COSO ENTERPRISE RISK MANAGEMENT FRAMEWORK

This article examines the guidance published by the Committee of Sponsoring Organisations (COSO)

COSO

The Committee of Sponsoring Organisations (COSO) was established in the mid-1980s, initially to sponsor research into the causes of fraudulent financial reporting. Its current mission is to: 'provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organisational performance and governance and to reduce the extent of fraud in organisations.'

Although COSO's guidance is non-mandatory, it has been influential because it provides frameworks against which risk management and internal control systems can be assessed and improved. Corporate scandals, arising in companies where risk management and internal control were deficient, and attempts to regulate corporate behaviour as a result of these scandals have resulted in an environment where guidance on best practice in risk management and internal control has been particularly welcome.

THE ERM MODEL

COSO's enterprise risk management (ERM) model has become a widely-accepted framework for organisations to use. Although it has attracted criticisms, the framework

has been established as a model that can be used in different environments worldwide.

COSO's guidance illustrated the ERM model in the form of a cube. COSO intended the cube to illustrate the links between objectives that are shown on the top and the eight components shown on the front, which represent what is needed to achieve the objectives. The third dimension represents the organisation's units, which portrays the model's ability to focus on parts of the organisation as well as the whole.

This article highlights a number of issues under each of the eight components listed on the front of the cube that organisations have had to tackle – issues which have featured in exam questions for Paper P1.

INTERNAL ENVIRONMENT

The internal environment establishes the tone of the organisation, influencing risk appetite, attitudes towards risk management and ethical values.

Ultimately, the company's tone is set by the board. An unbalanced board, lacking appropriate technical knowledge and experience, diversity and strong, independent voices is unlikely to set the right tone. The work directors do in board committees can also make a significant contribution to tone, with the operation of the audit and risk committees being particularly important.

However, the virtuous example set by board members may be undermined by a failure of management in divisions or business units. Mechanisms to control line management may not be sufficient or may not be operated correctly. Line managers may not be aware of their responsibilities or may fail to exercise them properly. For example, they may tolerate staff ignoring controls or emphasise achievement of results over responsible handling of risks.

One criticism of the ERM model has been that it starts at the wrong place. It begins with the internal and not the external environment. Critics claim that it does not reflect sufficiently the impact of the competitive environment, regulation and external stakeholders on risk appetite and management and culture.

OBJECTIVE SETTING

The board should set objectives that support the organisation's mission and which are consistent with its risk appetite.

If the board is to set objectives effectively, it needs to be aware of the risks arising if different objectives are pursued. Entrepreneurial risks are risks that arise from carrying out business activities, such as the risks arising from a major business investment or competitor activities.

The board also needs to consider risk appetite and take a high-level view of how much risk it is willing to accept. Risk tolerance – the acceptable variation around individual objectives – should be aligned with risk appetite.

One thing the board should consider is how certain aspects of the control systems can be used for strategic purposes. For example, a code of ethics can be used as an important part of the organisation's positioning as socially responsible. However, the business framework chosen can be used to obscure illegal or unethical objectives. For example, the problems at Enron were obscured by a complex structure and a business model that was difficult to understand.

EVENT IDENTIFICATION

The organisation must identify internal and external events that affect the achievement of its objectives.

The COSO guidance draws a distinction between events having a negative impact that represent risks and events having a positive impact that are opportunities, which should feed back to strategy setting.

Some organisations may lack a process for event identification in important areas. There may be a culture of no-one expecting anything to go wrong.

The distinction between strategic and operational risks is also important here. Organisations must pay attention both to occurrences that could disrupt operations and also dangers to the achievement of strategic objectives. An excessive focus on internal factors, for which the model has been criticised, could result in a concentration on operational risks and a failure to analyse strategic dangers sufficiently.

Businesses must also have processes in place to identify the risks arising from one-off events and more gradual trends that could result in changes in risk. Often one-off events with significant risk consequences can be fairly easy to identify – for example, a major business acquisition. The ERM has been criticised for discussing risks primarily in terms of events, particularly sudden events with major consequences. Critics claim that the guidance insufficiently emphasises slow changes that can give rise to important risks – for example, changes in internal culture or market sentiment.

Organisations should carry out analysis to identify potential events, but it will also be important to identify and respond to signs of danger as soon as they arise. For example, quick responses to product failure may be vital in ensuring that lost sales and threats to reputation are minimised.

RISK ASSESSMENT

The likelihood and impact of risks are assessed, as a basis for determining how to manage them.

As well as mapping the likelihood and impact of individual risks, managers also need to consider how individual risks interrelate. The COSO guidance stresses the importance of employing a combination of qualitative and quantitative risk assessment methodologies. As well as assessing inherent risk levels, the organisation should also assess residual risks left after risk management actions have been taken.

The ERM model has, though, been criticised for encouraging an over-simplified approach to risk assessment. It's claimed that it encourages an approach that views the materialisation of risk as a single outcome. This outcome could be an expected outcome or it could be a worst-case result. Many risks will have a range of possible outcomes if they materialise – for example, extreme weather – and risk assessment needs to consider this range.

RISK RESPONSE

Management selects appropriate actions to align risks with risk tolerance and risk appetite.

This stage can be seen in terms of the four main responses – reduce, accept, transfer or avoid. However risks may end up being treated in isolation without considering the picture for the organisation as a whole. Portfolio management and diversification will be best implemented at the organisational level and the COSO guidance stresses the importance of taking a portfolio view of risk.

The risk responses chosen must be realistic, taking into account the costs of responding as well as the impact on risk. An organisation's environment will affect its risk responses. Highly regulated organisations, for example, will have more complex risk responses and controls than less regulated organisations. The ALARP principle – as low as reasonably practicable – has become important here, particularly in sectors where health or safety risks are potentially serious, but are unavoidable.

Part of the risk response stage will be designing a sound system of internal controls. COSO guidance suggests that a mix of controls will be appropriate, including prevention and detection and manual and automated controls.

CONTROL ACTIVITIES

Policies and procedures should operate to ensure that risk responses are effective.

Once designed, the controls in place need to operate properly. COSO has supplemented the ERM model by guidance in 'Internal Control – Integrated Framework'. The latest draft of this framework was published in December 2011. It stresses that control activities are a means to an end and are effected by people. The guidance states: 'It is not merely about policy manuals, systems and forms but people at every level of an organisation that impact on internal control.'

Because the human element is so important, it follows that many of the reasons why controls fail is because of problems with how managers and staff utilise controls. These include failing to operate controls because they are not taken seriously, mistakes, collusion between staff or management telling staff to over-ride controls. The COSO guidance therefore stresses the importance of segregation of duties, to reduce the possibility of a single person being able to act fraudulently and to increase the possibility of errors being found.

The guidance also stresses the need for controls to be performed across all levels of the organisation, at different stages within business processes and over the technology environment.

INFORMATION AND COMMUNICATION

Information systems should ensure that data is identified, captured and communicated in a format and timeframe that enables managers and staff to carry out their responsibilities.

The information provided to management needs to be relevant and of appropriate quality. It also must cover all the objectives shown on the top of the cube.

There needs to be communication with staff. Communication of risk areas that are relevant to what staff do is an important means of strengthening the internal environment by embedding risk awareness in staff's thinking.

As with other controls, a failure to take provision of information and communication seriously can have adverse consequences. For example, management may not insist on a business unit providing the required information if that business unit appears to be performing well. Also, if there is a system of reporting by exception, what is important enough to be reported will be left to the judgment of operational managers who may be disinclined to report problems. Senior management may not learn about potential problems in time.

MONITORING

The management system should be monitored and modified if necessary.

Guidance on monitoring has developed significantly since the initial COSO guidance. At board level, the Turnbull guidance on the scope of regular and annual review of risk management has been very important.

COSO supplemented its ERM guidance with specific guidance on monitoring internal controls in 2009, based on the principle that unmonitored controls tend to deteriorate over time. The guidance echoes the Turnbull guidance in drawing a distinction between regular review (ongoing monitoring) and periodic review (separate evaluation). However weaknesses are identified, the guidance stresses the importance of feedback and action. Weaknesses should be reported, assessed and their root causes corrected.

Key players in the separate evaluation are the audit committee and internal audit department. Whether separate monitoring can be carried out effectively without an internal audit department should be a key question considered when deciding whether to establish an internal audit function. Once an organisation goes beyond a certain level of size and complexity, it becomes difficult to believe that an internal audit function will not be required.

The ERM model has provided a foundation for organisations to manage risks more effectively. However, managers need an awareness of the limitations of risk management and where the process could fail. Paper P1 questions have concentrated on organisations that have had serious shortcomings, as there is usually not enough to discuss about an organisation that is perfect!

Nick Weller is technical author for Paper P1 at BPP Learning Media