



RISK DOCTOR BRIEFING

PREREQUISITES FOR EFFECTIVE ENTERPRISE RISK MANAGEMENT



© December 2012, Dr David Hillson FIRM, HonFAPM, PMI Fellow

david@risk-doctor.com

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.