Management Accounting – Risk and Control Strategy

Does your FD use the green-cross code? **The examiner for paper P3** considers how people manage risk and compares their strategies to those of organisations.

Candidates taking paper P3 should understand the central role of risk management in every organisation, whether it's a business, a public-sector body or a charity. Risk management is sometimes thought of – incorrectly – as a method for reducing or eliminating risk. This view is too restrictive, because risk is an unavoidable part of life.

If we consider an event such as crossing the road, we face the risk of being killed or seriously injured by a vehicle, but that doesn't prevent us from crossing roads. Whether we realise it or not, we all go through a quick mental process to assess the risk and take appropriate action. First, we identify that there is a risk. If we don't, we leave things completely to chance, which is dangerous. Second, we estimate the scale of the risk: we automatically take into account the road width, the surface conditions, visibility, the density and speed of traffic and so on. We might also consider our own physical capabilities and other factors such as whether we've got children with us or whether we're running late for an important appointment. We perform a mental calculation that weighs all these factors and assesses the risk. Without thinking deliberately about it, we then balance the likelihood of being hit by a car against the consequences. In fast-moving traffic, we may get killed; in slow-moving traffic, cars may stop for us.

As individuals we make a decision about when and where to cross a road. We do not avoid risk altogether; we manage it through some deliberate action. We use a pedestrian crossing, we wait until the traffic diminishes – or we simply accept the risk, hope for the best and make a dash for it.

Why will some people run across a busy road while others always wait patiently at a pedestrian crossing for the lights to change, even if there's not much traffic? It's because we all perceive risks differently as a result of our upbringing, our education and our personality. It can also be influenced by cultural factors and our own experiences. If we've had a near miss ourselves or know someone who has been injured or killed in a road accident, this is likely to influence whether we're risk-takers or risk-avoiders when it comes to crossing roads.

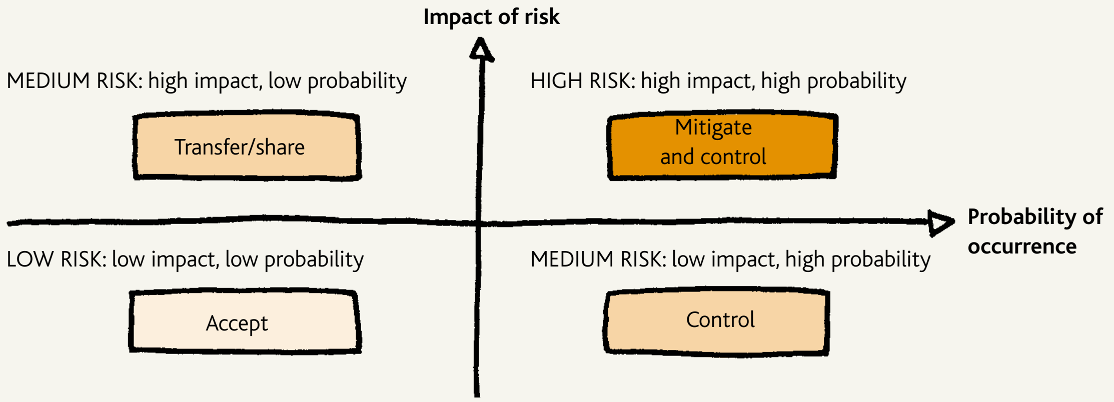
The fact that people don't approach risk in the same way makes managing risk in organisations a challenge. The process follows similar principles, but it is more complicated, of course. One complication is that organisations are collectives of people with different views of the conditions, different experiences and different attitudes to risk. For example, accountants are seen (stereotypically) as risk-averse, while sales people are seen as more risk-orientated. Another complication is that organisational objectives are far more complex than those of individuals, because organisations are trying to satisfy a range of stakeholders, whose attitudes may also vary. Organisations are expected to produce continuously improving results and set stretching objectives to satisfy their stakeholders. Risk, therefore, is not only about the possibility that something bad will occur; it's also about missed opportunities – goals that can't be achieved. In order to meet its objectives a business must take risks, such as introducing a new product, and there is usually a trade-off between risk and return. Investing in government securities is a safe option, for example, but the returns will be low. Introducing a new product, on the other hand, may pay much higher returns but there's a risk that the product may not be successful.

There are different organisational risk management models, but the following process contains seven key steps:

- **Identify the risks.** Risks are an everyday part of life, so organisations need a system to identify all those they face. This involves collecting information from a variety of sources: individuals, reports, observation and environmental assessments. Common methods of collecting data that identify risks include workshops, scenarios, brainstorming and surveys. These may be linked with consultations with stakeholders, environmental analyses, strategic plans etc.
- **Assess their impact.** Once the risks have been identified, some assessment needs to be made of their likely impact. This involves quantifying the risk in some way. We might conduct market surveys, computer simulations, cost-benefit analyses, use a Delphi technique or apply probabilities, statistical tests or sensitivity analysis. Alternatively, we may rely on subjective judgments.
- **Map the risks.** This involves prioritising the most critical risks by mapping the probability of each risk eventuating against the consequences of its eventuation. Organisations may use a simple high-medium-low scale for both likelihood and

Photograph: Alamy

MAPPING AND RESPONDING TO RISK


Impact of risk
MEDIUM RISK: high impact, low probability
Transfer/share
HIGH RISK: high impact, high probability
Mitigate and control
Probability of occurrence
LOW RISK: low impact, low probability
Accept
MEDIUM RISK: low impact, high probability
Control

Source: the Committee of Sponsoring Organisations of the Treadway Commission. (See also "Safety spec", page 25.)

consequences, or they may use a more complex scale. Whichever one they use, prioritisation is important because organisations typically face hundreds or even thousands of risks, and only the most significant ones can be managed.

- **Record risks in a register.** The risk register lists the risks that have been identified, together with the likelihood and consequences of the occurrence of each one. This is a comprehensive register that ensures that risks are constantly evaluated. But mapping ensures that the biggest risks get the most attention. Risks are often grouped into categories in the register to make many related risks more manageable.
- **Evaluate the risks against the organisation's appetite for taking them.** This must ultimately be the board's call. It's a question of setting the parameters for whether particular risks should be accepted, rejected or managed in some way.
- **Treat the risks.** This involves decisions on whether particular risks should be avoided, reduced, transferred or accepted. Avoidance involves withdrawing from high-risk activities. Reduction involves mitigating either the likelihood or the impact of a risk by introducing internal control mechanisms. Transferral can occur through methods such as outsourcing, insurance or hedging, while acceptance implies that no action is necessary. The panel above shows the prioritisation of risks and appropriate responses to them using the likelihood/consequences (or impact/probability) matrix.
- **Report the risks.** This informs the whole organisation about the risks it faces and its responses to them, explaining how they are identified, assessed and managed. Only the biggest risks, in terms of their likelihood and consequences, need to be reported. Risk reports should show both the gross risk (before controls are introduced) and the net risk (after the effect of controls is taken into account) to demonstrate the cost-effectiveness of those controls.

A question that often emerges is whether organisational risk management is a bottom-up or top-down process. In practice, it is both. Business units and departments must identify and assess risks facing them at local level. The top management team will see more strategic risks as a result of changing economic, competitive or regulatory conditions. Both processes need to be combined to ensure that risks are identified and assessed throughout the organisation.

Best practice suggests that a risk management group (RMG) should be established to perform this seven-step process. The RMG should report formally to the board, usually through the audit committee or a separate risk committee. The group's recommendations will influence the internal controls that the organisation implements. The RMG should also monitor the effectiveness of the whole risk management process, making improvements as necessary. Together with internal and external audit, the risk management process ought to provide a high level of assurance to the board that an effective system for risk management and control exists.

The RMG operates at corporate level but can also advise individual business units and departments on their risk management practices. The seven-step process also takes place in business units and departments, where operational risks are identified, assessed, mapped and recorded on a register.

While an organisation's appetite for taking risks and its responses to them will generally be established by the board, a portfolio approach may result in differing appetites in different business units or departments, because the risk/return trade-off often varies in separate parts of an organisation. For example, a marketing department may be able to take risks in new promotions while an HR department will be risk-averse for fear of the problems caused by poor employment practices. It is important that risks identified at each level are communicated up and down the organisation. This is an important function of the RMG.

So risk management at individual level has a great deal in common with how it's done at organisational level. The seven-step process is a good way to think about how organisations deal with the risks that they face. FM