Enterprise Risk Management

Introduction

No matter your business goals, an enterprise risk management framework ("ERM") can help you achieve them.

Although every company practices risk management in some way, a formal ERM process puts methodologies in place so that your organisation can systematically increase its ability to achieve its strategic objectives. In the absence of risk management, a company is less likely to meet its business goals consistently, may make poor decisions and be less prepared for changes in the environment in which it operates.

A key impetus for the development of ERM arose from the regulatory requirements for financial institutions. In this context, ERM was focused primarily on minimising identified risks. Over time, ERM has broadened to consider the impact of risks on the ability of the organisation to achieve its strategic objectives.

The COVID-19 pandemic has created an efficient case study that illuminates the importance of risk management. Almost overnight, companies were severely tested by a range of issues, including insufficient employee protections, supply chain deficiencies, and unpredictability in revenue and profitability.

The fundamental elements of ERM are the:

- identification and assessment of significant risks and the implementation of suitable risk responses;
- identification of the appropriate risk response or treatment;
- development of a plan to manage the identified risks;
- development of initial processes to manage identified risks; and
- ongoing evaluation and review of the organisation's risk profile.

Business Risk Assessment

Business risk assessment is the initial cataloguing of the risks faced by the business. The review of risks needs to cover all material functional areas of the company.

Risks are usually categorised as follows:

- strategic risks;
- market risks;
- credit risks;
- liquidity risks; and
- operational risks.

The risk assessment usually includes an evaluation of each risk's potential impact and the likelihood that the risk will, in fact, materialise. For most organisations, the risk assessment is based on a numerical scale of "say" 1 to 10. Each risk's impact and likelihood scores are then multiplied together to give each risk an inherent risk score.

Business Risk Treatment

At a conceptual level, the treatment of each risk will include some combination of the following items:

- acceptance or tolerance of the risk;
- avoidance or termination of the risk;
- risk transfer or sharing via insurance,
- a joint venture or other arrangement; and
- mitigation of the risk through internal control procedures.

The effectiveness of the mitigation process must be scored based on its reduction on both the impact and likelihood of the risk.

The net risk score for impact and likelihood are then multiplied together to drive a level for residual risk for each risk.

Business Risk Management Planning

After the risk diagnostic has been performed, management will have a better sense of what the risks are and the potential impacts and likelihood that they could have. Management will then be able to plan its response to the identified risks.

The next steps would include:

- creation of a structure to catalogue the identified risk – this is usually referred to as the risk register;
- assessment of inherent risk for each risk. Inherent risk is the multiplication of the pre-control scores for impact and likelihood;
- assessment of residual risk for each risk. Residual risk is the multiplication of the post control scores for impact and likelihood;
- ranking of the identified risks based on both objective and subjective considerations;
- identification of key or perhaps top 10 risks; and
- formulation of a go-forward enterprise risk management process and document it.

Management

Once the risk management plan has been developed, management must execute the plan. The early stages of the ERM plan include

- rolling out, by senior management, the key objective and operational framework of the ERM plan;
- over time, the organisation will get to the point where it can establish a risk tolerance framework. Risk tolerance is essentially the level of residual risk that the Board of Directors and the management team deems acceptable;
- where there are key risks that have residual risk levels above the risk tolerance level, plans need to be rapidly developed and executed to drive residual risk below tolerance;
- some risks may be identified where it may be relatively easy to achieve material reductions in residual at minimal cost;
- training concerning risk issues should be provided through the organisation. This will assist in the development of a risk-based culture.

Management Review and Evaluation

Once the enterprise risk management plan in place, the next steps include:

- assess compliance with the ERM plans objectives, framework and processes;
- ongoing assessment of the effectiveness of controls. In some organisations, this can take the form of formal risk control testing;
- as experience is gained in the ERM process, refine of controls to reflect enhanced knowledge or changes in the underlying risk;
- a periodic review of the risk profile by the Board of Directors and /or management will help to avoid unexpected risk issues and will also send a strong message regarding the importance of the ERM programme;
- as risk management experience increases, management will be in a better position to identify the company's emerging risks and develop an appropriate mitigation strategy; and
- ERM programme results should be formally reported to the Board of Directors, senior management and other key stakeholders regularly.