In the previous chapter we looked at how risks are identified, described and estimated using a likelihood and consequences matrix. This is an essential first step in evaluating the significance of risks and making decisions about how those risks can be avoided, mitigated, transferred or accepted, and the regular reporting to management and the Board about those risks.

### Risk evaluation

Risk evaluation is used to make decisions about the significance of risks to the organization. When risk analysis (identification, description and estimation) has been completed, the risks faced by the organization need to be compared against its risk appetite and the array of opportunities and exposures faced by the organization. Risk evaluation is then concerned with making decisions about the significance of risks to the organization and whether those risks should be accepted or whether there should be an appropriate treatment or mitigation.

### Risk treatment

Risk treatment is the process of selecting and implementing measures to modify the risk. This may include risk control/mitigation, risk avoidance, risk transfer, risk financing (e.g. hedging, insurance), etc. Risk treatment, also called risk response, involves decisions as to whether particular risks should be avoided, reduced, transferred or accepted.

Risk response may be:

- **Avoidance**: action is taken to exit the activities giving rise to risk, such as a product line or a geographical market, or a whole business unit. These are high-risk events.
Reduction: action is taken to mitigate (i.e. reduce) the risk likelihood or impact, or both, generally via internal controls. These risks occur more frequently but have less impact.

Sharing: Action is taken to transfer a portion of the risk through, for example, insurance, pooling risks, hedging or outsourcing. These are significant risks, although they occur rarely.

Acceptance: no action is taken to affect likelihood or impact. These have low impact even when they do occur, which may be frequent.

Each response needs to be considered in terms of its effect on reducing the likelihood and/or impact of the risk. Risk response also needs to consider the costs and benefits of alternative risk responses.

The risk map or likelihood/consequences matrix (see Chapter 7) enables an organization to prioritize risks (from high through medium to low) and to determine an appropriate risk response (or risk treatment) depending on the likelihood and impact of the risk. Figure 8.1 shows the COSO ERM approach to risk response on the basis of the risk map.

Risk response involves:

- Setting a policy defining the organization’s attitude to a particular risk within its risk appetite and the objectives of the risk response;
- Assigning individual accountability for the management of the risk, with the nominated person having the expertise and authority to effectively manage the risk;
■ The management processes currently used to manage the risk;
■ Recommended business processes to reduce the residual risk (after the application of controls, see below) to an acceptable level;
■ Key performance measures to enable management to assess and monitor risk;
■ Independent expertise to assess the adequacy of the risk response;
■ Contingency plans to manage or mitigate a major loss following the occurrence of an event.

Methods of risk treatment

There are many methods of treating risk, and some are described in more detail in subsequent chapters. Following are some general approaches to risk treatment. Internal controls are used for risk reduction, to mitigate risks, while portfolio, hedging and insurance are methods of sharing risks, that is risks are transferred to third parties.

Internal control

Internal control is the whole system of financial and other controls established to provide reasonable assurance of effective and efficient operation; internal financial control; and compliance with regulation. Internal controls include accounting controls (e.g. budgets) but include quantitative controls (non-financial controls such as measures of quality) as well as qualitative (e.g. personnel) controls. Control encompasses all of the processes used by managers to ensure that organizational goals are achieved and procedures adhered to, and that the organization responds appropriately to changes in its environment. Controls are put in place in response to identified risks in order to reduce the likelihood or impact of risk. Internal control is dealt with in detail in Chapter 9 and in the various risk applications in Part C.

Portfolio

The assumption that capital markets are efficient leads to the view by investors that unsystematic risk (i.e. that which does not pertain to the whole market but is company-specific) can be managed by diversification through a portfolio approach to investments, or by the use of derivatives (see below and Chapter 12) to transfer systematic risk to third parties.

In establishing a portfolio approach to risk management, management and the Board recognize the diversity of possible risks and responses and the effect on the
organization’s risk tolerance. The basic principle of portfolio theory is that it is less risky to have diverse sources of income through a portfolio of assets or investments. The portfolio approach to risk management enables risk to be spread over a wider range of investments, thereby reducing the impact of an adverse event in any one business area on the whole business. Spreading investments can be achieved through a combination of market expansion or diversification.

However, this approach ignores the impact of organizational failure on the company itself and its stakeholders. A crisis in one organization may result in a crisis in other organizations and to loss of employment, or unavailability of products or services to consumers. It may also lead to a decline in social welfare and trust in markets. Enterprise risk management is concerned with the identification, evaluation, treatment and management of risk at the individual enterprise level, so it is less concerned with investment decisions in capital markets. However the portfolio approach is relevant in spreading risk across different business units, geographic or product markets.

### Hedging

A hedge is a transaction to reduce or eliminate an exposure to risk. Hedging protects assets against unfavourable movements in an ‘underlying’ while retaining the ability to benefit from favourable movements. The most common ‘underlyings’ for which hedging takes place are in relation to changes in interest rates and foreign exchange fluctuations (but also exist for commodities, stocks and bonds). The instruments bought as a hedge tend to have opposite-value movements to the underlying and are used to transfer economic and financial risks within financial markets. This form of risk treatment is described in detail in Chapter 12.

### Insurance

Insurance involves protection against hazards by taking out an insurance policy against an uncertain event. Insurance involves payment of a premium to an insurer, who will pay the sum assured to compensate the loss suffered by the insured. An insurer is able to offer such cover on the basis of probabilities assigned to particular events and the pooling of risks by many insured parties. The premium cost will be influenced by the extent of risk management carried out by the insured in order to prevent or mitigate risks from eventuating such as fire prevention precautions. This form of risk treatment is described in detail in Chapter 21.

Although insurance is still widely used, large organizations have reduced their reliance on it as managers have recognized that insurance often does not meet
organizational needs cost-effectively. Risk reduction and risk sharing, and in some cases risk acceptance may be more appropriate responses.

**The risk register**

Once risks are identified, described, estimated using one or other quantitative or qualitative technique, and mapped according to their likelihood and consequence, most organizations record their risks in a risk register. This may contain as much information as may be considered useful for monitoring purposes. Examples of data to be included in a risk register are:

- Risk number (a unique identifier)
- Risk category (see Chapter 5)
- Description of risk
- Date risk identified
- Name of person who identified risk
- Likelihood
- Consequences
- A monetary value, if such can be allocated to the risk
- Interdependencies with other risks

The risk register will be updated with the risk treatment (or response) decided by management or the Board, including the responsible manager and the method of monitoring the risk and the effectiveness of the risk response. This will enable risk reporting (see below) and monitoring by management and the Board (see Chapter 9).

**Risk reporting**

Risk reporting is the provision of information to management and the Board that will explain the method of risk management, and how risks are identified and assessed. Although the risk register will contain all risks, only the highest risks (in terms of likelihood and consequence) will be reported at each organizational level (from business unit to corporate Board). For each identified risk, the risk response will also be recorded. Risk reports should show both the gross risk and the net risk to demonstrate the cost effectiveness of those controls.

- *Gross risk* involves the assessment of risk before the application of any avoidance, controls, transfer or other management response.
Net risk involves the assessment of risk, taking into account the application of any avoidance, controls, transfer or management response to the risk under consideration.

An example of risk assessment using gross and net risk assessments is shown in Figure 8.2 which shows how the likelihood and/or impact of risks eventuating has been reduced through risk treatment.

The residual (or net) risk is that which remains after avoidance, reduction, sharing and acceptance responses have been implemented. A comparison of gross and net risk enables a review of the effectiveness of risk treatment and the cost-effectiveness of that risk treatment. Effective risk treatment enables Boards to consider:

- The nature and extent of risks facing the organization;
- The extent and categories of risk which it regards as acceptable for the organization to bear;
- The likelihood of risks materializing;
- The costs and benefits of risk responses;
- How well the existing risk treatment techniques have reduced the overall exposure to the organization (or increased the opportunities available to it).

Reporting needs to address:

- The control systems in place for risk management.
- The processes used to identify and respond to risks.
The methods used to manage significant risks.

The monitoring and review system.

Risk reporting includes:

- A systematic review of the most significant risks.
- A review of the management responses to the significant risks.
- A monitoring and feedback loop on action taken and variance in the assessment of the significant risks.
- An ‘early warning system’ to indicate material change in the risk profile, or circumstances, which could increase exposures or threaten areas of opportunity.
- The inclusion of audit work as part of the communication and reporting process.

Risk reporting completes the feedback loop of setting objectives (risk appetite), estimating and evaluating risk, putting in place risk responses, and measuring performance (the effectiveness of risk treatment through monitoring and reporting).

**Case study: risk in a retail chain**

XYZ group (the name has been changed to preserve anonymity) had over 400 retail stores and sales in excess of £1 billion per annum. The group had been subject to significant adverse publicity several years earlier when senior managers had been charged with fraud following the reporting of inflated profits and the misleading of auditors over supplier documentation. Following a change of top management, the company had made a significant investment in risk management and internal control.

Risk management was part of the internal audit function. The internal auditor/risk manager said that the motivation for risk management was to ‘establish best practice in corporate governance’. The process commenced with a brainstorming by the internal audit team of ‘risk drivers’ to identify what could go wrong and what controls could be put in place to address risks. The internal audit team held interviews with all managers to determine a measure of the effectiveness of these controls on a scale from 1 to 5. The threat of inadequate controls was identified and recommendations were made for improvement. Although risks and controls were documented in a risk map, the internal auditor/risk manager did not see value in a formal risk register for hundreds of individual risks but rather saw risk management at a more aggregated level for the most significant risks.

A Risk Management Group (RMG) met every 2 months, comprising all senior business managers. The risk maps given by the internal audit team to the RMG showed the monetary value of what they called a ‘fundamental control breakdown’. For each risk
(e.g. supply chain failure) the ‘mitigating factors’ (i.e. controls) were identified. From
the monetary value of a control breakdown was deducted the monetary value arising
from controls implemented to give a ‘residual risk’ (i.e. the net risk after controls
were implemented) to which was assigned a probability, although it was admitted
that these values were subjective. The whole process was a ‘top down’ one, empha-
sizing a concern for ‘high level’ risks. The big risks identified through this process
were in relation to the supply chain and individual suppliers, people management, the
cost base, key business processes, retail property management, market share, prod-
uct offering and pricing, brand management, and information systems and business
continuity.

The audit committee of the Board comprised four non-executive directors, and was
attended by the external auditors, the chief financial officer and the internal auditor/risk
manager. The audit committee used the information provided by the RMG to monitor
progress in relation to the risk maps. The risk maps were the main driver of the annual
internal audit plan which was agreed by the audit committee, the RMG and individual
business managers. Results of audits were provided to the RMG and audit committee
where the value of the report was greater than £250 000.

At the time of interview, the internal auditor/risk manager wanted to implement
a risk intelligence report to provide early warning of risks, by looking at key per-
formance indicators to identify what the business should be concerned with. He also
wanted to introduce a risk marketing plan to help communicate risk and to pass on
the responsibility for risk to other managers within the business. The internal audi-
tor/risk manager expected it to take another 2 years to establish risk management in
the organization, to introduce more ‘bottom up’ involvement and to embed risk at the
cultural level.

**Case study: risk management in the Metropolitan Police Service**

Risk management models cannot always follow the ‘text book’ standard, but need
to be developed in a way that achieves ownership by managers. A case in point is
the Metropolitan Police Service (MPS) which polices London and employs 45 000
people. The MPS Business Risk Management Team (BRMT) tried to introduce a
risk register in each of its 33 commands, in a process that would record high-level
strategic business risks and escalate them to each level within the organization up to
a corporate risk register.

Procedures were written and training provided, but the BRMT faced resistance.
Risks identified tended to be very operational and expressed in terms of failing to
meet a target. They were generally shown to have a single cause and a single control.
The process was seen as bureaucratic and a waste of time by users. Consequently, the BRMT developed its own corporate risk register. They found that the complexity of outcomes the MPS is expected to deliver and its sheer size and reactive (to crime) culture blocked any meaningful adoption. This was not because of the risk management process, but because of the tools – the risk register – that were being used. There was also confusion about the distinction between ‘upside’ and ‘downside’ risk.

The BRMT developed two alternative approaches that found greater acceptance within MPS: the ‘Bow Tie’ and the ‘Butterfly’. The ‘Bow Tie’ took a risk event as the focus, and looking backwards, identified the causes of the event and the preventive controls that could be put in place. Looking forwards from the event, consequences of the event and mitigating controls were identified.

The ‘Bow Tie’ was subsequently developed into a ‘Butterfly’ model which had at its centre an opportunity or project. The (backwards) causal direction applied preventive controls for organizational weaknesses and threats and harnessing controls to take advantage of strengths and opportunities. (The forward) consequences were split into positive outcomes with enhancing controls and negative outcomes with mitigating controls.

The new approach focused more on the controls rather than scoring a risk. Control became important because it represented the degree to which the organization was tolerably or intolerably exposed to causes and consequences.

The full MPS report of their risk management implementation is available from http://www.alarm-uk.org/PDF/ALARM%20publication%20of%20MPS%20article%2011-9-07%20_2_.pdf.