8. Risk management

Introduction and aim

The governing body exercises oversight of the provider's risk management and seek assurances from the executive that key risks have been identified and are being effectively managed. This requires that risks are identified, their impact and likelihood assessed, and mitigation strategies adopted. To ensure there is a clear understanding of the extent to which risk is tolerated, the governing body should agree its risk appetite.

Topics covered

1. Risk management
2. Risk and the governing body
3. Risk appetite
4. Changes to the risk appetite
5. Disclosures relating to risk
6. The risk register
7. Risk cannot be avoided
8. Are risks increasing?
9. Some risks cannot be controlled
10. Risk and uncertainty
11. Is there an upside to risk?
12. Planning for contingencies
13. Sources of risk
14. Strategic risks
15. Financial risks
16. Reputational risks
17. Assessing risk
18. Mitigation of risk
19. More than compliance
20. What can go wrong?
21. Weak governance
22. Risk blindness
23. Poor executive leadership
24. Ineffective checks and balances
25. Conclusions
26. Questions to review.

1. Risk management

Risk management describes the process by which risks are identified and managed. It starts by identifying and understanding the risks associated with a given action, assesses the likely impact should a risk materialise and considers how the risk can be mitigaed through proactive management.

2. Risk and the governing body

The codes of higher education governance provide a clear steer as to the role of governing bodies and the management of risk. The Higher Education Code of Governance states that there should be 'effective systems of control and risk management'[1]. The Scottish Code notes that the governing body must be attentive to risks which could threaten the provider's sustainability, ensuring that it has appropriate procedures to identify and actively manage risk. Further, the code states that 'the governing body is responsible for determining the nature and extent of the principal risks it is willing to take in pursuing its strategic plan.'[2] This raises the question of the governing body's appetite for risk.

3. Risk appetite

The term 'risk appetite' describes the extent to which a governing body is prepared to tolerate risk. If the governing body's risk appetite is low, self-evidently, it has a low tolerance of risk; whereas if the risk appetite is higher, clearly their tolerance of risk will be greater. It is important that the governing has the opportunity to discuss and establish its appetite to tolerating risk. Before presenting proposals for approval, the executive team should be mindful of the governing body's risk appetite. Proposals out-with the agreed risk appetite are unlikely to be endorsed.

4. Changes to risk appetite

The 'appetite' to take risks does not necessarily remain fixed, and could, for example, change following a reassessment of the operating context and extent to which a given level of risk can be tolerated. Increased levels of uncertainty, might lead to the governing body to decide it should become more risk-adverse.

5. Disclosures relating to risk

Providers regulated by the Office for Students are expected to include in their annual financial statements a statement of 'internal control'. This should include information as to how the provider has evaluated the impact and likelihood of different risks, procedures for reviewing risks and how risk assessment and internal control is embedded in the organisation[3]. Similarly, providers in Scotland are expected to maintain a risk register, and provide 'an annual disclosure about risk management in audited financial statements.'[4]

6. The risk register

Following an assessment of the different risks facing the provider, typically a risk register will be developed. As its name suggests, this will provide a register of all risks, and include an assessment of their impact and their likelihood of occurrence. The register also typically includes information on the actions being taken by the executive to mitigate a risk. The risk register will normally be regularly reviewed by the governing body, often following prior review by the audit committee. As well as reviewing the full register, the audit committee may decide to regularly undertake a 'deep dive' (i.e. a detailed examination) of a specific risk to assure itself that the provider has fully assessed the risk and taken appropriate actions to mitigate its occurrence.

7. Risk cannot be avoided

The rationale for undertaking risk management is that the provision of higher education services by providers involves uncertainty and risk. Because the future operating environment cannot be known with certainty, the outcomes from the provider's strategies and actions involves risk.

8. Are risks increasing?

As a general observation, the operating environment for higher education providers has tended to become less stable and predictable. Some would suggest that as a consequence the level of risk faced by higher education providers has increased. As a consequence, the management of risk has received increased attention.

9. Some risks cannot be controlled

Many of the factors leading to increasing risk may be outside of the provider's control. For example, the higher education policy environment is not under a provider's control, although they may, individually and collectively, seek to influence policy-makers who determine policies. As a result, the provider may be unable to control a risk to which it is exposed. In such an event, the task is to assess the risk and consider what actions the provider can take which will mitigate the impact of the risk should it occur.

10. Risk and uncertainty

Although often used interchangeably, it is possible to distinguish between risk and uncertainty. Risk refers to events against which it is possible to attach a probability of the likely resulting loss or gain. In other words, it is possible to quantify the risk. In contrast, uncertainty relates to events for which there is insufficient data to attach objective probabilities[5]. Uncertainty has been associated with highly improbable and unpredictable events. Such events can be described as 'tail' risk (ie. at the far end of the probability distribution), and very rare[6].

11. Is there an upside to risk?

It is worth noting that although risks are generally framed in terms of negative outcomes, unforeseen events or unanticipated degrees of change can result in positive opportunities. For example, the freehold of a building in a strategically important location for the provider suddenly and unexpectedly becomes available to purchase. Should such an event occur, the key question is whether the provider is in a position to take advantage of the unforeseen opportunity?

12. Planning for contingencies

While some events can be foreseen, others are very difficult or impossible to predict. For example, there may be genuine uncertainty about future government policy towards higher education, suggesting that beyond the immediate period a key aspect of the operating environment cannot be reliably foreseen. As a result, providers may need to adopt a contingency approach and prepare for a number of different scenarios. In assessing the resilience to manage the different risks, the key question is how easy would it be for the provider to cope with the different scenarios.

13. Sources of risk

There are number sources of risk, and governing bodies must seek assurances that each are being effectively managed. Governing bodies should also be mindful that individual risks may be mutually exclusive and the realisation of one risk may lead to others. Risk may be organised under the head of strategic risks, financial risks and reputational risks.

14.Strategic risks

Strategic risks include major decisions relating to the future direction and development of the provider and its sustainability. By way of illustration, major decisions carrying strategic risks might include initiatives such as the development of a new campus, entering into a collaborative partnership with an overseas provider, significant changes to the provider's course portfolio and plans to expand or contract total student numbers.

15.Financial risks

Financial risks may result from poor budgeting and the failure of expenditure controls (operational risks), but may equally result from cost over-runs on major projects, which involve significant amounts of capital expenditure. Large-scale and complex projects, with tight timelines, can lead to difficulties in the absence of careful and effective procurement and project management. Equally, high-levels of borrowing to fund new developments may expose the provider to an increasing risk with regard to its ability to service the borrowing.

16.Reputational risks

Reputational risks arise from adverse publicity arising from any number of issues, including a failure of academic standards and quality, being associated with accepting a financial donation from a donor that compromises the provider's position, or matters relating to student well-being[7]. In each case, without an effective response, immediate, and sometimes longer-term, damage to the provider's reputation may result.

17.Assessing risk

The meaningful assessment of risk is not always easy. Approaches commonly categorise the level of individual risks, with most attention being given to those risks deemed to have the highest potential impact and deemed most likely to occur. Typically, starting with the risk register the process involves identifying and assessing risks based on their potential impact as 'high', 'medium', or 'low'. A high risk being one has the potential to have a widespread and significant impact on the institution. Alongside impact, the likelihood of the risk occurring will also be assessed; again, using the classification of 'high', 'medium', or 'low'. Those risks most likely to occur are rated as having a 'high likelihood'.

18.Mitigation of risks

'High/high' risks, those with a high impact and high likelihood of occurrence, are generally the subject of the greatest attention by the provider's management and highlighted to the governing body. The governing body can be expected to discuss such risks and seek assurances as to what action is being taken by management to mitigate (reduce) the risk. Although, 'high/high' risks are likely to receive the greatest attention, providers should regularly look across the risk profile, mindful, for example, that a high impact, low-likelihood risk, should it occur, would have a significant effect on the provider.

19.More than compliance

Risk management is rarely viewed as the most engaging, or interesting of topics by employees. As a consequence, there is a danger that although an assessment of risk is undertaken it can become one which focus primarily on compliance and essentially becomes a 'box-ticking' exercise. While this may 'technically' comply with the formal requirements placed on the provider, it is unlikely to result in effective management of risks. This requires an acceptance by staff throughout the provider of the importance of risk, and a culture which ensures the proactive management of risk. Governing bodies should seek assurances from management that an appropriate culture towards risk management is present throughout the organisation.

20.What can go wrong?

There are a number of areas – not necessarily mutually exclusive – where problems with risk management can arise. Governing bodies should be mindful that weak governance, risk blindness, poor executive leadership and ineffective checks and balances can each undermine the provider's system of risk management.

21.Weak governance

Weak governance may lead to a failure to 'manage' the head of the provider and, as a consequence, result in the management actions which involve significant level of unplanned risk. Weak governance may reflect a lack of competence amongst the membership of the governing body, or an unwillingness by governors to question effectively and challenge proposals brought forward by the executive.

22. Risk blindness

Risk blindness can occur when an individual or group is 'blind' to the risks associated with a particular course of action, or if they do see the risk, they underplay the concern. Risk blindness may be connected with 'group think'. This arises when the membership of a group is largely homogeneous and individuals use the 'same lens' to assess a proposal. A lack of diversity means the problem is not examined from multiple perspectives. As a result, the consensus which emerges, embodies the failure to examine the issue or problem from different perspectives. Consequently, risks are unforeseen or ignored.

23. Poor executive leadership

Effective executive leadership is a necessary pre-condition to ensure that a provider manages risk effectively. If the executive team does not have the skills or desire to inculcate a culture that treats risk management as a matter of high importance, then policies and processes are likely to be poorly implemented, and lack effectiveness.

24. Ineffective checks and balances

To provide confidence in the provider's approach to the risk management, policies and process should be subject to periodic checks. The internal audit service is important mechanism by which this takes place. The internal audit service, either supplied by an in-house function or professional auditor, should be regularly asked to examine key areas of risk and the processes by which they are managed. The effectiveness of the assurances they supply depends on the internal auditors being directed to examine key areas of risk, undertaking in-depth testing and auditing of specific risk management processes and issuing the governing body (generally via its audit committee) with a detailed assessment of the risk, and whether actions are required to improve the management of the risk. Should the internal auditor be poorly directed or its their audits lack depth, risks may go undetected. Audit committees (generally on behalf of the governing body) should make sure that the work of the internal auditors is directed at key areas of risk and their audits provide a thorough examination and testing of the risk management processes.

25. Conclusions

Governing bodies should assure themselves that the provider has proactive and effective processes for identifying and managing risk. There is a clear process for selecting the most 'critical' risks, and giving them appropriate attention. Governing bodies should expect to receive a detailed and objective evaluation of the risks identified, including their impact and likelihood. Actions to mitigate the risks should be clearly identified, with evidence that the actions have been, or are being, implemented. Governing bodies should also seek assurances from management that a culture of risk management permeates staff (and students) at all levels of the provider.

26. Questions to review

Q Have the most important risks been clearly identified and evaluated?

Q What has the executive team done to mitigate key risks?

Q Are the mitigating actions regularly reviewed and updated to ensure they remain effective?

Q Is the internal auditor effectively used to audit key areas of risk?

Q Is a culture of risk management embedded within the organisation?

Q Overall does the provider have effective systems of internal control and risk management?

End notes and further reading

[1] Element 3 of the seven primary elements of higher education governance. Committee of University Chairs, Revised June 2018, p.15.

[2] The Scottish Code of Good Higher Education Governance, Revised July 2017, p.8.

[3] See Regulatory Advice No.9: Accounts Direction. Guidance on preparing and publishing financial statements, OfS 2018.26, p.8.

[4] The Scottish Code of Good Higher Education Governance, Revised July 2017, p.8.

[5] For a brief discussion of the historical debate and the distinction between risk and uncertainty see John Kay (2018), Embracing radical uncertainty, April 16.

[6] Black Swan events are large-scale, large-impact, rare events that cannot be predictable using current assessment and forecasting methods. The term 'black swan' gained popularity following publication of The Black Swan: The Impact of the Highly Improbable (Penguin, 2008) by Nassim Nicholas Taleb.

[7] During the latter part of 2018, concerns were raised about the association of some UK higher education providers with individual Gulf States, and risks to the provider's reputation. For discussion of some of the issues, see Andrew English and Simeon Kerr, Universities challenged: scrutiny over Gulf money, Financial Times, December 13, 2018. Accessed December 14. 2018.