



## RISK DOCTOR BRIEFING

### HOW MATURE IS YOUR RISK CAPABILITY?

© December 2010, Dr David Hillson HonFAPM, PMI Fellow

[david@risk-doctor.com](mailto:david@risk-doctor.com)



Risk management is clearly an important factor in ensuring business and project success. But how can an organisation tell whether its management of risk is good enough? Maturity models provide a framework to benchmark capability and compare existing approaches with best practice. The first such model in the risk area was the *Risk Maturity Model* (RMM) developed in 1997. This describes four levels of increasing risk capability, termed *Naïve*, *Novice*, *Normalised*, and *Natural*:

- The *Naïve* risk organisation is unaware of the need for management of risk, and has no structured approach to dealing with uncertainty. Management processes are repetitive and reactive, with little or no attempt to learn from the past or to prepare for future threats or opportunities.
- The *Novice* risk organisation has begun to experiment with risk management, usually through a small number of nominated individuals, but it has no formal or structured generic processes in place. Although aware of the potential benefits of managing risk, the Novice organisation has not effectively implemented risk processes and is not gaining the full benefits.
- In the *Normalised* risk organisation, management of risk is built into routine business practice. Generic risk processes are formalised and widespread, and the benefits are understood at all levels of the organisation, although they may not be fully achieved in all cases.
- The *Natural* risk organisation has a risk-aware culture, with a proactive approach to risk management in all aspects of the business. Risk information is actively used to improve business processes and gain competitive advantage. An integrated multi-level risk process is used to manage opportunities as well as threats.

Each maturity level can be defined using four attributes – *culture*, *process*, *experience* and *application*:

- At Level 1 “Naïve”, the *culture* is resistant to change and the need for risk management is not recognised. There are no risk *processes*, no *experience* of using risk management and no *application* to projects or the business.
- The *culture* of the Level 2 “Novice” organisation tends to see risk management as an overhead and is not fully convinced of its benefits. *Processes* are ad hoc and their effectiveness depends on the limited *experience* of a few key individuals who have little formal training. Risk management *application* is inconsistent and patchy.
- Level 3 organisations have “Normalised” risk management into their way of operating, with a *culture* that recognises the existence of risk and expects to reap benefits from managing it. Generic and formal *processes* are in place, with the necessary resources available, and staff have adequate *experience* and expertise to undertake effective risk management. *Application* is routine and consistent.
- At Level 4 “Natural”, a risk-aware *culture* drives the organisation into proactive risk management, seeking to gain full advantage from its uncertain environment. Best-practice *processes* are implemented at all levels of the business, with regular updating, active feedback and learning. All staff have appropriate *experience* of using risk processes, and *application* is widespread and second-nature across all areas.

Risk management is too important for us to do it poorly. We need to assess and monitor our risk management capability, compare ourselves with best practice, identify areas of shortcoming that require improvement, and keep developing. Risk maturity models like RMM provide a valuable framework for such assessments. They can help organisations to benchmark risk management capability, design a structured path to improvement, and measure progress towards the goal of enhanced risk management effectiveness.