

February 2005/11

**Good practice**

Guidance

This report is for information and guidance

This report draws on good practice in the higher education sector and elsewhere, providing practical guidance to higher education institutions on enhancing and embedding their risk management processes. It complements earlier guidance published by HEFCE, and is aimed at all those involved in the risk management process within institutions, particularly risk managers, audit committees and governing body members.

# Risk management in higher education

**A guide to good practice, prepared for  
HEFCE by PricewaterhouseCoopers**

# Contents

	Page
Executive summary	2
Introduction	3
Involvement of the governing body	7
Risk appetite	10
Resourcing	13
Exploring and assessing the risks	16
Actions for improvement	21
Prioritisation of risk reporting	24
Embedding risk management	27
Sharing risk management knowledge	31
 <b>Appendices</b>	
A Self-assessment checklist for audit committees	33
B Organisations that contributed to this guidance	36
C Index of examples	37
D Further reading	38
E Glossary of terms	39

## **Executive summary**

### **Purpose**

1. This report draws on good practice in the higher education sector and elsewhere, providing practical guidance to higher education institutions on enhancing and embedding their risk management processes. It complements earlier guidance published by HEFCE (in particular HEFCE 01/28) and available on its web-site at [www.hefce.ac.uk](http://www.hefce.ac.uk) under Finance and assurance/Good practice.
2. The guide is aimed at all those involved in the risk management process within institutions, but is particularly relevant for risk managers, audit committees and governing body members. It is also commended to the related bodies funded by HEFCE.

### **Key points**

3. Institutions in the higher education sector are moving from achieving technical compliance with the Turnbull Report and with HEFCE requirements, and are now looking to realise the benefits of having implemented risk management. These include the ability to take better-informed decisions about opportunities, and to constructively address new patterns of risk.
4. The guide describes different techniques used by institutions to obtain maximum benefit from risk management, including drawing on the expertise of the governing body, academic staff and internal audit. It examines different models of resourcing risk management, scoring risks and reporting on them. It also looks at how different institutions have embedded risk management.
5. In the best-run organisations, risk management is synonymous with good management and good governance. It is not considered as a bolt-on to existing practices, or a separate exercise simply to meet regulatory requirements.
6. This guide was prepared by PricewaterhouseCoopers on behalf of HEFCE.

### **Action required**

7. As with the previous HEFCE guidance on risk management, this guide is not prescriptive. It is recognised that there is no single correct approach to managing risk in institutions.

## Introduction

### Key points

- This guidance builds on that issued by HEFCE in May 2001 (HEFCE 01/28). It is not mandatory but can be used by managers and audit committees as an aid for assessing progress made by their institution.
- The current requirements for the higher education sector are derived from the Turnbull Report. In addition, the Combined Code setting out principles of governance in the private sector, while not mandatory, builds on Turnbull and provides an important context.
- Institutions have identified a number of benefits to be derived from risk management, including the ability to take informed decisions about opportunities and to constructively address new patterns of risk.
- Good risk management includes the need to marry top-down and bottom-up assessments to produce a comprehensive picture of risk to the institution.

### Context

8. This guidance supplements and complements that issued by HEFCE in May 2001 (HEFCE 01/28). It aims to provide governing bodies (through their audit committees) and managers with a series of reference points to assess their institution's risk management arrangements against best practice from the sector and elsewhere.

9. The guidance was produced by PricewaterhouseCoopers on behalf of HEFCE, following visits during 2004 to different types and sizes of institution. Examples of good practice and innovation were derived from these visits, and have been used throughout the guide. They have been supplemented by examples from elsewhere in the higher education sector and from PricewaterhouseCoopers' experience of risk management practice in other sectors.

10. HEFCE and PricewaterhouseCoopers would like to thank all the institutions that have contributed to this guidance.

### Risk management in the higher education sector

11. The higher education sector has been implementing formal risk management procedures – based on the requirements of the Turnbull Report – for a number of years. The requirement originated from the Treasury in 2000 ('Corporate governance: statement of internal control' HM Treasury, ref DAO GEN 13/00).

12. Risk management requirements for higher education institutions are integral to the key regulatory documents for the sector: the Financial Memorandum with HEFCE (HEFCE 2003/54), the HEFCE Code of Practice for accountability and audit (HEFCE 2004/27), and the annual accounts direction from HEFCE (Circular Letter 23/2003). These requirements are elaborated on in HEFCE Circular Letter 12/2002 'HEI audit committees, risk management and statements of internal control'.

13. Our work has identified that the benefits of risk (and opportunity) management are widely recognised across the sector. This review has also shown that there is no single way in which risk management procedures need to be implemented to be effective. So it must be emphasised that this guidance is not mandatory, but is to be used where appropriate as an aid to enhancing the effectiveness of existing processes.

### The benefits of risk management

14. Our review found that the institutions that were most engaged with risk management were also most likely to have identified tangible benefits from the process.

15. Many of the activities associated with risk management were being undertaken in institutions before risk management was introduced. What risk management has brought is a consistency of approach. Put another way, one of the primary macro-benefits of risk management is that it has fostered consistent and

systematic management behaviour in institutions.

16. Risk management has provided the ability to systematically identify, assess and seize opportunities in ways that were not necessarily possible before.

#### **Example 1 Making the case for new initiatives**

At one institution visited, risk management has allowed managers and academics to construct a good and valid case for new initiatives. A manager who was looking for funds for a building extension used risk management techniques to establish a business case. This helped to demonstrate a robust and thorough approach to the project and the manager was successful in securing funding.

17. Risk management processes have also been found to promote healthy self-criticism within institutions, which has in itself opened up new directions and new opportunities.

#### **Example 2 Challenging the strategy**

A number of institutions use risk management as a tool for appraising key aspects of their strategies and business plans. Areas such as objectives, markets and quality have been subject to constructive challenge since the introduction of risk management. One institution recognised that one of its key objectives, that of income diversification, was partly derived from this sort of challenge, and that the identification and targeting of new overseas markets for its courses was directly linked to risk management processes.

18. At a more fundamental level we found that active risk management was responsible for the promotion of good management:

- projects and initiatives were better managed
- unnecessarily opportunistic risks have been avoided (balanced with the taking of realistic opportunities)
- risk management processes have promoted and facilitated better cross-institution working, both between academic departments and with service departments
- there was greater awareness of activities and initiatives throughout institutions (and indications that senior managers had become more involved throughout institutions as a result).

### **A changing pattern of risk and opportunity**

19. All the institutions visited recognised that the higher education sector is undergoing a period of change, driven by the need to maintain and enhance excellence, and that this impacted on their risk management processes.

20. Current factors driving risk and presenting opportunities at a strategic level include:

- variable tuition fees, increased competition for students and changing student expectations
- increased exposure and reliance on overseas markets, global competition and alliances
- restructuring, investment in infrastructure, institutional expansion and large capital projects
- commercialisation opportunities, and new and emerging technologies
- involvement in partnerships and associates.

21. Institutions saw risk management as helping to address these factors in an increasingly competitive environment. Along with these changes, we are also seeing the continued development of corporate governance practices in the private sector.

### **The Combined Code**

22. Within the private sector, the requirement for effective risk management underpins recent corporate

governance developments and the principles incorporated in the new Combined Code.

23. Although higher education institutions are not required to follow the Combined Code, it clearly sets out the context for risk management and provides a benchmark for good practice.

24. The principles of the Combined Code include:

- the governing body's role is to provide leadership within a framework of prudent and effective controls which enables risk to be assessed and managed
- governing body members need to receive accurate, timely and clear information, with good information flows within the governing body and its committees and between senior management and members of the governing body. Management has an obligation to provide such information but members of the governing body should seek clarification or amplification where necessary
- the governing body should maintain a sound system of internal control to safeguard stakeholders' interests and the institution's assets. It should, at least annually, review the effectiveness of the system of internal controls and should report that it has done so. The review should cover all material controls, including financial, operational and compliance controls and risk management systems
- members of the governing body need to constructively challenge and help develop proposals on strategy, scrutinise the performance of management in meeting agreed goals and objectives, and monitor the reporting of performance. They should satisfy themselves on the integrity of financial information and that financial controls and systems of risk management are robust and defensible.

### **An overview of good practice**

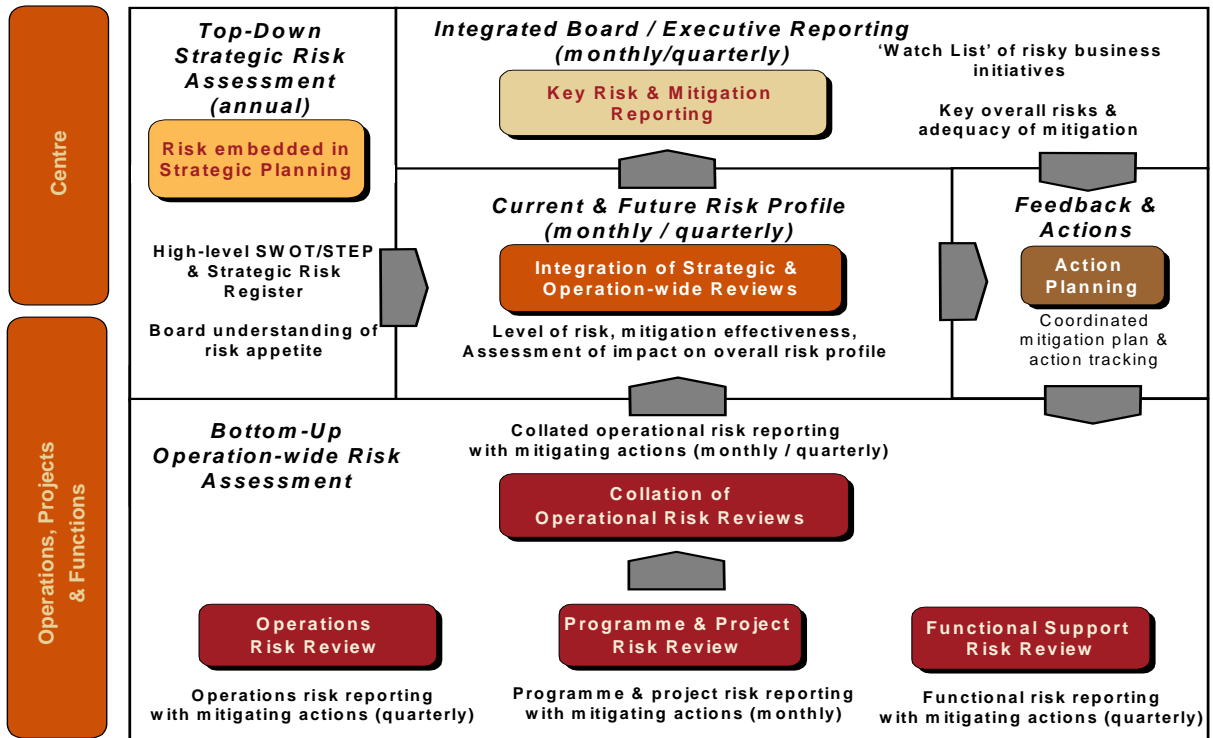
25. Good risk management practice is about having a holistic approach, driven by a desire to balance stability and innovation. We have outlined the risk management activities that we would expect to see in an institution following current good practice, and these are illustrated in Figure 1. This framework recognises the need for a top-down strategic assessment together with a bottom-up operations-wide risk assessment.

26. When combined this provides:

- an overall perspective on the risk profile of the institution
- a sound basis for robust reporting on risk at governing body level.

27. There is a perception that risk management deals only with the central corporate risks in an institution. We found that the institutions that benefited most from risk management are those that looked at all aspects of their activity (including academic activities) and involved as many different groups as possible within the institution. In many institutions, further work is needed to bring together and reconcile the top-down and bottom-up elements of the risk management process.

**Figure 1 Elements of an institution-wide risk management framework**



## Involvement of the governing body

### Key points

- Different governing bodies have varying degrees of involvement in risk management procedures.
- Risk management helps governing bodies to fulfil their responsibilities effectively.
- Governing bodies make an active contribution to risk management through their wider experience and by supporting and challenging managers.
- Audit committees are responsible for overseeing risk management processes, but the effectiveness of this could, in some cases, be enhanced.

28. Members of the governing body have an essential part to play in ensuring the integrity and transparency of risk management and corporate governance reporting.

### Responsibilities of the governing body

29. The governing body of any higher education institution is ultimately responsible and accountable for the operation of the organisation. This involves it in the stewardship of public funds and the operation of effective corporate governance, while at the same time identifying opportunities and supporting management in a strategic context.

30. The Financial Memorandum between HEFCE and institutions (HEFCE 2003/54) states that the governing body is ultimately responsible for the stewardship of public funds and must ensure that there is a sound system of internal control in place. In effect, the governing body must ensure that there are adequate corporate governance arrangements – a proper system for directing and controlling the institution.

31. The institutions we visited saw effective management of risk is an essential component of good corporate governance, and a contributor to the preservation and protection of the institution's assets. Risk management thus helps maintain and improve the quality of education and research provided by an institution. The governing body is responsible for providing direction for the organisation's risk management programme and ensuring that appropriate risk management activities are functioning effectively.

### Involvement of the governing body

32. Our research indicates that while governing bodies in the sector are aware of risk management and receive periodic reports on the topic, the quality and quantity of their involvement can be variable. Some institutions questioned the level of involvement that a governing body should have in risk management; while others used their existing governance frameworks to define boundaries of risk management responsibility.

### Example 3 Defining the responsibilities of the governing body

One institution has drawn a clear distinction between the role of managers and of the governing body in terms of risk management. A framework has been established where the governing body agrees the institution's key risks and is ultimately responsible for them. Managers are then held responsible for the management of these key risks. Risk management has clarified responsibilities of managers and the governing body.

### Challenge and support

33. Risk management should not solely be associated with accountability to the governing body (and to senior management and stakeholders). Indeed, where this view is taken it can have a negative impact. The institutions that benefit most from risk management are those that understand it as a two-way process: a way of feeding information up through the institution and providing support and targeting resources where they are most needed.

34. The governing bodies in some institutions have used risk management to support managers (as well

as providing constructive challenge) in some key areas.

35. We found that governors are able to assist managers in:

- providing a more complete picture of risk for the institution
- ensuring that risk management is integrated in strategic planning processes
- defining the institution's risk appetite
- receiving reports on the effective operation of the risk management process.

36. These areas are explored in more detail below.

### **A complete picture of risk exposure**

37. Our research found that where institutions have utilised the experiences of governing body members, they have benefited from the challenge and direction that this provides to the overall risk management process.

38. Members of the governing body can provide a more complete picture of risk exposure for the institution. We found examples where governing bodies had identified risks, and (arguably more importantly) provided a sounding board for management in assessing risk.

#### **Example 4 Governing body helping to identify risks**

At one institution, selected members of the governing body were involved in identifying key risks and designing risk management processes at the start of the implementation programme. While this has the danger of blurring the roles of managers and the governing body, it had the benefit of using the experience of governors to enhance the process and promote 'buy in' from the governing body.

### **Perceptions of risk**

39. Risk managers in institutions recognise that perceptions of risk vary among managers, senior management, academics, students and the governing body. For example, the personnel function will have a very different perception of risk to an academic department working in biotechnology research. This is another area where the governing body can help ensure that risk has not been defined too narrowly or too widely.

#### **Example 5 Governing body oversees operational areas**

Members of the governing body at one institution have been allocated areas to oversee that align with the institution's academic departments. They use the departmental risk registers to assist in exploring (but not managing) the key issues at their twice yearly meetings with academic heads. This was seen to enhance the governing body's contribution to the institution by cutting through the central administrative framework.

### **Linking risk management to strategic planning**

40. At most institutions visited, the governing body was working to ensure that risk management is integrated into the strategic planning process.

#### **Example 6 Governing body awaydays**

Several institutions have used 'awaydays' to involve governing body members in the risk management process. These events explicitly link discussions about strategy and risk. All members of the governing body can contribute to the debate, utilising their experiences to challenge and direct the institution's risk management strategy and processes.

41. An active contribution should be made in defining the institution's risk appetite (see paragraphs 48-65 below), as this helps set the framework within which the strategic planning process should operate.

### **Benefiting from the experience of governing body members**

42. We found a number of examples where the governing body had benefited an institution from its members' wider experience in business and the community.

#### **Example 7 Governing body contributing wider experience**

Institutions have benefited from its governing body members' wider experience of risk management: in the following areas:

- experience gained from risk management processes in other sectors (commercial, other public sector) used to challenge the 'risk appetite' of the institution and establish the tone at the top
- sharing tools and risk management methodologies to guide the production and monitoring of risk registers
- bringing in risk managers from other organisations to present their approach to risk management
- sharing information on best practice at other organisations and how the institution compares to others in the private and public sectors.

## Adverse outcomes

43. Sound risk management provides some protection for governing body members, and for the institution, in the event of adverse outcomes. Provided risks have been managed adequately, protection occurs on two levels. First, the adverse outcome may not be as severe as it might otherwise have been. Second, those accountable can demonstrate that they have exercised a proper level of diligence.

## Exercising responsibility through audit committees

44. Under 'Accountability and audit: HEFCE Code of Practice', audit committees must assess the risk management, control and governance arrangements and advise the governing body on their effectiveness.

45. Our review found that in all institutions the audit committee had taken on responsibility for reviewing the risk management process. The way in which the audit committee exercised its role varied from institution to institution.

### Example 8 Audit committees: interaction with risk management

Three different experiences of audit committees and risk management:

- one institution's audit committee reviews the full risk register at every meeting
- at another audit committee, individual departmental risks are explored in detail on a rolling cycle
- other audit committees only consider risk management in detail when internal auditors have reviewed this area.

46. Different levels of scrutiny are appropriate dependent upon circumstances, but the effectiveness of this role as overseer could be enhanced for some audit committees.

## Challenging the audit committee's effectiveness

47. The following questions could be considered in relation to the audit committee's role in risk management:

- has this role been formally defined?
- do audit committee members understand what aspects of risk management they should be looking at?
- how often is the audit committee considering risk management?
- has the audit committee set out the type of information that it wants to see on risk management?
- is the audit committee responsible for all aspects of risk management, or is it more appropriate for some aspects to be reserved for the governing body?
- does the audit committee have the opportunity to discuss how well key risks are being managed with those responsible for them?

## Risk appetite

### Key points

- The concept of risk appetite is under-developed in the higher education sector and is not always clearly defined by institutions.
- Where institutions have defined their risk appetite, they have used different methodologies depending upon their circumstances.
- Just as an institution's strategy will be influenced by changing circumstances, so should its risk appetite. Risk appetite should be subject to annual review.
- Risk appetite should consider the risk tolerances of an institution's stakeholders.

48. The first step for any organisation seeking to improve the alignment of its risk management activity with its key decision-making is the formal definition of the amount, and type, of risk that is acceptable in the pursuit of its business objectives. This is its risk appetite.

### Risk appetite in the higher education sector

49. Risk appetite as a concept is relatively under-developed in the higher education sector, as it is in other sectors. All the institutions we spoke to acknowledge the need to define a risk appetite; but in many cases risk appetite was seen to be inherent in the way that the institution conducts itself, rather than something which needs to be periodically and formally reviewed and described.

50. An institution's risk appetite should be linked to its strategic framework, yet it was not always clear that this was the case.

51. This is not to say that a great deal of time and effort should be directed at understanding an institution's risk appetite, but without this understanding managers may be exposing the institution to unacceptable risk, or to not taking risks where they should.

52. We found that many institutions do not have a proper definition of risk appetite. There is wide recognition that risk management should not be about making an institution risk averse (and this point had been made at governing body level). However, some institutions may have moved straight from identifying risk to treating it, without proper consideration of risk appetite. This approach can ignore the context of the risk and can lead to the implementation of costly, ill-conceived and inadequate 'quick fixes'. Such dangers can be prevented through a proper understanding of risk appetite.

### Defining risk appetite

53. There is no simple and readily understandable method of valuing every residual risk in monetary terms. If this existed it would be simple to define the limits of an institution's risk appetite, and a residual risk would either be acceptable or not.

54. Our review encountered a number of methodologies for defining risk appetite, both subjective and objective.

#### Example 9 Risk appetite: score limit

One institution scores each risk, by applying a scoring matrix. Risk appetite has been defined as any risk with a score of greater than 'x' being unacceptable.

55. It will not always be necessary to apply a process as regimented as a score level, but this does provide a transparent and logical framework within which to operate.

56. In other circumstances, the subtleties of risk scoring may become an unnecessary detail.

#### Example 10 Risk appetite: a defining statement

One institution recently found itself in financial difficulties and has worked in partnership with the

funding council to ensure continued operational viability. The governing body decided that the institution could not afford to take risks until the position had improved, and this was incorporated into the risk appetite statement.

57. It can be seen that there is no one correct way of defining risk appetite and this will be heavily influenced by an institution's circumstances.

### **The context for risk appetite**

58. Our review found that most institutions recognised that their appetite for taking risk was influenced by their portfolio of activities, their structure and other factors such as their market position and financial health.

59. Just as an institution's circumstances are subject to change (being influenced by macro external factors and internal developments) so it is appropriate that an institution's appetite for risk should be regularly reviewed and updated.

#### **Example 11 Risk appetite: annual review**

One institution reviews its risk appetite annually as part of its strategic planning process.

'The university's general approach is to minimise its exposure to risk. It will seek to recognise risk and mitigate the adverse consequences.

However, the university recognises that in pursuit of its mission and academic objectives it may choose to accept an increased degree of risk. It will do so, subject always to ensuring that the potential benefits and risks are fully understood before developments are authorised, and that sensible measures to mitigate risk are established.'

The revised risk appetite statement is incorporated into the annual plan and discussed and approved by the governing body.

60. The example cited above was the exception rather than the norm in our review, in that risk appetite appears to be revisited infrequently by institutions once it has been set.

61. Institutions recognised that the higher education sector is undergoing a period of changing dynamics, influenced by factors such as:

- variable tuition fees
- commercialisation opportunities
- increased competition for students
- diversification of institutional income (leading to some of the risk areas below)
- increased exposure and reliance upon overseas markets
- involvement in partnerships and associations
- restructuring.

62. Despite these significant and wide-ranging factors, there was no sense that risk appetites were being adjusted by institutions accordingly.

### **Risk appetite and stakeholders**

63. Where there is a tendency to associate risk management strongly with accountability to outside stakeholders, this can impact on the risk appetite of an institution, particularly in areas of activity perceived to be higher risk. Stakeholders' willingness to accept an honest assessment of risk factors and levels within institutions is a key element in making risk management work.

64. To establish its risk appetite, an institution needs to understand the current risk tolerances of its

stakeholders. We did not find any institutions that formally considered identifying those stakeholders affected by the institution's decisions and actions, and their degree of comfort with various levels of risk. Understanding the current state of risk tolerance of government, funding councils, students, business and other stakeholders could help the institution to define its risk appetite and to decide what risks must be managed, how, and to what extent.

65. Risk tolerance of stakeholders can be determined by consulting them, or by assessing their response to varying levels of risk exposure. Risk tolerances may change over time as new information and outcomes become available, as expectations evolve, and as a result of stakeholder engagement. HEFCE's plans to notify institutions of its risk assessment of them will contribute to this understanding of stakeholder tolerance.

## Resourcing

### Key points

- Institutions had different approaches to identifying what resources were needed for risk management processes.
- There are significant benefits to integrating risk management into existing processes.
- The approaches to resourcing partly depended on the size and type of institution.
- Academic staff can make a positive contribution to risk management.
- Some up-front and continuing investment is needed to implement risk management effectively.
- The role of risk management steering committees is evolving as risk management procedures become embedded in institutions.

66. Effective management of risk should assist in the efficient allocation of resources. Risk management provides a tool for giving due weight to any activity being resourced on the basis of the actual risk levels.

### Resourcing risk management

67. Institutions took a number of approaches to resourcing risk management, ranging from the investment of extra resource to drive the risk management process, to a clear ruling that the introduction of risk management must be completed within existing resources.

68. Some institutions identified a need to reallocate resources in training, communication, promotion and process support to ensure that there was common understanding, management and communications. This was on the basis that risk management processes cannot take hold and be practised routinely by management and staff without some dedicated up-front and ongoing investments.

69. All institutions visited had some sort of 'designated responsibility centre' that acts as a source of expert support to others, and to sustain the process and ongoing communications about risk. This centre is the most significant demand on resources for institutions.

70. For many institutions, resourcing has been a question of striking a balance between acceptable risk and control, and risk management processes. Resourcing is often tailored to their size and complexity.

### Integration into existing resources

71. Where institutions have integrated risk management into existing processes they have done so after identifying some clear benefits, in that risk management:

- is less likely to be seen as a 'bolt-on'
- becomes embedded more quickly
- links more effectively to existing processes such as strategic planning
- can often be implemented more economically.

72. Where this approach has been taken, completion and updating of risk registers has fallen either to staff within central functions, and/or (where the processes are well embedded) to existing staff (such as resource or general managers) within faculties and departments. The main cost to the institution is the opportunity cost.

### Additional staffing

73. Some institutions have supplemented their staff resources to handle any additional work associated with the implementation of risk management processes and procedures.

74. In a number of instances workloads have been reallocated to enable staff to take on risk management responsibilities. Some institutions have also incorporated risk management into job titles,

reinforcing the importance of resourcing this area.

#### **Example 12 Risk management: dedicated staff**

One institution has appointed a part-time 'Risk and Value For Money Officer', whose responsibilities include ownership and facilitation of key risk management processes. This new post has significantly assisted in driving forward risk management at the institution, and provides a central reference point for staff and management to consult.

### **Smaller institutions**

75. For institutions that are smaller and/or less complex, it may be appropriate for 'leaner' processes to be put in place for managing risk. In such cases, primary responsibility for risk management processes might rest in the hands of a few central, senior managers with less (or no) input from department/faculty managers.

76. This approach makes the best use of limited resources, but it can restrict the embedding of risk management as academic or less senior non-academic staff may not be fully initiated into an institution's risk management objectives.

### **Larger institutions**

77. Where an institution is larger and/or more complex, then the ownership and resourcing of risk management processes could follow a more involved pattern:

- the ownership for risk management processes might be in the hands of a central senior official such as the university secretary/registrar or head of administration
- ownership and responsibility for identifying and managing risks (by implementing controls and actions for improvement) rests with faculty/ departmental managers, both academic and non-academic.

78. This approach is more likely to promote a top-down review of risk which may be more successful in identifying and managing it.

#### **Example 13 Risk champions**

One larger institution has appointed 'risk champions' at departmental/faculty level. These are existing members of staff who have responsibility for promoting risk management in the department. The institution has also found it beneficial for the risk champions to share aspects of risk management processes between departments.

### **Professional facilitators**

79. A number of institutions have used professional facilitators as additional resource, particularly in the early stages, to introduce concepts and help to shape frameworks and identify risks. However, it is more usual for a facilitator to be used at the start of the risk management process.

#### **Example 14 Professional advisers**

One institution has developed a beneficial relationship with a firm of professional risk management facilitators and advisers, which includes providing risk seminars and involving the facilitators in the institution's business school.

### **Involvement of academic staff**

80. Most institutions have recognised the need to involve a broad cross-section of staff in the risk management process, both non-academic and academic.

81. Some difficulties have been acknowledged in obtaining the buy-in of academic staff to the benefits of explicit risk management, particularly where the process is owned by staff in a central administrative function. The challenges often relate to a devolved organisational structure coupled with cultural resistance of staff. Many institutions are addressing these challenges through training, education and embedding processes. Communication is a key tool, particularly the reinforcement of the messages that:

- risk management can improve the probability of success in an activity
- academic staff have already been carrying out risk management without necessarily knowing it.

82. It should also be recognised that academic staff are best placed (being in direct contact with students and subjects) to identify and manage the risks most closely associated with the core activities of institutions' academic quality.

#### **Example 15 Academic risks**

One institution has introduced a new approach to identifying and managing academic risk. For each academic department, staff are required to identify risks and underlying factors and to work through scenarios considering how the risk factors interact. This is an annual, forward-looking exercise and is used to feed messages up to the academic board. This has assisted in improving academic quality procedures which had previously been very bureaucratic.

#### **Example 16 Academic expertise in risk management**

One institution used its existing academic facilities to good effect in its risk management arrangements. An expert in risk management from the business school sat on the risk management committee. The risk management needs of the institution are also being supported by undergraduate research projects, in areas such as best practice in corporate governance statements.

### **Risk management committees**

83. Many institutions have set up committees to oversee the implementation of risk management practices and procedures. Often these are management committees, although they can sometimes be supported by members of the governing body.

#### **Example 17 Risk management groups**

One institution has established a Central Advisory Group to advise on the development of risk management processes. Significantly, this group includes academics from the institution's business school, tapping into existing expertise. This practice is evident at another institution, where the Risk Management Co-ordinating Group, a management sub-committee, includes an academic expert in risk management from the local business school.

84. As risk management processes become embedded within the daily routines and management of the institutions, these committees will evolve or be replaced. Institutions with more effective risk management processes have increasingly charged their senior management teams with this role, rather than establishing separate committees. In such cases, risk management processes have become more effectively embedded because the senior management team is in a better position to identify and manage risk, and to promote risk management. One institution visited was exploring a new role for its risk management committee as a facilitator in sharing good practice between academic departments.

## Exploring and assessing the risks

### Key points

- Formats for assessing and rating risks tend to be similar.
- Net risk is the risk faced after considering mitigating controls – residual risk.
- There is variable practice in the rating of gross and net risk.
- Controls and actions for improvement should be assessed and documented.
- Control effectiveness should be considered.
- There are different ways to present the findings of risk assessments.

### Risk register formats

85. Many institutions have adopted similar formats for exploring, and subsequently rating, risks and exposure. On the whole they have documented the following information in the form of a risk register:

- risk type
- risk description
- consequence or further narrative about the nature of the risk
- rating (by impact and likelihood)
- controls
- actions for improvement.

Figure 2 illustrates an example risk register following this format.

### Gross and net risk

86. There is variable understanding in the sector of the concepts of gross and net risk. Some institutions were unclear when challenged as to what their rating of risk by impact and likelihood actually showed:

- was it the assessment of the institution's risk at the gross or net level?
- what do we mean by 'gross' and 'net'?

87. Gross risk represents the assessment of a risk before anything is done to mitigate or manage it, that is, before controls are put in place.

88. To some, the assessment of gross risk is an academic exercise because in reality there are usually some controls in place. However, as will be discussed later in more detail, an initial assessment of gross risk does have a purpose when considering whether the controls in place are efficient.

Figure 2: An example risk register from the private sector

Risk Category	Risk Sub-Category	Specific Risk	Impact/Likelihood	Responsibility	Key Control Activities	Ongoing Actions
Strategy	Strategic direction	Clarity and understanding of Group strategy Alignment of Division strategy with Group strategy Clarity of Division strategy	H / H	AJB	Annual business planning process	
		Managing client expectations	L / H		Planners / sales receive feedback from clients and take this feedback into account in planning subsequent .	Planners/sales to relay feedback received from clients on to other internal depts
		Health and safety risks	H / L		Formal health and safety training for planners. In addition, on the job, senior planners supervise less experienced planners on health and safety issues.	
	Liaison with Operations*	Product knowledge	? H / H		As per controls for product planning and mgmt and Profitability / Pricing of products	
		Billing information	? H / H	/Operations	Division input to training conducted by other internal departments.	
		Customer liaison roles	? H / H		Liaison between sales team and operations	
	Staff	Management succession	H / H	HR	Senior Management hold workshops with HR and discuss this issue.	Awaiting proposals from Senior Management to feedback on the Senior Management workshops.
		Staff retention (especially sales)	H / H	HR	Introduced annualised hours and higher salaries for sales. Introduced a development planning matrix, with the intention of encouraging sales staff to be multi-skilled and allowing them to take more control of their career paths.	Awaiting proposals from Senior Management regarding plans to rollout annualised hours across the rest of the business.

89. Net risk is therefore the risk faced after putting in place controls or mitigating actions. Some call this the 'residual risk' or 'residual exposure'. It is this residual risk that it is important to understand.

90. It is important that institutions define clearly what their risk ratings show and ensure that all participants in the risk review process understand the thought process they should go through, otherwise incorrect assessments could be made.

### **Considering and documenting the controls**

91. Logically, the next step after considering risk at the gross level is to consider the controls or mitigating actions that are in place. There are a number of approaches to assessing the mitigating controls, and there is a wide range of opinions regarding the need to document them. Some see documenting controls as an overly bureaucratic measure. Other institutions consider, and document, controls and actions for improvement within their risk register.

92. It is up to each institution to follow the process they consider most effective.

93. However, certain questions should be considered by management and internal auditors when reviewing and documenting controls and residual exposure to risk. These include:

- are the controls adequate to reduce the residual risk to an 'acceptable' level?
- are the controls actually being carried out regularly?
- can we monitor and occasionally test them?
- are further actions required to reduce the residual risk to an acceptable level?
- can we track and monitor that these actions are implemented?
- if we wish to assess and rate the risk at the net level, do we have sufficient information documented?
- as part of review procedures, can we assess whether the mitigating actions and the cost of performing them are efficient and commensurate with the risk?

94. Best practice involves documenting key controls succinctly, and separately from the actions for improvement. This separate documentation facilitates the review of controls for adequacy and efficiency, and helps in monitoring and testing the controls.

### **Risk assessment and exposure ratings**

95. Risk scoring is a useful guide, but it is not the only driver in risk management processes.

96. Most institutions have implemented the concept of assessing risk using impact and likelihood criteria. The most common way of assessing each criterion has been using high, medium or low (1,2,3) or a scale of 1-10.

97. One area that could be more widely developed for managing risk is the rating of control effectiveness. This would aid in explicitly considering the gross risk, control and net risk – that is, the risk exposure. The previous good practice guide (HEFCE 01/28) included a 'risk exposure matrix' as a means of illustrating the exposure faced by an institution. Risk exposure matrices are not widely used, but can improve clarity in risk management.

### **Assessing net risk**

98. There are essentially two ways in which net risk can be assessed:

- a. Method 1. The likelihood and impact of the net risk are assessed after the controls are in place.
- b. Method 2. The impact and likelihood of the gross risk are assessed, and then the effectiveness of the control rated, and a factor applied to establish the net risk.

Below are two examples from institutions using the different methods.

### **Example 18 Assessing net risk: method 1**

One institution has considered the risk of failing to retain some key academic staff. The impact could be high (or 3 on a 1-3 scale) as in some courses the high-profile academics help to keep student applications high and therefore maintain income, as well as maintaining service delivery. The likelihood of staff leaving is also high (3) as they are mobile and in demand. However the institution is satisfied that the retention initiatives in place, as well as targeted recruitment programmes, reduce the gross risk quite considerably. The university benchmarks its salaries and rewards and knows that it is in the upper quartile against its peers. Taking these controls into account, both the impact and the likelihood fall to medium (2). The risk score is achieved by multiplying the impact score (2) by the likelihood score (2) and therefore the net risk is rated as 4.

### **Example 19 Assessing net risk: method 2**

Using a similar rating system and taking the same example as for method 1, the gross risk is rated as 9 (ie 3 x 3). The control effectiveness is then considered using:

- a. Controls are tight /little or no scope for improvement in control (0.25).
- b. Some scope for improvement in control (0.5).
- c. Controls are light/non-existent (1.0).

As the controls are considered to be effective, with only some scope for improvement, a factor of 0.5 is applied (factor b). This reduces the risk rating in the example to 4.5.

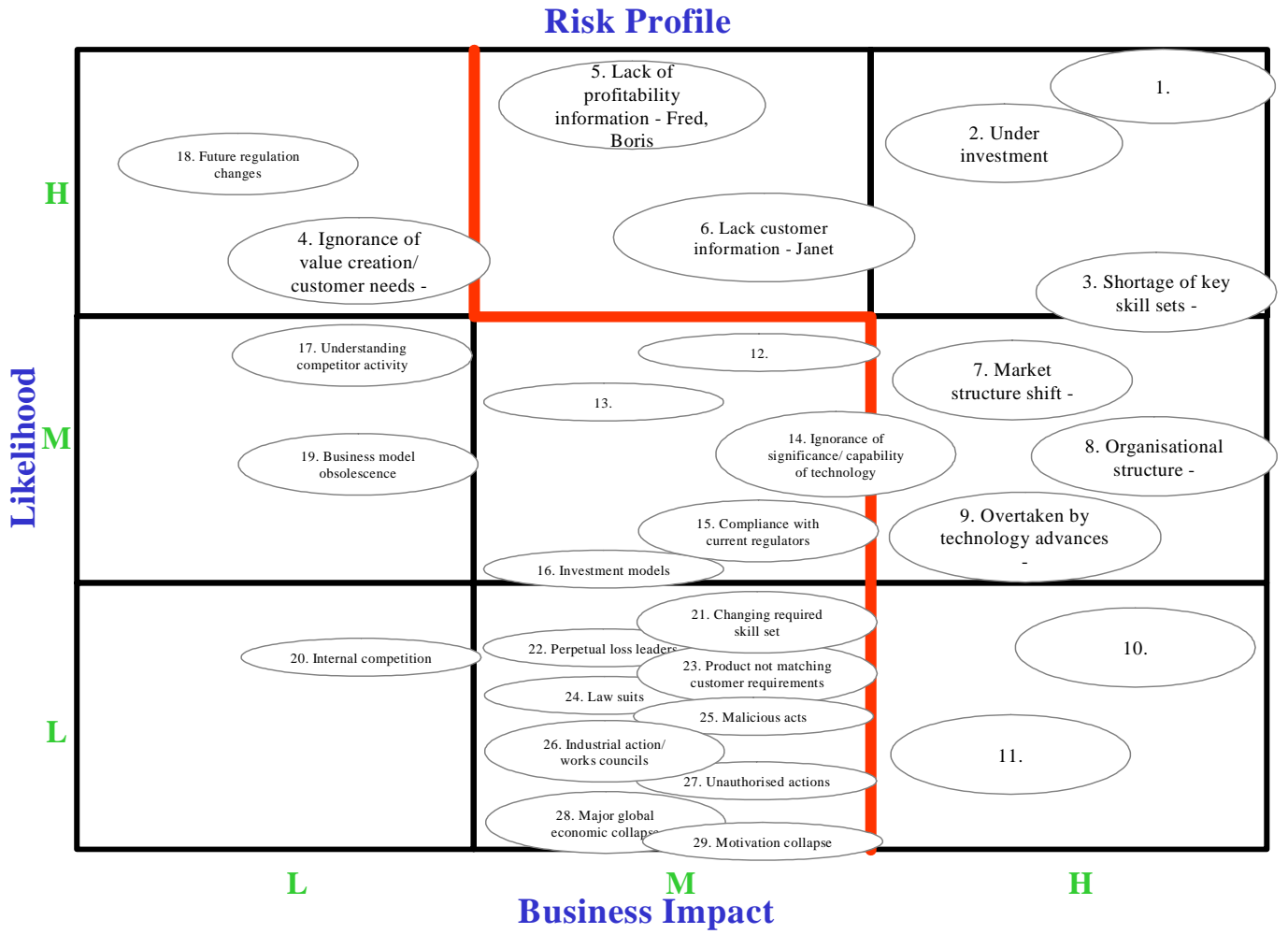
## **Presenting the findings**

99. There are a number of ways to present the findings of risk assessment, the most common being:

- nine-box matrices (3 x 3) using high, medium and low impact and likelihood (see Figure 3 below)
- impact and likelihood graphs using 1-10 on each scale
- tabular format.

100. There is an increasing trend for plotting the risk rating over time, tracking improvements and slippage. Many institutions are also setting targets for improvement in risk scores. Tabular formats lend themselves to this type of analysis. Graphs may become difficult to read with this much detail.

Figure 3: Use of matrix to present risk findings (from the private sector)



## Actions for improvement

### Key points

- Institutions should consider the trade-off between resources and risk when looking at options for mitigating the risk.
- Actions should dovetail with existing work and plans.
- Actions for improvement, timescales and people responsible should be clearly documented.
- Progress with implementing actions for improvement should be tracked.
- Internal audit can make an effective contribution to tracking actions for improvement.

### Options for treating risk

101. We found that documented actions for improvement feature in the risk registers of most institutions.

102. Actions for improvement should be designed to treat those risks that are considered unacceptable by the institution. A number of options are available:

- avoid the risk
- transfer the risk
- retain the risk.

103. Where the institution takes the final option, to retain the risk, then it should be reduced if possible.

### Different solutions for reducing the risk

104. For any organisation there will be a trade-off between the level of risks and the cost of reducing them to an acceptable level. The analysis of risks should have provided sufficient understanding of the factors which affect the likelihood and consequences to suggest methods by which the risks can be reduced.

105. The most effective methods of risk reduction are those which redesign the systems and processes so that the potential for an adverse outcome is reduced.

106. When considering actions for improvement, the type of solution also needs to be considered:

- a satisfactory (but not optimum) solution
- the most cost-effective solution
- the accepted practice (industry norm, good business practice)
- the best achievable result (given current technology)
- the absolute minimum result that could be accepted.

107. Which solution is acceptable depends on the circumstances and the established risk context – defined by the institution's risk appetite.

108. It is also important that any solutions should, where possible, dovetail with the existing work of managers and plans of the institution.

### Documenting the actions

109. Where risk reduction is considered both feasible and cost effective, then a budget and a responsible person will need to be allocated to the actions.

110. Some reporting templates focus on generating improvements, but do not always include implementation timescales and responsible people. By allocating responsibility and a deadline for action it is much easier to monitor its achievement.

111. In many cases, documentation of existing controls is grouped with actions for improvement, making it almost impossible to track implementation of improvements.

## Tracking actions for improvement

112. Rigour needs to be applied in tracking the implementation of actions to mitigate risk. Current processes and procedures used by institutions differ widely.

### Example 20 Risk assurance mapping

One organisation maps how and where assurances are to be obtained for each risk. This included assurances from the risk owner/manager, reports on progress of activities, policies and procedures in place, internal audit reviews, evidence of discussion in committees, and reviews of progress on strategic issues. This assurance mapping provides an audit trail that allows the board to sign off the corporate governance statement.

113. Most institutions documented actions for improvement in the risk register. In the same document were details of responsibility for improvement and timescales.

### Example 21 Risk register: summary of actions for improvement

At one institution actions for improvement were summarised on the risk register. Detail underpinning the actions, cost, responsibility, timescale and other factors were all recorded elsewhere, typically within strategic plans and similar documents, and cross-referred to the risk register. This maintained clarity in the risk register and made it easier to update and maintain.

114. Institutions use different mechanisms to track risks, including:

- self-assessment by risk owners that actions have been taken
- use of internal audit to confirm that actions for improvement have been addressed
- risk owners providing reports to the audit committee (or other relevant forum) on those risks managed
- using the risk management officer to check that actions have been taken.

## Implementing actions for improvement

115. It is important to ensure, however the detail is documented, that actions for improvement are implemented. Ways to support this include:

- a tracking mechanism to monitor progress towards implementation
- if the action plan is large, prioritising actions
- providing adequate resources to implement the action within the timescale specified.

116. Best practice would be to include the status and ownership of key actions in routine performance reports (monthly or quarterly).

117. In some risk registers, responsibility for specific risks has been placed at an inappropriate level to ensure that effective action is taken. For example, at some institutions responsibility for strategic risks has been mainly assigned to the vice-chancellor, but the practicalities of managing those risks will lie at a lower level within the institution.

## Use of internal audit

118. Internal audit is often used to track actions for improvement. In many respects this sits well with the central role of internal audit, related to internal control and governance. The interpretation of this role has changed to focus on providing advice, recommending control systems, and monitoring their implementation. Further guidance on this is provided in 'Risk-based internal audit in higher education' (available on the web at [www.hefce.ac.uk/finance/assurance/intext/guide.asp](http://www.hefce.ac.uk/finance/assurance/intext/guide.asp)).

119. In many institutions, internal auditors have evolved roles as facilitators and organisers of risk identification and assessment, generally through workshops. Education of staff and effective communication have become central to their work.

120. Where internal audit is used to track actions for improvement, care should be taken to ensure that internal audit does not become too closely involved in the risk management process and so loses objectivity.

## Prioritisation of risk reporting

### Key points

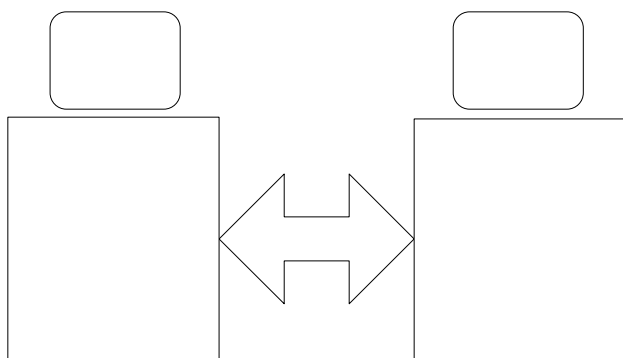
- Reporting on risks should be tailored to the needs of different audiences - the most effective reporting is presented simply.
- Mechanisms for reporting to stakeholders could be further developed.
- Audit committees and governing bodies should provide more of a steer on the type of information that they want on risk management.
- There is no 'right' number of risks which must be reported on. However, the number must be manageable, based on a prioritisation system.
- Many institutions use key risk indicators, but these are often not developed with any rigour.

121. Internal reporting on risk management is a key tool for ensuring that risks are effectively dealt with and managed.

### Reporting of key risks

122. In an institution, reporting on risk may be aimed at several different groups. Each group will require different levels and types of information.

**Figure 4: Reporting on risk management**



123. Each institution should determine what is appropriate to report to these groups, and to obtain feedback from them to ensure that most value can be obtained from their input.

124. There are different factors to be considered for reporting to different audiences.

### Reporting to external and internal stakeholders

125. In some ways reporting to stakeholder groups is very defined. For example, through the Statement of Internal Control in the annual accounts an institution can send out a clear message about its attitude to risk. This is particularly true where this statement has been tailored to reflect the institution's circumstances, rather than using a standard model. The more 'advanced' institutions have developed reporting mechanisms which include processes for bringing together all the elements of internal control in a single paper, which is presented to the audit committee in support of the statement made.

126. It is for individual institutions to determine how they communicate with other stakeholders about risk. Such reporting is probably not as sophisticated as it could be, and is often given low priority by institutions. Examples of good practice in this area include:

- sharing data on risk management through the institution's internet and intranet sites
- a periodic newsletter on risk management distributed to students and staff.

127. Internal reporting on risk management is a key tool for ensuring that risks are effectively dealt with and managed. The owner of the risk management process has a central role in defining what is reported, and how often. However, it should also be possible for key groups to specify the type of information they would like to see about risk.

## Reporting to the audit committee

128. This is particularly the case for the audit committee, which in most institutions has delegated responsibility for overseeing risk management.

129. Questions that audit committees should consider in relation to risk management reporting include:

- what type of information do they want to see on risk management?
- does this information relate to the audit committee's responsibilities in relation to risk management?
- how often does the audit committee want information on risk management? For example, at every meeting?
- how much information does the committee want on risk management?

130. One institution reported in detail on one key risk at each audit committee meeting. This approach may not suit all institutions, but it provided the committee members with a very good understanding of the management of key risks.

### Example 22 Audit committees: assurances

At one institution, the head of each directorate is called before the audit committee to explain how risk is being managed in their directorate. They are required to produce a mini-statement of internal control and to outline the key risks faced by their directorate. This process helps the audit committee gain assurance on risks below corporate level.

131. In another institution, risk management is a standing item on the audit committee agenda, but this approach will need to be balanced against audit committees' (ever increasing) workloads.

## Reporting to the governing body

132. The same questions will also be relevant to the governing body. It is not enough for the governing body to delegate responsibility for risk management to the audit committee. It is important that the governing body receives relevant information on the key risks faced by the institution.

### Example 23 Reporting to the governing body

One organisation reports quarterly to its board on key risks as part of the information on strategic and operational performance. The risk matrices for the current and previous quarters are shown on one page and this is backed by two pages listing the top 20 risks.

## What is the right number of risks?

133. For many institutions, their full risk register may contain as many as 100 risks. There is no right or wrong answer as to how many risks it is appropriate to have on a register. The key to making this information effective and usable is to prioritise it.

134. Clearly it would not be appropriate to present 100 risks to the governing body at every meeting. Prioritisation of key risks down to the top 10 or so for senior monitoring groups will make their input more valuable. An institution's risk appetite will be a factor in determining what type of risks and how many are reported to the governing body. However, the governing body should also give a steer in setting out what information it wants on risk.

135. It is important that detail underpins any summary of risks, and that rigour has been applied in any assessment and prioritisation mechanism. If risks cannot be prioritised down to a reasonable number then there may have been a lack of clarity by participants in the original assessment process.

136. Many institutions have found it helpful to maintain a rolling top 10 risks (or other manageable

number). This has the following advantages:

- it is easier to track changes in the institution's risk profile
- it is easier to see new risks emerging and others become less critical
- it helps to develop a broad overview of an institution's evolving nature.

137. Risk reporting should provide an integrated view of risk across the institution and incorporate both top-down and bottom-up elements. Currently few institutions have both top-down and bottom-up reviews in place.

138. The ability to recognise new risks and changes to existing ones is a key part of managing risk. We found that this was happening through periodic (annual or six-monthly) reviews of the risk register, but the tracking of risks was not always so transparent. This was particularly the case with risks that had 'dropped off' the register.

139. The following categorisations of risk may be useful for a risk register:

- new risks
- enduring risks
- challenging risks
- dying risks
- dead risks
- re-emerging risks.

140. Some institutions have implemented self-assessment procedures for reporting on risks.

#### **Example 24 Risk assurance: annual questionnaire**

At one institution an annual risk questionnaire is used to provide assurance to the governing body on those risks managed at an operational level. This requires formal sign-off by departmental heads on questions derived from the risk register. The questions cover the operational risks faced by the institution, including academic, operational, environmental, physical and financial risks.

### **Key risk indicators**

141. Few institutions have yet considered and clearly defined a set of key risk indicators.

142. Where key risk indicators are in place, they are based around the achievement of objectives. Many institutions have undertaken a top-down review of risk, taking account of risk as something that hinders the achievement of objectives. It is possible to drill down through the institution to identify how objectives impact on each level and then translate the objectives into a performance indicator. For those key risks for the organisation, the relevant performance indicators become key risk indicators.

#### **Example 25 Risk indicators: 'traffic light' reporting**

One institution has incorporated risk management into the monthly operational reporting cycle. Risks are flagged using a traffic light system and are central to the reporting (rather than being a bolt-on). Managers have found that this has encouraged ownership and embedding of risks, as well as providing a better understanding of how the organisation is performing across all its activities.

143. The development of key risk indicators in the sector has not been undertaken with any rigour. Many institutions have adopted existing performance indicators – such as student numbers, and health and safety incident reporting – and married the information with the risk management reporting processes. This could be developed and made more efficient by making a clear link between key risks and indicators for each, developing new indicators where necessary.

144. It may also be appropriate for institutions to set risk reduction targets as a key indicator. The dynamics of an institution's risk profile will change constantly, and an effective risk management system is about reducing the level of risk that the institution is exposed to.

## Embedding risk management

### Key points

- Effective risk management needs to be integrated into existing processes.
- Embedding of risk management in institutions is variable. Some recognise that an iterative process is needed over a number of years to achieve 'true' embedding.
- Risk management has been embedded in the strategic and operational planning in some institutions, and in some at departmental level.
- Personnel practices can assist in embedding risk management.
- Consideration should be given to embedding risk management in non-core activities.
- Embedding risk management will change the role of some risk management processes.

### Making risk management 'disappear'

145. Most institutions we visited observed that effective risk management cannot be practised in isolation. The institutions that had embedded risk management most successfully have built it into existing decision-making structures and strategic and operational processes.

146. The overall objective should be to embed risk management in the daily activities of individuals and teams while making 'bolted-on' risk management processes disappear; making it part of the 'language of management' in the institution.

147. Embedding risk management will include ensuring that the process is:

- responsive to the institution's objectives, organisation and environment
- owned by management
- built into the way business is conducted
- regularly and relevantly reported.

148. At one level, good risk management is just good management, and might appear to be little more than considering whether existing management practices are robust. However, as a minimum the regular review procedures should identify and assess management practices in relation to key risks. If this is not done systematically there is a greater likelihood of serious gaps in any system of internal control.

### How embedded is risk management in the sector?

149. All institutions that we visited considered risk management to be embedded. The extent of this embedding and how it is defined varied from institution to institution.

150. At one level some institutions considered risk management to be embedded where they had basic top-level risk management procedures in place, and these had been operating for a period of 12 months or more.

151. In contrast, some institutions felt that to achieve a beneficial end product from risk management they needed to be continually embedding and enhancing their risk management processes. They did not consider that 'true' embedding could take place in less than two years, and may take longer.

152. These institutions argue that good practice for integrating risk management is to build an organisational culture in which everybody is a risk manager.

153. Some institutions indicated that this is more important than developing extensive policies and procedures, as management of risk is then embedded in their management philosophy. Staff that take responsibility for their actions and outcomes become risk managers.

154. We also found that the extent of embedding was partly driven by the type and size of institution.

155. Smaller/less complex institutions have tended to adopt top-down risk management processes. This suggests that risk management processes are overlaid onto existing management processes rather than

being truly embedded. Better practice would be to fully involve faculty and departmental management (academic and non-academic) in the risk management processes, to make it part of the institution's culture.

156. Larger and/or more complex institutions tend to have a wider group of individuals involved in the risk management process, and their processes are more devolved. However, for some this is still an overlaid process. Others have had substantial success in embedding a consideration of risk within the annual budgeting cycle or strategic plan reviews.

### **Business planning**

157. Many institutions have taken the approach that their objectives and strategies for risk management should complement their existing strategy, vision and goals.

158. These institutions have taken the opportunity to integrate risk management with their planning process, and gain immediate benefits from being able to monitor threats to their business objectives.

#### **Example 26 Reporting risk management as part of existing processes**

One institution has produced risk-related outputs of the business plan, such as the SWOT analysis, in a compatible format with the risk management process. This has been used to populate a top-down, forward-looking risk register. This information is then combined with that from the bottom-up risk assessment to provide a comprehensive and robust picture of risk.

159. Some institutions have begun to link the risk management and business planning processes in terms of both format and timing. In some institutions, departments are required to undertake formal planning and risk management processes as part of the strategic/budget planning cycle.

#### **Example 27 Integrating risk management with business planning**

One institution has taken the opportunity to revise its business planning process and integrate it with risk management processes. The risk register is built around the annual operating plan and shows the risks of the institutional objectives not being met. Members of the governing body receive the output document periodically, and have found that it has enhanced their understanding of the key operational issues being dealt with by management.

160. Some institutions are planning to develop cost and financial implications for risks which can be fed into the business planning process, and enable sensitivity analyses to be run against risk factors.

161. Few institutions have yet implemented this type of structured consideration of future options and associated risks. Best practice is to develop a number of future risk scenarios, with the key risks and strategic options to respond to them. Probing and challenging the business plan from a risk perspective should ensure a robust plan is developed.

162. There is also scope to improve the articulation of risk appetite through business planning, by considering the relative risks of proposed initiatives, investments and major projects.

### **Embedding risk management in decision-making**

163. Examples of good practice for embedding risk management in the decision-making process at institutions include:

- explicit consideration of risk as part of existing reports and in respect of key decisions, such as those relating to capital programmes or new markets
- key decisions are underpinned by the timely involvement of all relevant functions (academic and non-academic) and identification of key risks and responses
- adopting common definitions of risk
- evaluating both the short and longer-term impact of the key risks identified, such as reputational impact.

### **Example 28 Assessing risks of a capital project**

One institution is about to embark on a major extension to its campus. Risk management has been used by management and the governing body to build a complete picture of the opportunities and risks associated with the project and will be used as part of the monitoring process.

### **Enhancing performance**

164. A key development area for all institutions is to link the ongoing assessment and monitoring of risk with monitoring the performance of all parts of the institution against the objectives and targets set out in their business plans.

165. Knowledge gained through the risk management process can be used to understand any performance shortcomings and variances in an institution. Forward-looking measures relating to key risks should be developed to provide early warning of possible crystallisation of these risks.

### **Managing risk at departmental level**

166. Many institutions are large and complex in terms of activities and structure. For such institutions it is not practical or effective to manage risks centrally. Indeed, the majority of institutions have looked to their academic and service departments to manage risk at this level, and see this as part of embedding risk management.

### **Example 29 Risk registers: departmental**

At one institution all academic schools and service departments are required to complete and maintain local risk registers as part of their annual planning process. This helps them play an active role in the risk management process. It was noted that the process for identifying risk may vary from area to area, but all risks are scored and prioritised using a standard methodology.

Academic deans at this institution commented on how risk management has added focus and a more commercial ethos to their areas of responsibility.

### **Completeness of embedding**

167. Most institutions recognise the need to disseminate risk management practice and procedures at all levels in their organisations, and see this as part of the embedding process.

168. Consideration should also be given to extending risk management beyond the 'core' activities. In a period when higher education institutions are being encouraged to work in partnerships and collaborations, a number of areas may be peripheral to the vision of central management:

- partnerships and joint ventures
- subsidiary companies
- students' unions.

169. In many institutions this type of activity can present a higher risk profile. So it is appropriate that, just as risk management procedures are embedded at department level, they should also be embedded within non-core activities.

### **Embedding risk management through HR practices**

170. The use of risk and opportunity management to enhance performance can be achieved by encouraging everyone in the institution to be a risk manager. This can be linked to human resources (HR) initiatives such as:

- encouraging managers to develop knowledge and skills in risk management through training programmes and self-development
- including risk management as part of staff performance appraisals
- aligning risk management with objectives at all levels of the institution

- introducing incentives and rewards linked to risk management
- recruiting on risk management ability as well as experience
- building risk management into staff inductions
- having managers 'champion' risk management
- encouraging innovation, while providing guidance and assistance in situations that do not turn out favourably.

171. People are key to any risk management process, and people initiatives can be used to help risk management embed and operate effectively.

### **Embedding controls**

172. Internal controls are an integral part of managing risk. Good practice is to embed controls within processes wherever possible rather than 'bolting them on'.

173. Where necessary, control systems will need to be improved to take into account risk management and results.

### **Changing structures**

174. In institutions where risk management is becoming increasingly embedded, the structures originally created to promote and establish risk management are evolving.

#### **Example 30 Risk group: evolving role**

One university had established a Risk Management Co-ordinating Group as a management sub-committee to help establish risk management procedures. Now that a sound risk management framework has been established, this group is considering its future role. Its original purpose has become increasingly redundant as the Executive Group has subsumed risk management procedures within its day to day business.

One option for the Risk Management Co-ordinating Group is to continue to work itself out of business. However, it also sees a role as a forum for sharing risk management good practice between academic schools and service departments.

### **Stand-alone risk management processes**

175. Institutions that have developed stand-alone risk management systems do not benefit from the more comprehensive approach adopted by others. In such cases there is sometimes confusion over how the system's outputs link into other operational and business planning processes. While stand-alone systems may be effective to some degree, they are often symptomatic of institutions where there are difficulties in convincing managers and staff of the benefits of risk management.

## Sharing risk management knowledge

### Key points

- Sharing risk management knowledge is part of communicating and consulting with all stakeholders.
- The sharing of risk management knowledge in the sector is variable.
- A variety of IT applications is used for capturing risk management information.
- Some institutions use their intranets and/or team briefings to share risk management knowledge.
- Sharing risk management knowledge should be incorporated in a communications strategy.

176. Communication and consultation with stakeholders, both internal and external, is an important element in sharing risk management knowledge. It can be defined as any two-way dialogue between stakeholders about the existence, nature, form, severity or acceptability of risks.

177. It is therefore critical that stakeholders have access to relevant information, and that this information is presented in a way they understand.

178. In most institutions each part of the organisation prepares their risk assessments in isolation from the rest. There is little sharing of risk information at faculty/departmental level or below senior level.

179. Some staff indicated that their institution could be uncomfortable with reporting risk exposures transparently, but nevertheless most felt that it would be valuable to share risk assessments more widely.

### Using technology to share data

180. Generally speaking there has not been widespread use of sophisticated electronic tools to capture and report risk data in any sector – private, public or not-for-profit. Apart from within extremely complex multi-location groups, opinions as to the value of electronic tools for risk and information capture are mixed.

181. Within the higher education sector, risk and control data are typically being captured using:

- databases
- spreadsheets (tailored and built into a model)
- risk registers in word processing packages.

182. Some institutions have recognised the value of sharing risk knowledge and lessons across the institution – between faculties and to and from the centre. Many are using their intranets to make this type of information available to the whole organisation.

183. For some institutions that store risk management knowledge on their intranet, managers still felt there was some way to go to establish a more 'joined up' method of storing and sharing risk knowledge. Undoubtedly a well constructed electronic database in which to store the various risk and control reports would facilitate sharing risk information across the organisation and creating a risk-aware culture.

### Internal briefings and seminars

184. A few institutions have established risk management team briefings, which are held periodically. These inter-disciplinary groups aim to share risk assessment outputs and good practice, address common issues and implement improvement actions.

185. Seminars can be an effective and cost efficient way to share information about risk management and the institution's approach to risk.

**Example 31 Seminars on risk management**

One institution organises periodic seminars on risk management, presented by high profile external speakers. The seminars take place during lunchtime and are intended to be accessible to all staff.

This same institution uses its weekly newsletter to publicise both the seminars and risk management in general to ensure that risk management maintains a high profile.

**Communications strategy**

186. Developing a communications strategy at the earliest stages in the risk management process can help to share knowledge. Efforts should be focused on consultation, rather than a one-way flow of information from decision-makers to stakeholders, especially those outside the immediate organisation.

## Annex A Self-assessment checklist for audit committees

This checklist for audit committees is not mandatory, but can be used to provide a 'sense check' of progress in implementing effective risk management. If this, or another risk management evaluation framework is used, then it may be appropriate for the institution to draw attention to this in the Statement of Internal Control.

	<b>Good practice questions</b>	<b>Is audit committee satisfied?</b> <b>Yes/No/NA</b>	<b>Follow-up steps necessary</b>
	<i>Involvement of the governing body (see paragraphs 28-47).</i>		
1	Does the governing body have sufficient involvement in risk management direction?		
2	Does the governing body provide direction in the risk management programme? Consider in particular the involvement in defining risk appetite and the link with strategic planning.		
3	How does the governing body know that risk management processes are operating effectively?		
	<i>Audit committees (see paragraphs 44-47).</i>		
4	Has the audit committee's role in relation to risk management been clearly defined?		
5	Do audit committee members understand what aspects of risk management they should be looking at?		
6	How often is the audit committee considering risk management?		
7	Has the audit committee set out the type of information that it wants to see on risk management?		
8	Is the audit committee responsible for overseeing all aspects of risk management, or is it more appropriate for some aspects to be reserved for the governing body?		
	<i>Risk appetite (see paragraphs 48-65).</i>		
9	Has risk appetite been clearly defined?		
10	Have all relevant criteria been taken into account when defining risk appetite? These criteria include the institution's strategy, the interests of stakeholders and financial performance.		
11	Is risk appetite consistently applied across the institution?		
12	Is risk appetite reviewed periodically to see whether it is still appropriate to the institution's circumstances?		

	<b>Good practice questions</b>	<b>Is audit committee satisfied? Yes/No/NA</b>	<b>Follow-up steps necessary</b>
	<i>Resourcing (see paragraphs 66-84)</i>		
13	Have sufficient resources been allocated to effectively implement risk management processes?		
14	Are all areas of the institution, including academic staff, sufficiently involved in risk management?		
15	Where a risk management committee is in place, is its remit and purpose reviewed periodically?		
	<i>Assessing risks and mitigating controls (see paragraphs 85-100)</i>		
16	Have risks been scored 'net' or 'gross' of mitigating controls?		
17	Are mitigating controls adequate to reduce the net (residual) risk to an 'acceptable' level?		
18	Is the cost of operating these controls efficient and commensurate with the risk?		
19	Are the mitigating controls being carried out on a regular basis?		
20	Are mitigating controls monitored and occasionally tested?		
	<i>Actions for improvement (see paragraphs 101-120)</i>		
21	Has consideration been given to options for treating risk?		
22	Where actions for improvement have been identified, are these allocated to individuals and given implementation timescales?		
23	How are actions for improvement tracked?		
24	Are actions for improvement reported on periodically?		
	<i>Prioritisation of risk reporting (see paragraphs 121-144)</i>		
25	Has consideration been given to reporting on risk management to stakeholders?		
26	Has the Statement of Internal Control been tailored to reflect the institution's circumstances?		
27	Have the governing body and audit committees given a steer to management on what information they want on risk?		
28	Have risks been prioritised for reporting purposes?		
29	Has consideration been given to the development of key risk indicators?		
	<i>Embedding risk management (see paragraphs 145-</i>		

	<b>Good practice questions</b>	<b>Is audit committee satisfied? Yes/No/NA</b>	<b>Follow-up steps necessary</b>
	175)		
30	Have steps been taken to build a culture where everyone is a 'risk manager'?		
31	Do risk management objectives complement the institution's existing vision and goals?		
32	Is risk explicitly considered as part of existing reports and in respect of key decisions?		
33	Is risk management used to understand performance shortcomings?		
34	Is risk management built into HR practices, such as training, staff performance appraisals, and staff inductions?		
	<i>Sharing risk management knowledge (see paragraphs 176-186)</i>		
35	Is there a communications strategy for risk management?		
36	How is information about risk management shared?		

## **Annex B Organisations that have contributed to this guidance**

We would like to express our thanks to the following organisations, all of whom have contributed directly to this good practice guidance.

University College Chichester

Coventry University

Edge Hill College of Higher Education

Falmouth College of Arts

Higher Education Funding Council for England

University of Leeds

University of Northumbria at Newcastle

University of Sheffield

Standing Conference of Principals

University of Sussex

York St John College

## Annex C Index of examples

Example	Number	Page
Academic risks	15	15
Assessing risk: method 1	18	19
Assessing risk: method 2	19	19
Audit committees: assurances	22	25
Audit committees: interaction	8	9
Governing body away days	6	8
Governing body oversees operational areas	5	8
Governing body: contributing wider experience	7	8
Governing body: defining responsibilities	3	7
Governing body: helping to identify risks	4	8
Governing body: reporting	23	25
Initiatives: assessing risks of a capital project	28	29
Initiatives: making the case for new initiatives	1	4
Reporting risk: as part of existing processes	26	28
Risk appetite: a defining statement	10	10
Risk appetite: annual review	11	11
Risk appetite: score limit	9	10
Risk assurances: mapping	20	22
Risk assurances: annual questionnaire	24	26
Risk champions	13	14
Risk groups	17	15
Risk group's role	30	30
Risk indicators: traffic light reporting	25	26
Risk management: academic expertise	16	15
Risk management: dedicated staff	12	14
Risk management: integrating with business planning	27	28
Risk management: professional advisers	14	14
Risk register: summary of actions for improvement	21	22
Risk register: departmental	29	29
Seminars on risk management	31	32
Strategy: challenging the strategy	2	4

## Annex D Further reading

- 'Academic Risk: Quality Risk Management in Higher Education' (Interim Report), Colin Raban, Elizabeth Turner (2003)
- 'Accountability and audit: the HEFCE code of practice', HEFCE 2004/27
- 'Audit committees: good practices for meeting market expectations', PricewaterhouseCoopers (2004)
- 'Canadian government integrated risk management framework', Canadian Government (2001)
- 'Guidance on audit committees' (the Smith Guidance) (2003)
- 'Guide to risk management in further education', the Learning and Skills Council (2003)
- 'Guidelines for managing risk in the healthcare sector', HB 228 - Standards Australia/Standards New Zealand (2001)
- 'HEI audit committees, risk management and statements of internal control', HEFCE Circular Letter 12/2002
- Housing Corporation Risk Management Topic Papers 1 to 5 (2002)
- 'Internal control: guidance for directors on the Combined Code' (the Turnbull guidance), ICAEW (1999)
- 'Management of risk: a strategic overview', National Audit Office (2001)
- 'Model financial memorandum between HEFCE and institutions', HEFCE 2003/54
- 'Organisational experiences in implementing risk management practices', HB 250, Standards Australia (2000)
- 'Risk management in British universities: a review of current attitudes, organisation and practice', Corporate Risk Group (2004)
- Risk Management: A briefing for governors and senior managers - HEFCE (2001/24)
- Risk Management: A guide to good practice in higher education institutions - HEFCE (2001/28)
- Risk Management Technical Notes - Strategic Partnership Taskforce/Office of the Deputy Prime Minister (2004)
- Risk: Improving government capability to handle to handle risk and uncertainty - HM Treasury (2002)
- Supporting innovation: Managing risk in government departments - National Audit Office (2000)
- The Combined Code on Corporate Governance – Financial Reporting Council (2003)

## Annex E Glossary of terms

Bottom-up	An assessment (of risk) driven from the operational, ground level aspects of an entity.
Combined Code	The Combined Code is an amalgamation of codes of best practice drafted by several committees, the first of which, being that chaired by Sir Adrian Cadbury, who reported his findings in 1992. The FRC (Financial Reporting Council) released an updated version of the Code in 2003. The purpose of the Combined Code is to provide assurance that companies are managed in a diligent manner.
Embedding	Embedding is a term used to describe the integration of risk management processes into the culture and day-to-day activities of an entity.
Financial Memorandum	The financial memorandum, between HEFCE and the institutions funded by HEFCE, sets out the terms and conditions for payment of HEFCE grants.
Gross risk	Gross risk represents an assessment of a risk <b>before</b> anything is done to mitigate or manage that risk i.e. before controls are put in place.
HEFCE	Higher Education Funding Council for England
HR	Human resources
Mitigating controls	Controls put in place to manage and/or reduce the level of risk.
Net risk	Net risk is the risk faced after putting in place controls or mitigating actions. Some call this the 'residual risk' or 'residual exposure'.
Residual risk	See net risk above.
Risk appetite	Risk appetite is a definition of the overall level of risk exposure that an entity is prepared to expose itself to.
Risk assurance mapping	A process for identifying how assurance is to be obtained against each risk.
Risk champion	A promoter of the risk management process.
Risk management	The processes, culture and structures whereby an entity's risks (uncertain outcomes – whether positive or negative) are managed by taking action on probability and/or impact.
Risk manager	The 'process owner' or 'designated responsibility centre' for sustaining the risk management process and acting as a source of expert support for others.
Risk register	A systematic form of documenting and recording identified risks.
Statement of Internal Control	This is a narrative statement which accompanies the annual accounts. It provides disclosures about the process for identifying, evaluating and managing the significant risks faced by the entity, that it has been in place for the year under review and up to the date of approval of the annual report and accounts, that it is regularly reviewed by the board and accords with the guidance in the Combined Code.
Top-down	An assessment (of risk) driven from the strategic, overview aspects of an entity.
Turnbull	Turnbull refers to guidance published by the Institute of Chartered Accountants in England & Wales on the implementation of the internal control requirements of the Combined Code on Corporate Governance. The guidance requires the identification, evaluation and management of significant risks and the assessment of the

effectiveness of the related internal control system. Boards of directors should review regularly reports on the effectiveness of the system of internal control in managing key risks, and undertake an annual assessment for the purpose of making their statements on internal control in the annual report.

Upside risk

Those risks identified as part of a bottom-up risk assessment.