

# Towards a Risk Maturity Model

\*

**Dr David A. Hillson**

Head of Risk Management, HVR Consulting Services Limited, Selborne House, Mill Lane, Alton, Hampshire GU34 2QJ

## ABSTRACT

Organisations wishing to implement a formal approach to risk management or to improve their existing approach need a framework against which to benchmark their current practice. Best practice benchmarks can be defined in terms of maturity, usually reflecting increasing levels of sophistication together with other features. This paper describes a Risk Maturity Model with four levels of maturity, each linked to four attributes. Organisations can use this model to assess their current level of maturity, identify realistic targets for improvement, and produce action plans for developing or enhancing their risk capability.

## INTRODUCTION

All enterprises face risk and uncertainty, both at the project level and the business level, and there is an increasing recognition of the need for formal structured approaches to deal with risk. Many organisations are becoming aware of the importance of risk management for the success of both projects and enterprises. There is a growing demand for assistance in developing effective processes to help in the identification, assessment and management of risk, as organisations seek to tackle the uncertainties facing them.

Despite the widening consensus on the value of risk management, effective implementations of risk processes into organisations are not common. Those who have tried to integrate risk management into their business processes report variable degrees of success<sup>1,2,3</sup> and many give up the attempt without achieving the promised benefits. In many cases it appears that expectations were unrealistic, and there was no clear vision of what implementation would involve or how it should be managed.

Organisations wishing to implement a formal structured approach to the management of risk need to treat the implementation itself as a project, requiring clear objectives and success criteria, proper planning and resourcing, and effective monitoring and control. In order to define the goals, specify the process and manage progress, it is necessary to have a clear view of the organisation's current approach to risk, as well as a definition of the intended destination. The organisation must be able to benchmark its present maturity and capability in managing risk, using a generally accepted framework to assess current levels objectively and assist in defining progress towards increased maturity.

\* Current contact details :



**DR DAVID HILLSON** PMP FAPM FIRM  
PARTNER

### RISK DOCTOR & PARTNERS

3 Lower Heyshott, Petersfield, Hants GU31 4PZ, UK  
Tel/Fax: +44 (0)1730 300895 Mobile: +44 (0)7818 098886  
Email: david@risk-doctor.com Web: www.risk-doctor.com

### **EXISTING MATURITY MODELS**

The concept of maturity models is well developed and accepted. The Software Engineering Institute (SEI) at Carnegie-Mellon University has developed a Capability Maturity Model (CMM) for software engineering organisations<sup>4,5</sup>. This defines five levels of increasing capability and maturity, termed Initial (Level 1), Repeatable (Level 2), Defined (Level 3), Managed (Level 4) and Optimising (Level 5). Each level is clearly characterised and defined, enabling organisations to assess themselves against an agreed scale. Having discovered its CMM level, an organisation can then set clear targets for improvement, aiming towards the next level of capability and maturity.

Although the SEI CMM is well established, its application is limited to organisations involved in software development processes. There have been several attempts to broaden the scope of the CMM to other types of project, but these have not gained widespread currency.

Another common model for benchmarking organisational performance is the Business Excellence Model from the European Foundation for Quality Management (EFQM)<sup>6</sup>. This defines nine criteria for business excellence : Leadership, People Management, Policy & Strategy, Resources, Processes, People Satisfaction, Customer Satisfaction, Impact on Society, and Business Results. Each criterion is defined in terms of success factors, allowing the enterprise to assess current performance, compare itself against European best practice, and develop strategies for improvement.

The SEI CMM and the EFQM Model are general models of capability, maturity and business excellence. Neither model provides specific assistance to an organisation intending to implement formal risk management processes, or wishing to improve its existing approach, although some preliminary work has been reported on modifying the CMM to apply to risk<sup>7</sup>. This work was limited to risk management within software development organisations, focusing on tools and techniques, and does not appear to have been developed further.

A generic risk-focused maturity model would be of considerable assistance to organisations wishing to implement formal risk processes or improve the existing approach. Such a model could draw on the principles of the CMM and EFQM Model, but specifically apply them to the risk management arena. It should also be applicable to all types of organisation in any industry sector.

This paper offers a framework to allow an organisation to benchmark its approach to risk management against four standard levels of maturity, and outlines the activities necessary to move to the next level. The Risk Maturity Model (RMM) described here provides clear 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 four RMM levels are outlined, followed by guidelines to allow diagnosis of current level. Suggested strategies for developing towards the next level of maturity are then discussed.

### **THE RISK MATURITY MODEL FRAMEWORK**

The approach of organisations towards the management of risk can be categorised into groups which range from those who have no formal process through to organisations where risk management is fully integrated into the business. In order to reflect this with clarity

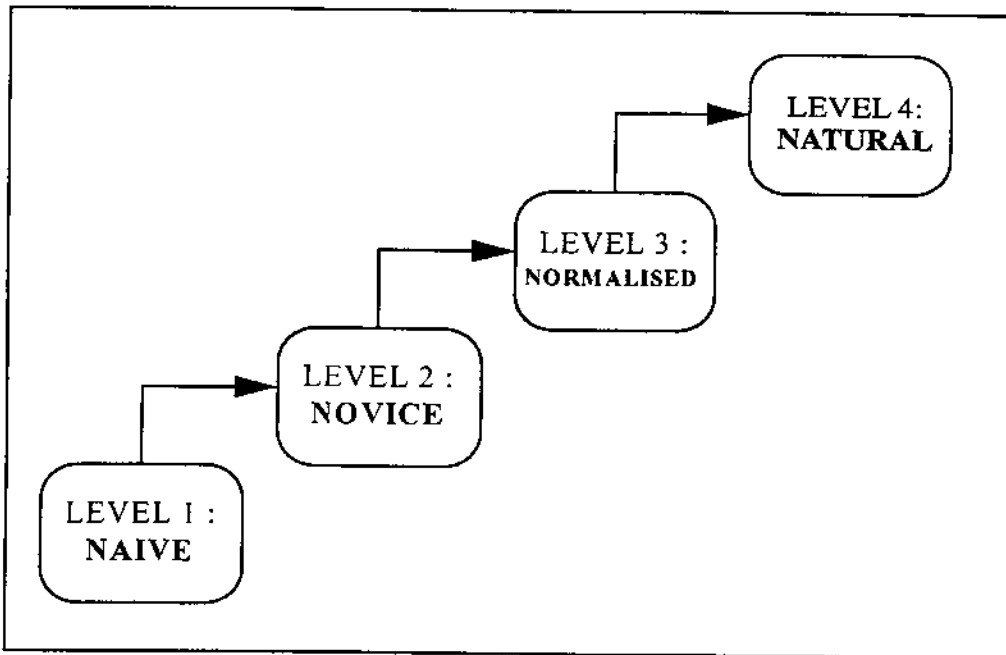


Figure 1. The four levels of Risk Maturity

and simplicity, the Risk Maturity Model (RMM) proposed here provides four standard levels of risk maturity (Figure 1). It is recognised that some organisations may not fit neatly into these categories, but the RMM levels are sufficiently different to accommodate most organisations unambiguously. It is felt that more than four levels would increase ambiguity without giving sufficient additional refinement to aid use of the model.

The RMM levels are as follows :

*Level 1 - Naïve*

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 uncertainties.

*Level 2 - Novice*

The Novice risk organisation is experimenting with application of risk management, usually through a small number of nominated individuals, but 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.

**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.

**DIAGNOSING RISK MATURITY LEVEL**

The brief descriptions of each RMM level indicate where an organisation stands in terms of the relative maturity of its risk processes, but a more detailed diagnostic tool is required for objective and consistent assessment of risk maturity.

Table 1 presents attributes of the typical organisation at each RMM level, under four attribute headings: Culture, Process, Experience, and Application. This enables an organisation to compare itself against clear criteria in order to assess its current level of risk maturity. It is recognised that some organisations may cross the boundaries between successive RMM levels, but the granularity between levels is such that there should be a clear distinction in most cases, and it should prove possible to allocate most organisations unambiguously to a single level.

The assessed RMM level can be used in a number of ways. For example, organisations may wish to enhance their level of risk capability, devising strategies to enable more effective management of risk. Alternatively, they may want to rate themselves against key competitors in order to gain advantage in the marketplace.

**PROGRESSING BETWEEN MATURITY LEVELS**

Once risk maturity is assessed, steps can be taken to develop action plans for moving towards the next level. The author is not aware of any organisation which is currently at Level 4. Many are at either Level 2 or Level 3, or have embarked on the transition from Level 2 to Level 3, while a significant number remain at Level 1.

Given the increasing profile of risk management, and the growing awareness of the business benefits that can be gained by effective management of uncertainty, many organisations are seeking to implement formal risk processes. Most start at Level 1 and aim for Level 3. It is important however for an organisation to accurately identify its current position, since the barriers to be overcome in moving from Level 1 to Level 3 are considerable, and a more measured approach (for example via Level 2) may be more successful in the long term. Similarly, if an organisation is already at Level 2, some of the early steps in developing a risk process may be omitted or shortened. Finally, once the goal of Level 3 is reached and an organisation has implemented formal risk management into its routine

	<b>LEVEL 1 - NAIVE</b>	<b>LEVEL 2 - NOVICE</b>	<b>LEVEL 3 - NORMALISED</b>	<b>LEVEL 4 - NATURAL</b>
<b>DEFINITION</b>	Unaware of the need for management of risk. No structured approach to dealing with uncertainty. Repetitive & reactive management processes. Little or no attempt to learn from past or to prepare for future.	Experimenting with risk management, through a small number of individuals. No generic structured approach in place. Aware of potential benefits of managing risk, but ineffective implementation, not gaining full benefits.	Management of risk built into routine business processes. Risk management implemented on most or all projects. Formalised generic risk processes. Benefits understood at all levels of the organisation, although not always consistently achieved.	Risk-aware culture, with proactive approach to risk management in all aspects of the business. Active use of risk information to improve business processes and gain competitive advantage. Emphasis on opportunity management ("positive risk").
<b>CULTURE</b>	No risk awareness. Resistant/reloctant to change. Tendency to continue with existing processes.	Risk process may be viewed as additional overhead with variable benefits. Risk management only used on selected projects.	Accepted policy for risk management. Benefits recognised & expected. Prepared to commit resources in order to reap gains.	Top-down commitment to risk management, with leadership by example. Proactive risk management encouraged & rewarded.
<b>PROCESS</b>	No formal processes.	No generic formal processes, although some specific formal methods may be in use. Process effectiveness depends heavily on the skills of the in-house risk team and availability of external support.	Generic processes applied to most projects. Formal processes, incorporated into quality system. Active allocation & management of risk budgets at all levels. Limited need for external support.	Risk-based business processes. "Total Risk Management" permeating entire business. Regular refreshing & updating of processes. Routine risk metrics with constant feedback for improvement.
<b>EXPERIENCE</b>	No understanding of risk principles or language.	Limited to individuals who may have had little or no formal training.	In-house core of expertise, formally trained in basic skills. Development of specific processes and tools.	All staff risk-aware & using basic skills. Learning from experience as part of the process. Regular external training to enhance skills.
<b>APPLICATION</b>	No structured application. No dedicated resources. No risk tools.	Inconsistent application. Variable availability of staff. Ad hoc collection of tools and methods.	Routine & consistent application to all projects. Committed resources. Integrated set of tools and methods.	Second-nature, applied to all activities. Risk-based reporting & decision-making. State-of-the-art tools and methods.

**Table 1: Attributes of RMM Levels**

business processes, it should be recognised that there is a further level to which an organisation may aspire, namely Level 4 where the full benefits of effective risk management can be gained.

Different barriers are faced by organisations at each of the RMM levels, which must be overcome if progress is to be made to the next level of risk maturity. These are outlined below, together with suggested strategies for overcoming them.

*Level 1 to 2 - Naïve to Novice*

The Naïve Level 1 organisation faces a number of obvious handicaps if it wishes to start the journey towards implementing effective management of risk.

- Initially there will be no understanding of the risk process, and even the language and terminology will be unfamiliar.
- There is no clear concept of the benefits that can be gained from formal risk management, and the cost of implementing the process is also unlikely to be recognised.
- There is no in-house expertise or experience in performing risk management, with no specific experience on which to draw when considering the applicability of risk management to the needs of the organisation.
- Since the Naïve organisation has no formal risk management in place, it is likely that at least some of its projects and business processes will be in crisis at any given time, leading to a lack of time, energy or resources to commit to a new process.
- Finally, the management of a Naïve organisation may not be receptive to anyone external to the organisation who is promoting the risk management discipline, since they are uninformed customers and lack any track record or yardstick against which to judge the promised benefits. Also recognition that the organisation's processes are subject to uncertainty may be seen as an admission of weakness.

In order to develop from a Naïve Level 1 organisation towards the next RMM level, a number of actions can be undertaken. These are listed below.

- Clearly define the objectives of the risk implementation project, to enable the risk process to be tailored and scoped accordingly.
- Take advice from recognised external experts who have a track record in assisting organisations in this type of implementation. These should be selected carefully, and the organisation should beware of being encouraged to adopt a generic solution that does not match their particular requirements.
- Identify staff to act as the advance party, carefully selecting and building a prototype team. Ensure adequate training and support for these staff, including all the necessary risk skills and techniques, to ensure that internal staff can act as "intelligent customers".
- Undertake awareness briefings (perhaps using the selected external experts), to sell the vision of risk management and its potential benefits. This should include

the entire organisation, from senior management to front-line workers. Senior management should be briefed on corporate benefits, with project staff being made aware of the impact on their areas of responsibility.

- Ensure corporate backing, with nomination of a senior management sponsor to promote the implementation process.
- Nominate pilot applications for risk management, carefully selected to maximise the chances of early success.
- Publicise and celebrate successes. Seek to develop momentum in the risk process, to encourage others to apply risk management to their areas as they see clear benefits.
- Plan for the long-term, recognising that effective implementation of risk management will not be achieved overnight. Count the cost of the implementation project, and ensure commitment of the necessary resources before embarking.
- Build effective controls into the process from the outset, with breakpoints to enable progress to be monitored and reviewed at key intervals.
- Investigate availability of appropriate tools, considering the need to integrate with existing infrastructure. Beware of selecting tools too early, before the process is fully defined.
- Consider producing draft risk procedures, with templates for key inputs and outputs.

*Level 2 to 3 - Novice to Normalised*

The organisation currently at Level 2 (Novice) probably has a number of individuals (possibly only one) nominated to investigate and apply risk techniques. These people will be aware of the potential benefits of risk management, and will be exploring possible avenues for using risk processes. Limited support may have been sought from external consultants. At the Novice level, risk management is seen as an additional activity to be undertaken where necessary, and so the risk process is unlikely to be used consistently or widely, with application limited to a few major or significant projects.

This introduces a number of barriers to be overcome if the Novice organisation is to reach Level 3 and normalise the application of risk management across the organisation. It should be recognised however that some organisations may choose to remain at Level 2, with risk management being undertaken by a small in-house team on selected projects only. The transition to Level 3 should only be undertaken if the benefits are worth the cost and effort involved.

Barriers faced by the Level 2 organisation wishing to progress to Level 3 are listed below.

- Lack of formal risk processes produces inconsistency of application.
- Dependence on the skills of in-house staff could limit effectiveness of the risk process.
- The enthusiasm of those promoting risk management may be counterproductive, resulting in alienation of peers, management, customers etc.
- Lack of support for those championing risk management may lead to disillusionment and low morale.

*Dr D. A. Hillson*

- Limiting promotion of risk to the lone enthusiast can undermine the credibility of the risk process.
- Partial or inconsistent application of risk processes is unlikely to generate useful metrics which demonstrate the benefits of managing risk. There is therefore no auditable track record of what risk management can achieve, resulting in a lack of credibility and a reluctance to adopt risk more formally.

These barriers can be addressed in a number of ways to enable the Level 2 Novice organisation to progress towards Level 3. Where the actions listed above for the Level 1 to 2 transition are not in place, these should be considered in addition to those given below.

- Reinforce and strengthen corporate backing for those nominated to undertake the risk process. Visible endorsement from senior management is essential to give the necessary credibility.
- Undertake formal risk training to develop existing in-house expertise.
- Use external expertise to reinforce and support existing internal skills. This can also be particularly useful to extend the existing risk process into new parts of the business, which may be outside the areas of expertise or knowledge of internal staff. External consultants can also be used to apply the risk process to novel or difficult areas.
- Allocate adequate resources to the risk process, with transfer or recruitment of suitable staff, and nominated budgets for risk training, risk assessment tools and risk management activities.
- Select key projects to demonstrate the benefits of risk management in all areas of the organisation's business.
- Continue to publicise and celebrate successes, encouraging wider application of risk management to other areas as benefits become clear.
- Expose internal staff to outside influences, including training courses, conferences and seminars, expert bodies, books and journals etc.
- Formalise the risk processes, with clear definition of the scope and objectives of risk management, together with agreed procedures and properly selected tools. Consider developing and promulgating a company policy statement on use of risk management.
- Build risk management into the routine management of projects and business processes. Include regular risk reporting in management reviews.
- Start to gather metrics from the risk process, to identify generic risks, effective responses, the cost of risk reduction, etc. Specific checklists can be generated to facilitate the risk identification and assessment processes, based on actual experience of risk management within the organisation.

*Level 3 to 4 - Normalised to Natural*

Many organisations would be content to reach Level 3, where risk processes are integral to the business and are consistently and routinely applied to most or all projects. However

the Risk Maturity Model identifies a further level beyond Level 3, where identifying, assessing and managing uncertainty becomes second-nature and is built into all the activities and business processes of the organisation. In addition, risk processes can be used to address those uncertainties which have potential positive impact, i.e. opportunities or "upside risk". In many ways the Level 3 to 4 change is the most difficult transition to make, since the Normalised organisation may be complacent, believing that it has fully implemented risk management and no further change is needed. Indeed an organisation may wish to remain at Level 3 if this provides adequate management of project and business uncertainty. If, however, the Level 3 organisation wishes to progress to Level 4, the following threats are likely to be encountered.

- Loss of momentum could result in failure to maintain the required standards of application, with resultant loss of quality of risk support. This would reduce the credibility of the risk process, which could be seen as a temporary management fad whose time has passed.
- The organisation could fail to update the risk process to take account of changes in business needs or other developments in the marketplace. This would result in the risk process becoming outdated and increasingly irrelevant to the business of the organisation.
- Lack of continued investment in the risk process could also result in reduced relevance or capability, as tools become obsolete, techniques become superseded and staff skills are not updated or refreshed.
- Development of in-house expertise might result in risk management being seen as a specialist discipline which is undertaken by experts, with consequent reduction in commitment and ownership by others in the organisation.

Actions to assist the Level 3 organisation in its progress towards Level 4 are given below.

- Ensure effective learning from experience. Undertake regular reviews of the risk process, with value engineering of the process to ensure that it remains fully effective.
- Amend and strengthen the risk process where necessary, including investment in new tools, new methods, staff training etc.
- Investigate novel applications of the risk process beyond those already covered. Seek to modify and apply risk management to every activity within the business.
- Use every means possible to develop a "Total Risk Management" culture, encouraging staff to "think risk", being aware of uncertainty and using risk techniques to assess and manage potential threats. Build risk thinking into the corporate culture.
- Ensure that risk is included as a routine criterion in all decision-making.
- Identify and counter incidence of "risk fatigue", where staff are losing interest in the process or there is a potential loss of momentum. Use regular re-launch promotions to renew the process, celebrating successes, publicising improvement

*Dr D. A. Hillson*

metrics, and rewarding effective risk management.

- Undertake regular refresher training to ensure that skills remain current.
- Consider use of external risk expertise to widen the application of risk management into novel areas of the organisation, or to add the necessary momentum to maintain progress or introduce change.

#### ***Maintaining Level 4***

Few organisations succeed in making risk management a natural part of corporate culture, applying risk techniques throughout the business and proactively managing uncertainty (including both risks and opportunities) in order to maximise the benefits. Once this is achieved however, effort must be expended to maintain this position. The Level 4 Natural risk organisation is threatened by complacency and boredom and should consider a number of actions to counter these, including those listed below.

- Ensure continued commitment of senior management. It may be necessary or beneficial to change the sponsor from time to time to allow injection of fresh ideas and momentum.
- Use audit and review techniques to keep application of risk techniques at the required quality and standards.
- Take full advantage of the competitive edge which results from proactive management of uncertainty (including both risks and opportunities).
- Extend risk management beyond the usual applications, pioneering its use in all areas of the business.
- Continually invest in improving the risk process, tools, techniques, staff skills etc.
- Involve customers and suppliers in the risk process.

#### **CONCLUSIONS**

The implementation of risk management into an organisation is not a minor challenge, and cannot be undertaken in a short period of time. It is also not a simple process of identifying techniques, sending staff on training courses, buying software and getting on with it. Risk capability is a broad spectrum, ranging from the occasional informal application of risk techniques to specific projects, through routine formal processes applied widely, to a risk-aware culture with proactive management of uncertainty.

The Risk Maturity Model (RMM) presented in this paper allows organisations to benchmark their risk capability against four standard levels of maturity, in order to identify what needs to be done in order to improve and develop their ability to manage risk. Use of the RMM will also enable those who offer support to organisations to diagnose the current position, and will aid in the development of specific strategies for progressing implementation effectively.

Future work is required to enhance the diagnostic elements of the RMM, and development of a self-assessment questionnaire is being considered, to further aid in identification of the current RMM level at which an organisation is operating. However the present RMM framework provides a useful tool to those wishing either to implement

a formal approach to risk management or to improve their existing approach.

#### **REFERENCES**

1. LAY G. (1997) Implementing project risk management in Lloyds Bank IT, *Int J Project & Business Risk Mgt*, 1 (1), 49 - 56.
2. KRANTZ L.G. & TURNER G.J. (1997) Introducing Project Risk Management into an International Business, *Int J Project & Business Risk Mgt*, 1 (1), 65 - 80.
3. FISHER D. & WELLS D.E. (1997) Risk Management on the Inland Revenue CESA Project, *Int J Project & Business Risk Mgt*, 1 (1), 17 - 27.
4. PAULK M.C., CURTIS W., CHRISSIS M. & WEBER C.B. (1993) Capability Maturity Model, Version 1.1, *IEEE Software*, 10 (4), 18-27.
5. PAULK M.C., WEBER C.B., CURTIS W. & CHRISSIS M. (editors) (1995) *The Capability Maturity Model: Guidelines for improving the software process* (Addison-Wesley, ISBN 0-201-546647)
6. Contact the European Foundation for Quality Management (EFQM), Avenue des Pléiades 15, B-1200 Brussels, Belgium. Telephone +32.2775.3511, Fax +32.2775.3535, e-mail info@efqm.org
7. HALL E., "Evolution of essential risk management technology", 3rd SEI Conference on Software Risk, Pittsburgh, April 1994.

*Dr David Hillson is Principal Consultant and Head of Risk Management at HVR Consulting Services Ltd, Alton, UK. He is responsible for the company's Risk Group, as well as undertaking consultancy tasks for major clients. David is Editor of The International Journal of Project and Business Risk Management, a fellow of the Association for Project Management, and a member of the Institute of Management.*