Prerequisites for Effective Enterprise Risk Management

Dr David Hillson FIRM, HonFAPM, PMI Fellow

The term Enterprise Risk Management (ERM) describes ***a comprehensive and integrated framework for managing risk at all levels within an organisation.*** Four organisational characteristics are required if ERM is to work properly:

1. *Defined objectives at all levels.* Risk is defined in terms of objectives and without clearly defined objectives it is not possible to identify or manage risk. Objectives exist at various levels in an organisation, forming a hierarchical structure. ERM requires these objectives to be *clear* (everyone knows and agrees what they are), *aligned* (all objectives contribute to the overall goal) and *coherent* (fitting together as a set, both top-down and bottom-up).

2. *Matching organisation to objectives.* Effective organisations have structures that mirror the hierarchy of objectives, with clear mapping between levels. Senior management are responsible for achieving strategic objectives, and front-line staff (project teams, operational groups, supply chain partners etc.) must meet operational and delivery objectives. The levels in between are covered by middle management, and it is often here that objectives lose clarity, alignment and coherence.

3. *Clear boundaries.* Effective ERM requires clear interfaces between levels, for both objectives and the organisation. There must be no uncertainty about whether a particular objective belongs at a particular level or to the level above or below. The organisational hierarchy must be equally clear, with defined lines of responsibility, communication and decision-making authority.

4. *Risk-aware culture.* The organisation needs a fully mature risk-aware culture at all levels, with a commitment to manage risk wherever it is found, and this must be properly resourced and supported. ERM cannot operate effectively if any level within the organisation denies the existence of risk or refuses to take responsibility for managing risk in their area of authority.

What happens if one or more of these four elements are missing in your organisation? Perhaps there are no clear overall objectives, or your organisation is unstructured or has inconsistent boundaries, or the risk culture is immature? Is it possible to implement ERM in these circumstances?

An organisation that is deficient in one or more of these characteristics should take steps to develop them. Objectives can be put in place at the various levels across the business quite quickly, but it might take some time to implement structural changes to the organisation with clear boundaries and thresholds, and developing a risk-aware culture takes much longer.

In the meantime, it should be possible to get started. Why not use your part of your organisation as a pilot or demonstrator? First ensure that your objectives are clear and understood, and begin to develop risk awareness among your team. Then start to implement a cut-down version of ERM in your own "mini-enterprise". When this starts to make a difference, communicate and celebrate your achievements, telling your colleagues what you have discovered.

Success stories will encourage others to follow in your footsteps and will lead to a wider take-up of the principles and practice of ERM. If you have the courage and determination to act as a pioneer for ERM, others will follow, and eventually the whole organisation will change.

To provide feedback on this Briefing Note, or for more details on how to develop effective risk management, contact the Risk Doctor (info@risk-doctor.com), or visit the Risk Doctor website (www.risk-doctor.com).

About the Author

Dr. David Hillson

Author

Dr David Hillson CMgr FRSA FIRM FCMI HonFAPM PMI-Fellow is The Risk Doctor (www.risk-doctor.com). As an international risk consultant, David is recognised as a leading thinker and expert practitioner in risk management. He consults, writes and speaks widely on the topic and he has made several innovative contributions to the field. David's motto is "Understand profoundly so you can explain simply", ensuring that his work represents both sound thinking and practical application.

David Hillson has over 25 years' experience in risk consulting and he has worked in more than 40 countries, providing support to clients in every major industry sector, including construction, mining, telecommunications, pharmaceutical, financial services, transport, fast-moving consumer goods, energy, IT, defence and government. David's input includes strategic direction to organisations facing major risk challenges, as well as tactical advice on achieving value and competitive advantage from effectively managing risk.

David's contributions to the risk discipline over many years have been recognised by a range of awards, including "Risk Personality of the Year" in 2010-11. He received both the PMI Fellow award and the PMI Distinguished Contribution Award from the Project Management Institute (PMI®) for his work in developing risk management. He is also an Honorary Fellow of the UK Association for Project Management (APM), where he has actively led risk developments for nearly 20 years. David Hillson is an active Fellow of the Institute of Risk Management (IRM), and he was elected a Fellow of the Royal Society of Arts (RSA) to contribute to its Risk Commission. He is also a Chartered Fellow of the Chartered Management Institute (CMI) and a Member of the Institute of Directors (IOD).

Dr Hillson can be contacted at *david@risk-doctor.com*.