An appetite for risk

Emma Cundiff weighs up the pros and cons of developing an enterprise risk management programme.

Risks affecting organisations can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organisations to perform well in an environment full of uncertainty.

One of the roles of a health and safety professional is to support the development and maintenance of an effective safety management system. Within that system, they may devise risk assessment systems and oversee the process of assessing the risks to health and safety of employees and others as directed by various pieces of legislation. To many, this is ‘risk management’, but to others, risk management has a much wider context.

Setting the standard

The ISO 31000 Risk Management Standard defines risk management as ‘coordinated activities to direct and control an organisation with regard to risk’. Enterprise risk is often thought of as just financial risk, but to the general risk practitioner, it encompasses a whole range of risks that an organisation faces. Many of the spectacular business failures in recent years have been down to inadequate, or complete lack of, risk management. The effects reverberate around the globe and at a micro level affect those caught up in their negative aftershocks.

There is little regulation for the management of enterprise risk. Principle C2 of the UK Corporate Governance Code 2014 (UKCGC) states that ‘the board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives’. The law dictates how far an organisation must go in protecting people, but it is up to the board to decide how much risk the business is willing to take and how far they will take the risk management process. A board needs to be entrepreneurial in advancing the development of the organisation and sometimes they will need to take some risks.

But this risk taking must be informed. Directors who take entrepreneurial risks are seeking positive outcomes and need to identify what risks must be taken to achieve this, but they must also know what the downsides are and take steps to control them. How far these risks are controlled is entirely up to the directors.

ISO 31000 requires a policy – the allocation of risk responsibilities and analysis procedures need to be defined. The risk management process involves identifying the context in which the organisation operates. Risk events are identified and analysed using a predetermined set of risk descriptors. This enables the organisation to decide if the risk is adequately controlled in the context of its risk appetite.

Enterprise risk management is too broad a subject to be covered in a short article. But the skills that have been applied in the health and safety domain can be very useful in implementing an enterprise risk management system. Safety professionals need to be adaptable and accept that in some cases it’s going to be goodbye to ‘so far as is reasonably practicable’.

Emma Cundiff is an international enterprise risk management and occupational safety and health specialist

Further information
For more information, visit www.iso.org/iso/home/standards/iso31000.htm