Simple Tools and Techniques for Enterprise Risk Management, Second Edition
by Robert J. Chapman

Appendix 6
Risk Maturity Models

This appendix should be read in conjunction with Section 8.7.2.

As discussed in Section 8.7.2, risk maturity models are useful tools in understanding the degree of sophistication of a business risk management process, its reliability and effectiveness in identifying, assessing and managing risks and opportunities. Hillson (1997) proposes a risk maturity model and provides guidance to organisations wishing to develop or improve their approach to risk management, allowing them to assess their current level of maturity, identify realistic targets for improvement and develop action plans for increasing their risk capability. The model is composed of four levels, which are described in ascending order as "naïve", "novice", "normalised" and "natural". The levels are defined as shown in Box A6.1.

Box A6.1 Hillson (1997) maturity model

Level 1 Naïve
The naïve risk organisation is unaware of the need for risk management and has no structured approach for 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 uncertainties.

Level 2 Novice
The novice risk organisation is experimenting with [the] application of risk management, usually through a small number of nominated individuals, but has no formal or structured generic process 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.

Level 3 Normalised
The normalised risk organisation has built management of risk into routine business processes and implements risk management on most or all projects. Generic risk processes are formalised and widespread, and the benefits are understood at all levels of the organisation, although they may not be consistently achieved in all cases.

Level 4 Natural
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. Risk processes are used to manage opportunities as well as potential negative impacts.

An alternative description of levels of maturity is proposed by the Central Computer and Telecommunications Agency (Government Centre for Information Systems 1993), again distinguishing between the levels of maturity by describing where in the organisation risk management is carried out and who is responsible for implementation (Box A6.2).

Box A6.2 Central Computer and Telecommunications Agency maturity levels

First level of maturity
The first type of organisation structure is the "virtual organisation", in which the management of risk is everyone's responsibility. In this situation, it is up to an interested individual manager to pursue good practice in respect to the management of risk.

Second level of maturity
The second level is where there is a separate management of risk group consisting of specialists who conduct analyses for operations, projects, and programmes and senior managers. Usually these groups operate on a task-by-task basis, examining a single high-risk project, for example. The usefulness of these groups depends greatly on the talents of the specialists involved and the individual managers' willingness to accept advice.

Third level of maturity
The third type of management of risk organisation exists when the specialist risk group is integrated within existing management groups at each organisational level. More formal mechanisms are needed to communicate risk information among these different groups. Although still mainly task oriented, more structured or formal management of risk approaches are put in place.

Fourth level of maturity
The fourth type of organisational structure is the fully integrated management of risk organisation. In this structure, the management of risk is everyone's responsibility, but formal mechanisms exist to help bring this about. A management of risk infrastructure that incorporates a standard analysis and management process exists.

Within the description of his model, Hillson describes four evaluation criteria – culture, process, experience and application – against which the four maturity levels are assessed. Each criterion using attributes of the typical organisation at each risk maturity model level. Hopkinson (2000) describes two Microsoft Access-based risk maturity models produced by a consultancy, one for use at the company (or business) level and one that is specifically applicable to the project environment. Both models adopt the four levels of maturity described by Hillson. The models determine the maturity of a risk management system (assumed here to be synonymous with process) by evaluating it against six criteria (called perspectives). For the company model these perspectives are management, risk identification, risk analysis, risk control, risk review and culture. For each perspective a series of questions are asked. The questions are weighted in accordance with the model's view of the significance of that question to the overall effectiveness of a risk management system. The overall assessment is considered to be only as high as the weakest score among the six assessments. Hopkinson explains that the rationale for this scheme of assessment is that the overall system for risk management is only as strong as its weakest area. The example he provides is "there is little point in having state of the art risk analysis, if the risk identification processes are so ineffective that many

of the important risks are ignored". Hopkinson describes the characteristics of organisations operating at what he defines as level 4 (the most mature level) – see Box A6.3.

Box A6.3 Hopkinson risk maturity model for businesses, level 4

Management
- Board's risk management (RM) policy reported to shareholders
- Management leads RM by example. Practical definition of "significant risks"
- Practical definition of the risks to be borne
- Clear RM channels of communication

Risk Identification
- All sources of risk considered, including strategic, financial, technological, resource, disaster, projects, operational and external
- New risks identified in a timely manner
- Unusual events investigated for risk
- All employees can identify risks

Risk Analysis
- Consistent definition of probability
- Consistent definitions of impact
- Prioritisation influences agendas and promotes cost effectiveness
- Widespread availability of RM expertise
- Analysis traces risk source and secondary effects
- Risk records retained on state of the art tools

Risk Control
- Risk control actions based on cost–benefit analysis after considering all strategies
- Well-focused actions on individuals
- Actions are consistently completed
- Business continuity planning as appropriate

Risk Review
- Annual formal board review of RM effectiveness
- Strategy for review of all risks maximises cost effectiveness
- New information on significant risks is reported immediately
- Board regularly review significant risks
- Risk reports optimised for effectiveness

Culture
- Board's policy translated into management instructions understood by all employees
- Atmosphere of mutual trust
- Proactive risk management rewarded. Key managers have good RM skills and relevant experience in the core business

Table A6.1 describes a business risk maturity model developed by the author for assessing business risk management processes. It has four maturity levels – initial, basic, standard and advanced. Each level is assessed against five criteria – culture, system, experience, training and management.

Table A6.1 Business risk maturity model

	LEVEL 1 - INITIAL	LEVEL 2 - BASIC	LEVEL 3 - STANDARD	LEVEL 4 - ADVANCED
OVERVIEW	• Compliance only approach • Risk appetite not defined • No framework developed • Risk profile not defined • No senior management buy-in to RM as a decision tool	• RM established for business improvement • Risk appetite defined • Framework established • Risk system established • Risk profile defined	• RM built into routine business processes covering end-to-end production or delivery of services • Benefits recognised at all levels of the organisation	• RM considered critical to achievement of the business goals • Approach communicated to the organisation as a whole • Risk appetite transparent • Business seeks continuous improvement • Proactive upside (opportunity) RM • Sophisticated modelling techniques
CULTURE	• RM established to meet the Combined Code, the Listing Rules and annual reporting • Specific risk management roles not defined	• Risk exposure defined • Roles and responsibilities defined • Meeting structure defined • Decision-making mechanisms established	• Pro-active approach to RM to improve business performance • Central risk management function created • High level risks and responses debated at the board on a regular cycle	• RM culture lead by the chief executive • RM information used in decision making • RM roles and responsibilities included in the induction process, job descriptions and performance appraisals • Proactive enforcement of RM through employment contracts

SYSTEM	• Risk strategy unclear • Risk framework (and its constituent parts) embryonic	• RM framework under development • OR or business continuity management not addressed • Poor data collection and trend analysis	• RM strategy defined, relevant and practical • RM framework developed • OR and business continuity management frameworks being implemented	• RM strategy defined and kept under review • RM framework developed and benchmarked against best practice
EXPERIENCE	• Very limited understanding of systems, terminology or software	• Limited to small number of the audit committee and company secretary	• In-house core of experienced individuals in systems, modelling and response planning	• Risk awareness throughout the organisation plus external support
TRAINING	• No training provided in-house or from external support	• Training undertaken by audit committee members	• Risk manager appointed • Risk committee established	• Training and education programme provided to all business unit heads
MANAGEMENT	• Management practices focussed on satisfying the Combined Code and the Listing Rules	• Economic capital allocated to Operational Risk • Operational Risk management reactive • Risks reviewed on a yearly basis	• Guidance on risk–reward balance provided to line management • Early warning indicators established for OR • Economic capital allocated to risk	• Guidance on risk–reward balance provided to line management • Early warning indicators established for both OR and business context • Reputational risk addressed

REFERENCES

Government Centre for Information Systems (1993) *Introduction to the Management of Risk*. HMSO, Norwich.

Hillson, D. (1997) Towards a risk maturity model. *International Journal of Project and Business Risk Management*, 1(Spring), 35–45.

Hopkinson, M. (2000) Risk maturity models in practice. *Risk Management Bulletin*, 5(4).