Risk identification and measurement framework

The publication by the Financial Services Authority (FSA) of Consultation Papers (CP) 140 and 142 has increased the need for management of all types of risk, including operational risk. The CPs focus on the FSA's requirements in the form of management information and processes, but do not offer guidelines for implementation. This article explores the difficulties of implementing risk management and proposes a framework to ensure best practice risk management is achieved throughout the organisation.

Risk management

Regardless of the regulatory need, a governing board wants to know that all the risks inherent in its business are identified and quantified. Where appropriate, the risks should be mitigated efficiently, so that the extent and cost of the mitigation is commensurate with the risk impact. A high-level summary of the risk-management process can be described as follows:

– Identify each risk.
– Quantify each risk's significance as:
  - the probability of the risk occurring; and
  - the magnitude of the potential loss.
– Quantify the effectiveness of the mitigating controls.
– Take appropriate steps to reduce either the probability or the amount of the net loss to a level that can be retained.

In practice this process presents many difficulties, which we will illustrate by examining some of the questions that arise.

Risk identification

Successful risk management relies on a common understanding within the organisation of the risks it is exposed to. To someone unfamiliar with the topic, operational risk might be loosely associated with administration and IT systems. In fact, the Basel Committee on Banking Supervision has suggested operational risk is: 'the risk of loss, resulting from inadequate or failed internal processes, people and systems, or from external events.' Using this definition, operational risk is embedded in every aspect of a business. The most pressing question facing any organisation is: 'how do I know that I have completely identified all of the risks in the business?' While 100% risk elimination is neither desirable or possible, every effort must be made to identify the critical risks. A multi-faceted approach is needed to consider the risks inherent in the industry and those that are unique to the firm's own processes. This approach must take into account industry practice, as well as existing controls and the knowledge of management and staff.

Quantification of the risk probability and size of loss

In the June issue of The Actuary Mark Chaplin illustrated the problem of risk quantification. He showed a table of estimated mortality increases for one year ranging from 20% to over 50%, derived using various methods. These estimates were for mortality risk, which is clearly defined, easy to identify, has a large pool of supporting data, and is widely studied. It is much more difficult to estimate potential losses from an intangible event, such as the failure of a process.

How effective is our risk mitigation?

It is important to identify and quantify the effectiveness of the mitigating controls. While some controls are tangible, such as economic hedges, others are less tangible, and rely on people completing processes correctly. Measurement of the effectiveness of processes, their documentation and level of compliance must be part of any risk management review.

The risk management framework

Consistent methods must be applied throughout an organisation to ensure risk management standards are maintained in all areas. This framework should form part of a common risk philosophy embedded in the organisation's culture.

There are various approaches to facilitate risk management and each has its own strengths and weaknesses. Research conducted at Cranfield University helped develop an approach combining the best aspects of a number of techniques. The risk identification and measurement (RIM) framework is a tool for collecting information on risk and mitigating controls, and analysing that information to assess the performance of a risk management programme.

Implementation

Although it is tempting to try and assess the whole organisation simultaneously, it is better to divide the organisation into a number of units, based on either organisational or functional boundaries. Each of these units becomes the basis of a review area. Precise scoping of the review area and review objectives is critical to success.

The review team must then identify the existing business controls and processes. They also identify best practices in the relevant industry and in other industries facing the same issues. A panel of experts is chosen from the business area under review. Each panel member is interviewed to identify the risks in their area.

By combining the data gathered in the interviews with industry best practices, and the organisation's business processes, the review team can produce a comprehensive list of the risks the organisation faces. The list forms the basis of a questionnaire which is used by the expert panel to assess the probability and impact of the risk, and to give their opinion as to how well the firm has mitigated the risk. These results are tabulated, and the members of the panel are presented with the group response or their individual response and given an opportunity to reassess their opinion. This process is repeated three or four times until either consensus is reached or results between each iteration are stable.

The plotted results illustrate the significance of each risk and how successfully it is mitigated. If the level of significance and mitigation is broadly proportional then the results should fall along a diagonal line.

In practice, some risks are managed very well when compared to their level of significance. These are called 'excessive' risks. Other are not well mitigated when taking into account their significance these are 'negligent' risks. Every organisation can be expected to have at least a small number of negligent and excessive risks. However the RIM method has shown a significant number of risks can fall into these categories. An example of the results from a RIM review is shown in figure 2. The number assigned to each point on the graph references a specific risk. There are a significant number of negligent and excessive risks, showing that the organisation in question is overmanaging some less significant risks while undermanaging and even ignoring some very significant ones.

Continual self-assessment

The framework forms the basis of continual self-assessment of risk analysis and mitigation. Once the process has been conducted once or twice, it can be implemented by the organisation itself as often as necessary.

The RIM framework can also be applied to special projects, such as a major change project, an acquisition, or responding to a crisis. Implementing a RIM practice over the project helps manage the new risks and also makes the organisation appreciate that this is 'out of the ordinary', automatically changing risk culture in the project team.

The risk and mitigation analysis can be a cornerstone for discussion with the regulator in assessing capital adequacy for operational risk. It will also allow management to be better informed as to the nature and extent of the risks being borne by the shareholder's capital.