Risk Management and the Audit Committee

All the UK higher education funding bodies require audit committees to assess risk management, control and governance arrangements. The audit committee must form an opinion on these arrangements, and to do this it needs to establish how key risks are identified, evaluated and managed, and the rigour and comprehensiveness of the review process. However, this does not mean that the governing body should not be actively involved in risk: this is a matter for the whole board as well as the audit committee.

The role of the audit committee is considered separately, but it has been found that audit committees generally exercise their risk role in different ways, such as:

- The audit committee may review the full risk register at every meeting
- The committee may explore individual departmental risks on a rolling cycle
- The committee may consider risk management in detail when internal auditors have reviewed the area concerned

An issue to consider here is the balance of responsibility between the audit committee, the full board, and the executive, and whether any other body should be involved. A few institutions have introduced separate risk committees, perhaps combined with governance, to make a risk and governance portfolio. There is no requirement to do so, but those institutions that have such a committee may use it to develop and review the overall risk policy, or as an ad hoc committee to consider, for example, major project risks.

A number of issues relating to risk management processes, and the role and effectiveness of the audit committee in that area, are raised by Sir David Melville in his ‘Independent Review into the circumstances and issues associated with the clawback of significant funds’ from London Metropolitan University in 2009.

Governance and Risk Management

Some high-profile corporate failures have, among other factors, led to a much greater focus on systems of risk management, both in the private sector and higher education. This has been a catalyst for much of the ‘best practice’ guidance on risk management and good governance both in the business world and in higher education. Best practice now sees risk management and good governance not merely as a way of avoiding risk, but as an integral part of the planning process.

In the private sector there have been two particularly influential reports brought together within the Financial Reporting Council (FRC) Governance Code:

- The Turnbull Report (on internal controls), which required a company's board to establish a sound system of internal control based 'on a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed'
- The Smith Report which established a key role for the audit committee in 'monitoring and reviewing the effectiveness of the risk management, control and governance arrangements'

The Combined Code provisions are mirrored in the CUC Code of Governance (included within the CUC Guide). The CUC Code states that ‘institutions must have a sound system of risk management, control and governance’, and one of the essential elements of such a control system is seen as "the identification and management of risk embedded in all business systems."

Governing bodies can support institutions by ensuring that an effective risk management system is in place, and that it informs the strategic development processes which are the board’s responsibility. This is likely to help keep the institution heading in its chosen direction, and to be better able to manage the vagaries of getting there.
What is Risk Management

Most common definitions suggest that risk is always something bad. It is true that for any decision there is the chance of failure, and a potential penalty of some loss or other. This is risk as a threat. But there is another risk: that of failing to pursue an opportunity, and thereby failing to maximize true potential. These two perspectives have been refined into a definition of risk by CUC as being, 'the threat or possibility that an action or event will adversely or beneficially affect an organisation’s ability to achieve its objectives'.

Risk management can be done (just as in our personal lives) in an unconscious and unconsidered way, but what a formalised system of risk management seeks to achieve is more systematic management behaviour.

Elsewhere, HM Treasury notes that ‘good risk management also allows stakeholders to have increased confidence in the organisation’s corporate governance and ability to deliver’, and positive risk management thereby helps an organisation to:

- Have increased confidence in achieving its desired outcomes
- Effectively constrain threats to acceptable levels
- Take informed decisions about exploiting opportunities

Risk in Higher Education Institutions

Higher education in the UK is diverse and, in comparison with other sectors, is generally felt to be low-risk. Accepting this, however, the nature of risk in individual institutions varies considerably. Risks can be classified into 6 major areas:

- **Strategic risks**, relating to major and probably long term plans. This is an important matter for governing bodies
- **Financial risks**, which relate both to overall financial capacity and viability and to financial procedures and systems
- **Legal risks**, including those at institutional level, those which might arise from the establishment of subsidiary companies or joint ventures and those relating to staff undertaking private external work
- **Reputational risks**, which can be significant in terms of both staff and student recruitment
- **Operational risks**, which are principally matters for management, and can include people issues, estates issues and health and safety
- **Major Project risks**, where there can be financial exposure, legal risks and potential for damage to reputation

Risk Management Processes

Governing bodies are normally expected to approve and, from time to time, review a risk management policy. This may well include its scope and objectives, setting out roles and responsibilities, tools and techniques and reporting arrangements. Hefce has produced an example of a policy. Risk is related to the ability of the institution to achieve its objectives, so risk management should be integrated into strategic planning and review processes.

There are various ways in which risks can be identified; this is usually a management responsibility. When identified risks have to be assessed. It is then important to respond to the identified risks and take steps to mitigate them. Governing bodies will also require a reporting and review system.

Business Continuity

Risk management and business continuity planning are closely related. Business continuity is intended to achieve an effective and robust framework that will enable an
organisation to plan for and recover as quickly and effectively as possible from a major incident that interrupts normal business operations, such as:

- A major fire, flood or other environmental incident that involves death or significant injury to numbers of employees or students, or major damage to facilities that required emergency services
- Major demonstrations against an institution or one of its research centres
- Any incident involving a major breach of security, either physical security of plant and facilities or computer security
- Terrorist incidents directly or indirectly affecting staff, students or facilities
- Loss of computer applications, telecommunication links or utilities

**Risk Management Documentation**

In addition to the risk policy, the main risk management document is the **risk register**. This is likely to be a substantial document, primarily for reporting to management, and may well be too detailed for reporting to the governing body. The governing body and the audit committee will have to determine how risk matters should be reported and how frequently.

How regularly risk is reported to governing bodies varies. Some 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 approach is to have 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.

Increasingly, governing body or audit committee monitoring of risk is combined with simple presentational devices such as traffic lights, so that progress being made on specific items is easy to see.

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.

**Find more information and resources on this topic on our website at:**
[www.lfhe.ac.uk/en/governance/ba/committees/risk-management](http://www.lfhe.ac.uk/en/governance/ba/committees/risk-management)