ICE Briefing Sheet

Enterprise Risk Management (ERM) Short Guide

Introduction

1. This Guide is for the Board Directors and senior staff of civil engineering organisations. It discusses Enterprise Risk Management (ERM), which goes to the very heart of the business and affects the whole corporate strategy. Particularly relevant at the present time of great uncertainty, the Guide covers some of the most important points which need to be addressed in thinking about an ERM framework for a company or other organisation, and recommends some key questions for the Board to consider.

What is Enterprise Risk Management (ERM)?

2. ERM is an ongoing proactive process across the enterprise, focussing on uncertainty and risk, and acting as a catalyst for radical thinking which can influence the organisation's future, helping it to survive and flourish in a rapidly changing world. ERM adopts a holistic approach to the uncertainty and risk which may affect, either positively or negatively, the achievement of key purposes and objectives. Uncertainty means lack of sufficient knowledge and risk means the possibility that outcomes may be different from those expected, either better or worse. ERM should lead to action to achieve greater business robustness and flexibility, efficient risk-taking, and an appropriate risk-reward balance. It will pay particular attention to achieving financial sustainability.

The need for a central focus on risk

3. The key point is that ERM requires a single central focus on the big uncertainties and risks. While all the parts of the organisation will have their own data and methods for tackling risks in their own specific areas of responsibility, ERM brings their results together, studies underlying causes of risk, and adds insights into how the business as a whole will react in a variety of future scenarios. This may lead in turn to new corporate strategies which enable the business to avoid the worst negative outcomes and seize opportunities which increase the chances of success.

4. So what do we mean by a central focus? In a very small organisation it could form part of the job of the CEO or Finance Director, but in a larger business it will probably need to be carried out by a full-time Risk Unit, headed by a Risk Officer who will report to a Board Member and may have a small specialist team. One of the functions of the Risk Officer will be to advise the Board on the key threats and opportunities for the entire business, and some of the options which might exist for reducing threats and increasing opportunities. He or she will be responsible for bringing newly emerging risks to the Board's attention. Another of the Risk Officer's functions will be to guide the rest of the organisation on the best ways in which they can manage uncertainty and risk.

5. One of the most important requirements is to have a good flow of information to the central risk function from all departments in the organisation. This will include the major threats and opportunities which the managers responsible for each department perceive in relation to their own parts of the business, and the actions they are taking as a result. The

risk function will analyse the information and consider the potential overall impacts on the business. One aspect the risk function will examine is whether there are common underlying causes which may result in the risks in different sections of the business materialising simultaneously. In addition, the risk function will continue to gather as much additional information as possible, from a variety of sources, about the risks and uncertainties for the business as a whole. The results of the ongoing analysis will be fed through to the Board regularly so that consideration can be given to any actions which may need to be taken.

Some challenges to setting up an ERM Framework

6. We believe that there are many organisations which have tried to establish an ERM Framework but have found it too difficult to make all the cultural and organisational changes which are required. Some of the main challenges that have been found in practice are:

- Creation of a risk-aware business culture throughout the enterprise, which facilitates top-down and bottom-up flows of quality information, allowing emerging risks to be identified in time to take action
- The integration of risk management within the business's culture and other business processes
- The establishment and maintenance of a single central focus on the key uncertainties and risks
- Difficulties in quantifying the likelihood and potential impact of risks
- Lack of necessary knowledge and skills within the organisation.

The result is that there may be risk practices which are called ERM but actually fall well short of what is needed.

Review of existing practices

7. We therefore recommend that the Board should review existing risk practices in the organisation and consider whether an adequate ERM Framework already exists. The key questions which could be examined in such a review include the following:

- Is there a central risk function?
- Does the leader of the central risk function and his team have the qualifications and experience to be able to identify the key threats and opportunities and to carry out the necessary analytical work?
- Does the business (and all parts of it) take a proactive and unbiased approach to the management of uncertainty, seeking to gather relevant additional knowledge as far as practicable?
- Is there enough knowledge about the extent to which risks may be connected with each other?
- Is there a proactive approach to the identification of newly emerging risks, so that responses can be developed before it is too late?
- Are any steps being taken to "model" the business as a whole, in a holistic manner, to enable the risks taken to be matched to the capability of the business to absorb risks, through the exploration of various possible future scenarios?
- Is enough thought being given to the wide range of scenarios which might arise?
- Are "stress tests" carried out, to investigate the capability of the business to respond to extremely adverse scenarios?
- Is there a focus on having sufficient financial flexibility in extreme scenarios?
- Is the risk function interwoven with corporate strategy and the business development process?

- Does the Board itself make sufficient time to discuss key threats and opportunities?
- Is there throughout the organisation, involving all staff, a suitable “risk aware culture” which focuses on opportunities as well as threats and does not normally allocate blame when adverse events occur?
- Is the communication system for reporting information and risks to the centre adequate?
- Is the governance process which is in place to control the big risks sufficiently strong?
- Are there some big risks which are already embedded in the organisation but are lying hidden?
- Is the Board’s risk map validated against independent/external sources?
- Does the Board define the organisation’s risk appetite and its risk tolerance, i.e. the extent to which it can safely take risks?

Conclusion

8. After a review of existing practices has been undertaken, decisions can be taken on whether it is worthwhile to put the necessary time, effort and expense into establishing a comprehensive ERM framework. Some organisational and cultural changes may be necessary, internal reporting systems may need to be strengthened, and a few specialists in risk management might have to be recruited. Depending on how much change is necessary, the amount of work required could be substantial. However, once an ERM framework is fully in place, the business will undoubtedly be more sustainable and have better chances of future success.

Acknowledgements

This note was prepared by the Risk Group of Civil Engineers and Actuaries, May 2020.