A	To receive annual assurance from the Audit and Risk Committee that effective Risk Management is taking place.	To receive annual assurance from the Audit and Risk Committee that effective Risk Management is taking place.	To approve the Strategic Risk Register twice per year.

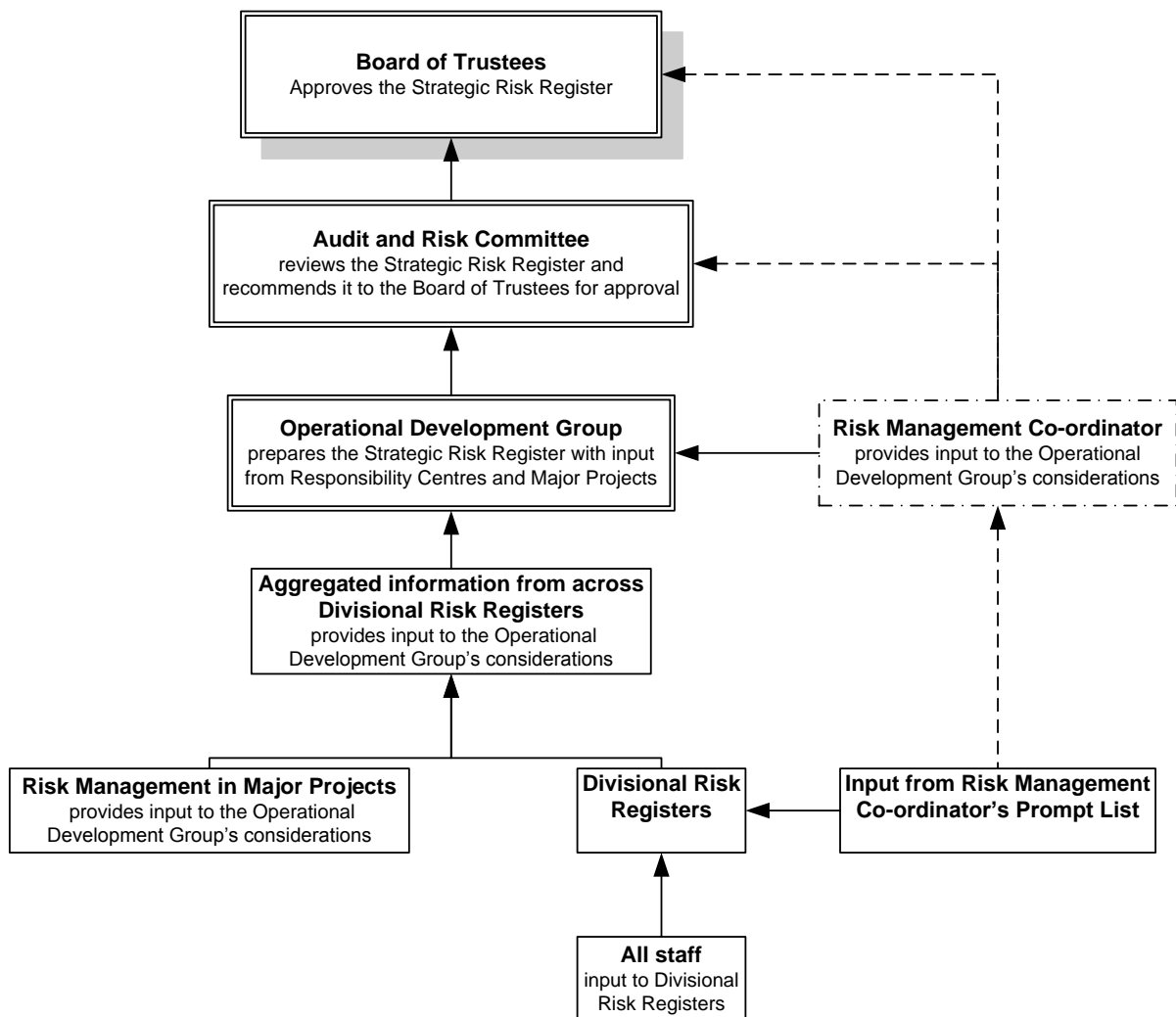
Guidance on how to carry out the responsibilities detailed above are given on the next pages.

Reporting Risk Management and Escalating Risks

All members of staff are responsible for managing risks in their areas of work, and for reporting developments that may affect the risks faced by the Department or wider University to their line manager. Nevertheless, the responsibilities of Risk Management largely lie with Heads of Departments who, by recording risks faced within their Departments on Risk Registers, alert the Operational Development Group to significant risks which can be considered for inclusion on the Strategic Risk Register and managed at a strategic, as well as Departmental, level. (Project Managers, through the use of Risk Registers for major capital investment projects, also contribute to the assessment of the risks faced by the University.)

The result is a clear process for reporting risk up to the Board of Trustees, and for escalating major risks to an appropriate level of management. This structure is illustrated in the chart below.

Risk Management Reporting and Escalating Structure in the University



PREPARING A DEPARTMENTAL RISK REGISTER – WHAT TO DO

Under the Risk Management Policy, Heads of Departments are required to prepare 'local' Risk Registers for their Departments at least twice per year, and also in response to particular events (see paragraph 23 of the Risk Management Policy). The following notes explain how to prepare a 'local' Risk Register.

Step 1 – Refer to the current 'prompt list' at the end of this Guide

This list details ideas and starting points for thinking about risks within your Department (it is updated based on changes to the University's external environment and current Risk Registers at all levels, making the process iterative).

Step 2 – Arrange a meeting of the senior managers in your Department

Each attendee should individually review the 'prompt list' and the existing Risk Register prior to the meeting.

Step 3 – Review the strategic objectives of the Department

Discuss the impediments to the achievement of the strategic objectives – what could go wrong?

Step 4 – Review the risks on the Risk Register

Go through the existing register.

- Is each risk still valid? If not, delete it.
- Is each risk similar to any others with which it could be combined?
- Are there risks missing, either impediments to achieving the strategic objectives or ideas from the Risk Management Co-ordinator's 'prompt list'?

Step 5 – Amend or add scores to each risk

Taking each of the risks in turn, discuss and rate the likelihood, impact and control over the risk.

Thinking about the Likelihood Score

There are two ways to think about the likelihood: (i) Frequency; and (ii) Probability.

Frequency

How many times will the adverse consequence being assessed actually be realised? For example, in considering the risk of health and safety incidents, depending on the building and staff, students and visitors in question, the likelihood could be graded as expected to occur monthly or even weekly. If health and safety incidents are unlikely, the risk could be graded as expected to occur annually. A simple set of time-framed definitions for frequency are shown in the table below.

Probability

Probability is a more useful way to score certain risks, especially those associated with the success of time-limited or one-off projects such as a new IT system. Instead of basing the likelihood score on how often the consequence will materialise, it can instead be based on whether it will occur at all in a given time period. A set of definitions from this perspective are shown in the table below.

Score	General description	Frequency description	Probability description
1	Very unlikely to materialise imminently	Barely feasible	1/1000 chance or less
2	Unlikely to materialise imminently	Extremely unlikely in the current year but possible long term	Between 1/1000 – 1/100 chance
3	Possible some likelihood that the risk will materialise imminently	Not likely in the immediate future but reasonably likely in the medium/long term	Between 1/100 – 1/10 chance
4	Likely to materialise imminently	Possible in the current year and likely in the longer term	Between 1/10 – 5/10 chance
5	Very likely to materialise imminently	Probable in the current year and highly probable in the longer term	1/2 chance or more.

Thinking about the Impact Score

When assessing the impact, remember the following gradings in financial, operational and reputational terms:

Score	Description
1	financial loss <£250K / no significant adverse publicity / minor operational impact
2	financial loss £250K-£500K / limited unfavourable media coverage / service disrupted but key activity not delayed
3	financial loss £500K-£750K / unfavourable local or short-term media coverage / sporadic provision of key activity
4	financial loss £750K-£1M / significant public, media concern / key activity unavailable delaying processes, wasting resources
5	financial loss >£1M / adverse national, prolonged media coverage / key activity unavailable for more than one week

Score	Description
1	Insignificant – Very little significant (IMMATERIAL) impact on ability to deliver objectives/outcomes (nothing to worry about)
2	Fairly Serious – Little significant (LIMITED) impact on ability to deliver objectives/outcomes (possibly important but can be managed although would take up some time and resources)
3	Serious - Some impact on ability to deliver objectives/outcomes (it would cause us some problem and would definitely take up time and resources)
4	Very Serious – Significant impact on ability to deliver objectives/outcomes (would hinder achievement of our strategic objectives and or would take up considerable time and resources)
5	Major Crisis – Very significant impact (MAJOR/SEVERE) on ability to deliver objectives outcomes, and/or significant impact on reputation, and/or ability to meet statutory requirements (could seriously undermine the standing and position of the organisation)

Score	Description
1	Insignificant – Very little significant (IMMATERIAL) impact on brand/reputation (nothing to worry about)
2	Fairly Serious – Little significant (LIMITED) impact on brand/reputation (possibly important but can be managed although would take up some time and resources)
3	Serious - Some impact on brand reputation (it would cause us some reputational problems and would definitely take up time and resources)
4	Very Serious – Significant impact on brand/reputation (would damage the University's brand in the internal and external environment, would take considerable time and resource to deal with and would hinder achievement of strategic objectives)
5	Major Crisis – Very significant impact (MAJOR/SEVERE) on brand/reputation (could seriously undermine the standing and position of the organisation and could lead to major loss of income)

Score	Description
1	Insignificant – Very little significant (IMMATERIAL) impact on staff morale (nothing to worry about)
2	Fairly Serious – Little significant (LIMITED) impact on staff morale (possibly important and would need corrective action))
3	Serious - Some impact on ability to staff morale (it would cause us some problem and would definitely take up time and resources)
4	Very Serious – Significant impact on staff morale (would hinder achievement of our strategic objectives, affect staff performance or would take up considerable time and resources)
5	Major Crisis – Very significant impact (MAJOR/SEVERE) on staff morale (could seriously undermine the standing and position of the organisation, severely affect staff performance and could lead to industrial action)

Step 6 – Review the controls

This is the most important part of the process.

Given your likelihood, impact and control scores, consider:

- whether the controls you have in place are adequate to prevent each risk from happening, (or deal with it if it does happen)?
- what other controls you could you put in place
- whether it would it is a sensible use of time and energies to put each new control in place?

Remember that:

- For risks graded 8 or more, you must have an action plan, where practical, to reduce the risk to an acceptable level (this level is called the University's risk scoring tolerance).

Step 7 – Add details of Early Warning Indicators to the controls

Consider how you will know if a risk is happening? Will there be near-miss incidents? Will there be warning signs or trends? Can you quantify these warning signs or trends (e.g., if x falls below a pre-determined level, there is a danger that risk y could be happening so we will need to do z).

Step 8 – Add a review date for each risk

For risks rated 8 or higher, you should have an action plan (see above) which should include a date by when the plan will be implemented. For other risks, the review date should be no longer than 6 months away.

Step 9 – Add details of who is responsible for each risk or action plan.

A named post-holder must be given as responsible for managing each risk on the register. If the risk is graded 8 or higher, this must be the person responsible for implementing the action plan devised to lower the likelihood of the risk materialising

Step 10 – Publicise Your Risk Register

The final version of the Register should be widely circulated within the Department so that staff are aware of its contents – why not post it on your Department's areas of the Intranet? It should also be forwarded to the Risk Management Co-ordinator once finalised.

CONDUCTING A PEER REVIEW – WHAT TO DO

The format of Peer Reviews is for guidance only; each Reviewer should use his/her judgement in presenting the Peer Review. The suggested format is available on the Intranet here. In any event, low-level risks (i.e. those with a score of 7 or less) need not be reviewed.

Guide to the Suggested Format

The format splits the review into two sections: High-level and Medium-level risks. The same process could be used for both sections.

Consider starting each section with a few bullet points to summarise any key points. For example: do these risks link to the Department's operation, or are they wider, strategic risks for the University? Are there any themes to be drawn out, either in the type of risks or their in their controls?

In the table overleaf, the first two columns giving details of the Risk should already have been completed by the Reviewee.

The third column is designed to detail the Reviewer's comments. You may wish to consider:

- Have controls (on impact and on likelihood) been identified in the Risk Register for this risk?
- Have controls been identified for all risks, and how good are the controls identified? Did the review identify any additional controls?
- Are Early Warning Indicators identified? Do they seem adequate?
- Consider the review date: 'Ongoing' is not a valid review date; a specific date or timeframe must be given.
- Is a named individual responsible for each risk?
- *High and Medium-level risks only*: is there an action plan for each level risk that is Specific, Measurable, Achievable, Realistic and Timed?
- Are any of the risks identified possibly inter-dependent to another Department?
- Are there any opportunities to share best practice, in dealing with the risk, during the review?

The fourth column is designed to detail any resulting next steps. For example you may wish to note any implementation or improvements of controls, or arrangements for Early Warning Indicators being triggered.

The last two columns are for the Reviewee to assign tasks, with estimated completion dates.

A sample completed Peer Review is given on the next page. Further guidance is available from the Risk Management Co-ordinator.

Sample completed Peer Review of Risk Register

A few bullet points are used to summarise the information given for High-level risks.

The first two columns of both sections should be already completed by the Reviewee.

Insert your comments about the risk and how it is being managed here: Have controls been identified in the Risk Register for this risk? How good are the controls identified? Did the review identify any additional controls? Are Early Warning Indicators identified? For High-level risks, is there a SMART action plan?

Responsibility Centre	Head of Responsibility Centre	Reviewed by	Date
Risk Management Department	Rosalind Sector	Paul Sullivan	April – May 2007

This information should already be completed by the Reviewee.

Summary of High level risks (Residual Score = 12 or more)

- There are few high level risks for the department. Two of the risks identified relate to the wider University while the third is an operational risk of the department.
- One risk does not have a SMART action plan developed but it has been agreed that this is necessary. Staff have been tasked with this to specific deadlines.

Description of Risk	Residual Risk Score	Peer Reviewer's comments on identified actions and controls	Next steps to be taken	By Whom	By When
Failure to implement and facilitate an adequate Risk Management Programme	13	Controls to mitigate against the likelihood and impact of this risk have been identified and Early Warning Indicators have been developed. A SMART plan has been agreed	Implementation of SMART action plan and quarterly review of effectiveness.	Risk Management Co-ordinator	Implementation by July 2007
Business Continuity Plans are not adequately tested	12	Controls to reduce the likelihood of the risk from occurring are in place. There are no controls possible to reduce the impact of the risk. A SMART plan to reduce the likelihood of BCP plans being inadequate has been agreed and will be implemented later this year.	Implementation of agreed SMART plan. Monthly review of identified controls to ensure continued validity.	Risk Management Co-ordinator	Implementation by August 2007
Lack of engagement in benefits of Risk Management from staff	12	The existing controls may not be sufficient and a SMART plan should be developed.	Development of SMART action plan to improve risk control measures.	Risk Management Co-ordinator	SMART plan developed by July 2007

For this column, add the Next Steps to be taken. You may wish to note any implementation or improvements of controls, or arrangements for Early Warning Indicators being triggered.

Summary of Medium-level Risks (Residual score = 8-11)

- There are few Medium-level risks for this department. The most pressing concern is the second risk, 'Inadequate communication of BCP leads to lack of awareness among staff', for which no controls were identified. Actions have now been identified to remedy this situation and these are expected to be complete by September 2007.
- Throughout, analysis of likelihood and impact seems accurate and monitoring of risks takes place regularly with staff involvement.

Description of Risk	Residual Risk Score	Peer Reviewer's comments on identified actions and controls	Next steps to be taken	By Whom	By When
Internal auditors cease trading	9	The analysis of this risk rightly treats it as unlikely but accepts the significant impact if it does occur. No mitigating controls and no Early Warning Indicators are identified.	Identify and implement controls and Early Warning Indicators.	Risk Management Co-ordinator	Nov. 2007
Inadequate communication of BCP leads to lack of awareness among staff	8	The department is well appraised of the need for top-rate communication and continually works to improve this: good controls are in place to ensure communication (ie prevent this risk from occurring).	Identification of Early Warning Indicators that communication of BCP maybe lacking. Devise methods to monitor effectiveness of communications.	Assistant Risk Management Co-ordinator	Sept. 2007

The Reviewee should decide who will complete the agreed Next Steps and by what deadline.

RISK MANAGEMENT IN MAJOR PROJECTS – WHAT TO DO

Due to the variable size and complexity of major capital investment projects, the Risk Management Policy does not specify how a project manager should undertake Risk Management. Nevertheless, project managers are expected to meet the expectations of the project board regarding Risk Management, and in a manner aligned with standard project management methodologies such as PRINCE2. Project Managers should be aware that the Audit and Risk Committee regularly receives reports on the Risk Management in major capital investment projects. Guidance and support is available from the Risk Management Co-ordinator, along with examples of Risk Management from other projects.

RISK IN PLANNING

It is important to utilise risk management in the planning process (Departmental and Strategic) to ensure that the University is taking an integrated approach to all areas of risk management and operational outputs. When developing a plan and its objectives; the risks to the success of the objectives, and the mitigating actions for these risks, must be considered and identified at the planning development stage. The optimum approach is to link risks directly to the objectives of the plan; it is also recommended that the plan is cross referenced against the existing Departmental Risk Register to ensure that all areas of risk have been considered. An example planning template can be seen here [‘intranet hyperlink’](#) to illustrate this approach. The benefit of including risk management in the planning process is that risks linked to operational success will be identified, communicated and mitigating actions agreed at the development stage.

This approach can also be utilised when developing a business case proposal and an example business case proposal template can be viewed here [‘intranet hyperlink’](#).

PREPARING THE STRATEGIC RISK REGISTER – WHAT TO DO

Under the Risk Management Policy, the Operational Development Group is responsible for preparing the Strategic Risk Register twice per year.

In preparing the Strategic Risk Register, the Operational Development Group will use a similar process to that described above by which Departments prepare their ‘local’ Risk Registers. The discussions of the Operational Development Group will be informed by:

- The high level risks detailed on the Departmental Risk Registers (extracted by the Risk Management Co-ordinator in an ‘aggregated risk analysis’);
- The findings of the Peer Review process;
- The findings of the internal and external audit processes;

- Analysis of the University's risk profile by the members of the Operational Development Group during its meetings; and
- The Risk Management Co-ordinator's 'prompt list'.

Not all of the above sources of information need be used during every preparation of the Strategic Risk Register.

The Operational Development Group will then report to the Audit and Risk Committee on the management of risk within the University.

GLOSSARY OF RISK MANAGEMENT TERMS

Departmental Risk Register	A Risk Register detailing the risks faced by a particular Department, e.g. the Finance Department Risk Register.
Strategic Risk Register	A Risk Register detailing the risks faced by the University as a whole.
Peer Review	The process whereby one Head of Department reviews the Risk Register of a different Department.
Aggregated Risk	A means of analysing similar risks across different Departments in order to determine whether they are cumulatively of sufficient magnitude to warrant inclusion on the strategic Risk Register.
Risk Scoring Tolerance	A level of risk beyond which the University Risk Management Policy requires an action plan to be developed to reduce the risk to acceptable levels. On Risk Registers, any risk with a residual score of 8 or greater is requires an action plan.
Mitigation	Actions that are taken, or which could be taken, to address risks faced either by reducing the likelihood that they will occur, or by managing their impact if they do occur. Also referred to as: 'mitigating actions'; 'controls'; or 'mitigating controls'.
Action Plan	A plan of response to address risks beyond the University's established risk appetite. A good Action Plan will detail: who will do precisely what, when and how.
Early Warning Indicator	An established factor, often a regular management report, in which changes in patterns of data would indicate a risk becoming more likely to happen, or may be about to happen.
Risk Management Co-ordinator	The Risk Management Co-ordinator has responsibility for ensuring that the Risk Management process work effectively and also offers advice and guidance on its operation. The Risk Management Co-ordinator's contact details are here .

RISK MANAGEMENT PROMPT LIST

The following list is intended to prompt Heads of Departments to consider various possible sources of risk when preparing Departmental Risk Registers. It also serves as a general reminder of possible risks faced by the University and should also therefore be used as a general checklist.

1. Macro-economic factors (national or international)
2. Changes to the political outlook of government
3. Changing legal restriction on activities, or regulatory restrictions, e.g. HEFCE or ICO regulations
4. Governance of the University / particular Department
5. Changing funding sources
6. 3rd party contracts or accreditation by third parties
7. Buildings and facilities / adequacy of accommodation
8. Security risks (personal, premises and assets)
9. Ethical or Corporate Social Responsibility
10. Leadership
11. IT software failure
12. Staff recruitment and retention (especially specialist staff)
13. Environmental / Green issues
14. Ongoing major projects
15. Reputation / media risks
16. Economy and value for money
17. Contingency planning (activities, buildings, staff skills, staff knowledge)
18. Fraud and other crime
19. Employees' skills and mismatch with required skills
20. Academic quality
21. Failure of budgetary control or financial planning
22. Loss of confidential data
23. Robust management of data for returns to funding bodies

24. Staff Morale
25. Health and Safety