

## 5. DOCUMENTING AND REPORTING RISK MANAGEMENT

- 5.1 If it is to do its job, a governing body is almost totally reliant on the information on risk it is provided with. Too little information and it won't know what is going on, too much (or poorly presented) and it will suffer from overload, and members will stop reading governing body papers.
- 5.2 As a governor, you have two major concerns in this area: directly reviewing the key board level risks (basically the things that should keep you awake at night whether as opportunity or threat), and ensuring that there are effective and tested systems in place in respect of the lower level risks. Some organisations have escalation policies, linking the escalation of risks to their priority - all the high priority ones are reported to the board, while other risks are reported at lower levels.
- 5.3 In any organisation the risk process is predicated on both a top down and bottom up approach. Strategic risk issues will generally be considered at the higher level, whilst a range of operational risks will be dealt with at a variety of levels across the HEI. So it follows that reporting on risk may be aimed at several different groups. Each will require different types of information, so, with all this risk management information available within the institution, what kind of reports will you be involved with or receive as a governor? Perhaps the simplest distinction is between external and internal risk reporting.
- 5.4 So far as external risk reporting is concerned, the main route will be to the funding bodies (authorised and approved by the governing body), through the annual accounts and the statement of internal control, where an HEI can clearly state its attitude to risk. Part of the Sorp on accounting for further and higher education advises that the financial statement "should provide information to assist funders and financial supporters to assess the strategies adopted by the institution and the potential for those strategies to succeed" including "the resources, principal risks and uncertainties and relationships that may affect the institution's long-term financial position"<sup>23</sup>. This issue is considered in more detail in the companion volume on finance in this series.
- 5.5 It is up to each HEI to decide how it communicates risk issues to external sources, whether concerning regulatory requirements or otherwise. External reporting of risk information has been noted as not being "as sophisticated as it could be, and is often given low priority by institutions"<sup>24</sup>. However, some examples of good communication have been found, including the sharing of data on risk management through an HEI's website.

<sup>23</sup> Statement of Recommended Practice: Accounting for Further and Higher Education (2007), Universities UK at [www.universitiesuk.ac.uk](http://www.universitiesuk.ac.uk)

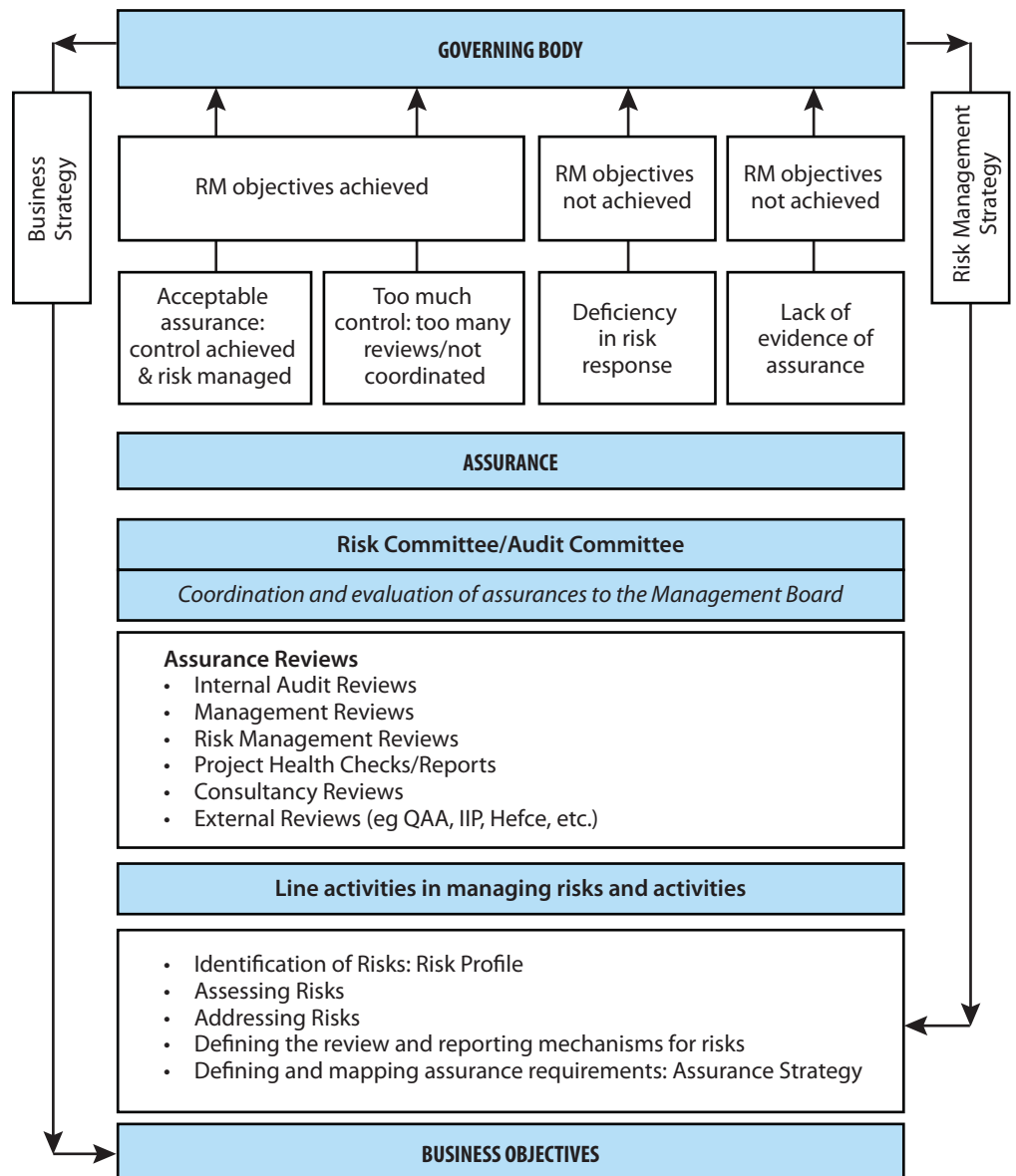
<sup>24</sup> Hefce, (2005) PricewaterhouseCoopers, Risk Management in Higher Education at [http://www.hefce.ac.uk/pubs/hefce/2005/05\\_11/](http://www.hefce.ac.uk/pubs/hefce/2005/05_11/) page 24

5.6 Beyond issues of compliance and accountability, it is internal reporting to the governing body that is the main concern of this volume. There are a number of key documents on risk management and control that your governing body should receive. The main ones are (and each is considered briefly in the following paragraphs): the risk policy; the risk register; regular reports on progress on key strategic, financial and reputational risks; reports as required on key operational risks (at least annually); reports on major project risks as required; audit, assurance and audit plans; and business continuity plans and documentation.

### SUGGESTED TASK

What does implementing this diagram mean for providing information to your governing body?

5.7 The Treasury (in its Orange Book) provides the following flowchart which sets out the typical layers of risk reporting to a governing body<sup>25</sup>.



<sup>25</sup> Amended from HM Treasury, (2004), The Orange Book: Management of Risks - Principles and Concept

## The risk policy

5.8 This was described in Chapter 4, and although it may vary between HEIs, it should provide sufficient data to guide both internal and external stakeholders as to how the risk management process is being overseen and managed. Importantly, it should be signed off by the board, and underpin the work of the audit committee and (where it exists) the risk committee.

## The risk register

- 5.9 Let's be clear about one thing immediately: a risk register is a recording and monitoring tool for management, and not a reporting tool for the governing body. A board should not be asked to wade through a full risk register - in truth most members wouldn't if asked. To be useful for most boards it needs to be tailored for presentational purposes.
- 5.10 Having said that, it is probably the main document used in the risk management process, so much so that all too often it is seen as *the* process, with completion of this paper/IT record as the end product of risk management! However, it is true that the risk register is the proof - the formal evidence - that you are in some way implementing a risk management system. Of course, your HEI will be asked to provide evidence of a risk register as part of its governance responsibilities, and as a governor you should have sight of it, and an understanding of the key risks on it.
- 5.11 However, for a governing body the challenge is to gauge the right level of scrutiny, so in practice, many HEIs will have a series of scaled risk registers, with the board only concentrating on the major threats and opportunities. The Hefce guide on good practice in risk management suggests "... initially focus on the 20 most significant risks that could damage the institution. Then expand into other areas, starting with those that seem to produce the greatest exposure"<sup>26</sup>. The audit committee or risk committee (if you have one) will look in more detail, but even then many operational risks should be a delegated management responsibility.
- 5.12 So, what should your principal risk register consist of? As a minimum, it should have the following information: identified risk; cause/effect; probability; likely impacts; risk owner; timing (impact window/action window); risk status; agreed actions (immediate/ contingency/fallback); action review dates; and action owner. In essence the risk register is a 'to do' list. An example risk register is provided in Annex A.
- 5.13 How often should the risk register be reviewed? A key issue here is the link to your HEI's strategic planning cycle, and it makes sense to have the review of key risks integrated into the same business planning processes. Your HEI should undertake a full strategic review on a regular basis (perhaps every three to five years) with an annual review of the business plan, and with ongoing risks considered at that time. This can then assess new risks, changing risks, dead or irrelevant risks and re-emerging risks.

### SUGGESTED TASK

Reflect on your HEI's risk register. Have you seen it, and what can you glean about risk in your HEI from it? Does it adequately capture key threats and opportunities as you see them?

<sup>26</sup> Risk Management: a Guide to Good Practice for Higher Education Institutions, Hefce 01/28 at [www.hefce.ac.uk/pubs/hefce/2001/01\\_28.htm](http://www.hefce.ac.uk/pubs/hefce/2001/01_28.htm)

## Regular risk reports

- 5.14 How regularly risk is reported to governing bodies varies. Some HEIs have a standing item at meetings consisting of a short progress update against key risks, and this might generally be considered to be good practice. Others ask for detailed reports on one of the major board level risks at every audit committee meeting, and many have risk management as a standing item on the audit committee agenda. Another has quarterly reports to the governing body as part of the review on strategic and operational performance. In a well run board, the need to discuss the issues causing concern will be identified beforehand in discussions between the chair and the clerk, and additional information on these items might be expected.
- 5.15 Increasingly, governing body or audit committee monitoring of risk is combined with simple presentational devices such as traffic lights, so that everyone can see the progress being made on specific items. If all is well then no discussion may be required; if all is not well then it is easy to identify the issues to pursue. In addition, a board should at a minimum receive - and approve - an annual risk report (usually prepared by the audit committee) which notes progress on all key identified risks. This is essential for internal purposes, and will form part of its compliance reporting to the funding body.

## Key operational and project reports

- 5.16 Much of this work will be delegated to the audit committee (and the risk committee where it exists) and to individual managers. Nonetheless the board needs to keep a 'watching brief', usually by receiving committee minutes. Major projects should have a risk plan and agreed monitoring system. Indeed, this is a requirement of projects undertaken under some professional standards (eg the Royal Institute of British Architects or the British Computer Society), as well as more generic project management systems such as Prince 2. Where a project is itself a key strategic objective (and therefore a key risk), specific monitoring reports might be expected.

## Reporting from committees

- 5.17 In Chapter 3 the audit committee's role was considered in relation to risk. Here the concern is on assessing and testing the assurances that are in place for a range of risks, right across the HEI. By comparison the governing body is really focused mainly on primary risks. It follows then that an audit committee has an important role in providing regular information, critical commentary, and assessment back to the full board on the wider range of risk issues. The same is true for the risk committee, where it exists.
- 5.18 It is standard practice for the minutes and reports of such committees to be received at each board meeting as part of an integrated committee reporting cycle. Perhaps the most important issue here is to ensure that committee minutes and reports meet fully the requirements of the main body, so that the process for monitoring risk is 'joined up'. This is not always the case; for example it is not unknown for a strong chair of an audit committee to have a particular view about audit and risk reporting which may not match the requirements of the main board. Of course, the audit committee needs to be independent, but that should not mean the main board does not receive the information it wants in the way it wants it. Clearly the professional role of the clerk or secretary of the governing body (who will often serve the audit committee in the same capacity) is crucial here, and a good committee secretary will ensure such a joined up approach.

### Final commentary

- 5.19 Let's go back to the start. You may recall that in Chapter 1 it was acknowledged that risk management has sometimes had a bad press, and has been seen by some people as a paper exercise to keep regulators happy. Certainly what you may find difficult as a governor is that there is no absolute 'end game' or final position in respect of risk management. It is fluid in both concept and application - a constant balancing act to achieve an appropriate level of analysis, whilst not being too inhibiting.
- 5.20 As a governor you can help provide the lead by ensuring that risk management is on the agenda, and is regularly seen in papers, reports and discussions. You can encourage frank analysis, recognising that risk is always with us and that we need to accept a level of residual risk in everything we do. You can help establish the no blame but continuous improvement agenda which is the challenge of effective risk management.

### Self-challenge questions

- As a governor, what type of information do you want to see on risk management? Do you get the information you want?
- How can you be sure that the audit committee or risk committee (if one exists) is getting the information it needs to do its job?
- What kind of risk management information is included in your annual accounts?

#### A GOVERNOR'S DILEMMA 5:

As a governor you find yourself increasingly swamped with information on risk registers and other reports discussing risk, but somehow they seem to miss the point: it's hard to see the wood for the trees! How do you seek to deal with this, and what might be done to manage and improve the reporting process?