The Project Risk Maturity Model

Measuring and Improving Risk Management Capability

GOWER

Level 3

Level 2

Overall
Asessment

Level 1

75%

50%

Stakeholders

Risk
Identification

Risk
Analysis

Risk
Responses

Project
Management

Culture
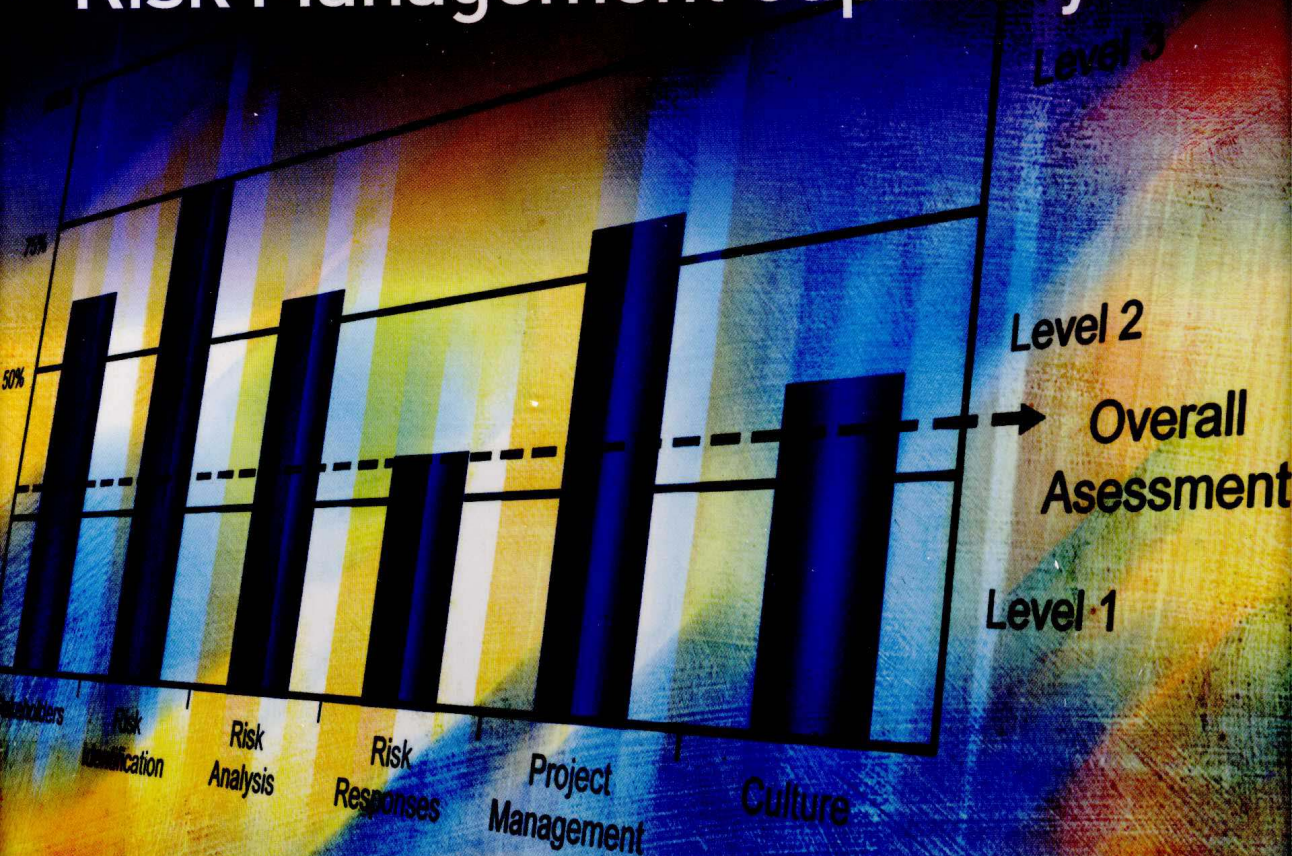
Martin Hopkinson

Foreword

As I write this Foreword I've just celebrated another birthday. Among the cards are an increasing number that mention memory loss, hair loss, or the fire hazard caused by the large number of candles on my cake. This is confusing. Long-time acquaintances have started referring to me as an 'old friend' and younger relatives appear to think I'm already past it. But a good friend in his late seventies sent a card describing me as 'the Birthday Boy'. And my self-perception is of someone in his prime, finally getting to an age where life is beginning to make some sense. Older? Definitely. Wiser? Maybe.

Apparently I'm not as young as I was. Perhaps I am maturing.

But what is maturity? The word is used in at least two ways. One meaning is to be fully developed, ripe, at the peak of perfection, having reached the maximum level of development. A fully mature cheese or wine is a delight. But the word is also used to mean no longer young, with implications of being old and of no further use. When an investment matures it reaches the end of its life, and some think that the same applies to older people. One-time sex kitten Brigitte Bardot recognised this dual meaning when she was interviewed at the age of 73. Asked how she felt about being old, she defiantly replied 'I have not grown old, I have ripened.'

The Irish poet John Finlay defined maturity as 'the capacity to endure uncertainty', and as we face increasing uncertainty all around us, more and more organisations aspire to maturity in a range of areas of competence. There has been a rapid growth in so-called 'maturity models' which claim to measure degrees of capability in various disciplines, aiming to help organisations become 'more mature'. In 2007 the UK Association for Project Management (APM) surveyed maturity models in the project management space, and found many competing offerings. For example the Project Management Institute (PMI®) offers its Organisational Project Management Maturity Model (OPM3®), the UK Office for Government Commerce has both the Portfolio, Programme and Project Management Maturity Model (P3M3©) and the PRINCE2 Maturity Model (P2MM©), and the International Project Management Association has developed their Project Excellence Model.

Even in the relatively specialised area of risk management, several specific maturity models exist, some of which have a considerable track record of use in different industries and organisations across the world. I have a long-standing interest in the subject dating from the mid-1990s, and in 1997 I published the first framework for assessing the maturity of risk management capability within an organisation. It has always seemed important to me not just to do something and to be seen to be doing it, but to do it well. But how would you know whether your management of risk is good, bad or indifferent? There are many factors that contribute to competence in managing risk, for example, the risk culture of an organisation, as well as its risk processes, its risk infrastructure, and the risk knowledge and skills of its people. The better risk management maturity models incorporate all these areas, and the organisations with more mature approaches to managing risk are competent in each aspect.

So what is 'risk management maturity'? Does it mean that the approach to risk management in a particular organisation is fully ripened, has developed as far as it can, no further improvement is possible, and everything is as good as it's going to get? Or does it imply being past it, with a degree of inflexibility, being set in one's ways, in a rut, and doing things because 'we've always done it that way'? Neither of these seems to be attractive options or worthwhile goals.

The clue is in the full name of the original maturity model first produced by the Software Engineering Institute of Carnegie Mellon University (SEI), which was responsible for triggering my interest in the topic of maturity. Targeting software development organisations, the SEI Capability Maturity Model (CMM) framework was first outlined in 1989 and fully published in 1993, and the key word in its name is 'capability'. The aim is not merely to 'be mature' but to have a 'mature capability'.

Having a mature risk management capability appears to be a desirable goal to which every organisation should aspire. This requires an approach to risk management which is constantly refreshed and renewed, adopting new techniques as appropriate, keeping up to date with the latest thinking and developments, learning from leading practitioners in our own and other industries, offering refresher skills training to our staff and so on.

But something is required to enable us to become and remain mature in the way we manage risk. We need an accepted framework to assess our risk management maturity, allowing us to benchmark ourselves against a recognised standard. We also need a structured pathway for improvement, not just telling us where we are now, but describing the steps required for us to reach the next level. The *Project Risk Maturity Model* detailed in this book provides such an assessment framework and development pathway for risk management capability in projects. It can be used by organisations to benchmark their project risk processes, and it can support introduction of effective in-house project risk management. Using this model, implementation and improvement of project risk management can be managed effectively to ensure that the expected benefits are achieved in a way that is appropriate to the needs of each particular organisation.

We all need to beware of complacency, especially in risk management. In our ever-changing world, what worked yesterday may not be good enough for today or tomorrow. Just because we've been doing something for a long time doesn't mean we're doing it well. Risk management is too important for us to allow it to fade away or become ineffective. 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. The *Project Risk Maturity Model* provides an answer for those who know that they haven't yet peaked in project risk management capability, or who want to maintain or improve their ability to manage project risk. Martin Hopkinson has done a great job over the past ten years in developing the *Project Risk Maturity Model* into a robust framework, and this book allows others to access and apply his insights and experience. I'm pleased to recommend it.

Dr David Hillson, The Risk Doctor
Petersfield, Hampshire, UK
March 2010

Preface

I joined HVR Consulting Services in 1999, impressed by both its customer reputation and the range of risk management and cost forecasting tools it had developed. Given that it was a company of 60 employees focusing on consultancy rather than tool development, it was clear that its people had been encouraged to engage in development activities as well as fee earning work. I would have a similar opportunity. The most interesting opportunity for development struck me as being the Risk Maturity Model (RMM).

The Risk Maturity Model had originally been conceived by David Hillson during his time leading risk management at HVR. His paper 'Towards a Risk Maturity Model' had been published in the *International Journal of Project and Business Risk Management* in 1997. This paper described four levels of risk management capability that could be found in projects and businesses. It also included a matrix (reproduced in Appendix A) to help organisations measure the maturity of their risk management process by assessing their capability level. The ideas behind this seemed both sound and useful. Given my 14 years' experience of projects, I was interested in building upon these ideas to produce a model specific to project risk management.

On this basis, I compiled and refined a collection of questions to include in the Project RMM. To help in this task, I drew not only on my own experience but also that of other members of the HVR risk management team. This team had established a good reputation amongst its clients over a period of many years. It had a particularly good record for producing realistic risk-based project forecasts; project outcomes tended to fall within the range of forecast possibilities to a much greater extent than I had seen in other organisations. Indeed, where relationships with clients had been difficult, this was usually the consequence of HVR's forecasts being more realistic than the client liked to admit! Lessons learned from HVR's risk management experience could therefore be incorporated into the RMM. Later, as the model was being calibrated, there was also a wide range of projects that could be used for this purpose.

As the model was being developed, I also drew upon other sources. First, with fortunate timing, the Turnbull Guidance[1] was published in October 1999. The Turnbull Guidance recommends the use of a risk-based system for a company's system of internal control. In 1999, it was issued as guidance for companies listed on the London Stock Exchange in order to clarify requirements of the Combined Code and into which it has since been fully incorporated. In effect the Turnbull guidance is a high level guide to corporate risk management. As such it provides context for the project risk management process. Its content is an important source for the RMM stakeholders and risk management culture questions.

In parallel with the Project RMM, I also developed a Business Risk Maturity Model, drawing again from the Turnbull Guidance, together with other relevant standards and sources. The Business RMM can be used to assess the capability of a corporate risk

---

1   N. Turnbull et al. 1999. *Internal Control: Guidance for Directors on the Combined Code*, hereafter referred to as the Turnbull Guidance or the Turnbull Report.

management process used by a company or any other form of organisation. Whilst it shares a lot of common ground with the Project RMM, there are also a number of significant differences. It was useful to understand how, where and why this differentiation was important.

The other external sources for the Project RMM were provided by the project and risk management literature. Of the many books and papers used, two deserve particular mention. First, *Project Risk Management: Processes, Techniques and Insights* by Chris Chapman and Stephen Ward (1st edition 1997, 2nd edition 2003) is widely recognised as being a first-class academic text on the subject. It is also an antidote to approaches that treat risk management as being a procedure that is identical on every project. In practice, following a single recipe is all too common. In contrast, best practice requires the intelligent application of principles and the selection of techniques appropriate to the project in question. The second particularly influential book was the Association for Project Management's guide to *Project Risk Analysis and Management (PRAM) Guide*. The first edition of this guide was also issued in 1997. A key feature of the *PRAM Guide* process is the use of a top-down iterative approach. The importance of this is explained in more detail in several chapters of this book, most notably, Chapter 3.

When finally assembled, the prototype Project RMM was based on 39 questions. It was then calibrated using projects that HVR's risk management team members had been involved with. The key questions addressed by the calibration process were: 1) did the model produce a valid overall result and 2) did it identify the key weaknesses of the project risk management process in each case? Although the prototype frequently passed these tests, a number of adjustments had to be made to the wording of questions and the weightings assigned to them to increase its accuracy. Additional questions were also identified and incorporated into the model.

Amongst the projects used for calibration purposes was one that I had been involved with during the time with my previous company. My opinion was that the risk management process had been ineffective. Not only did the RMM confirm this, but it also now gave me new insight into why this had been so. Previously, my view had been that the team had failed to translate planned risk response into implemented action. Whilst the RMM confirmed that this had indeed been a problem, it suggested that risk identification and risk management culture had been the areas of greater weakness. On reflection, this was correct. In the environment of a project in difficulty, management politics had created barriers to the identification of significant and emerging risks. Actions to improve the risk management process would have had to address these barriers as a priority.

The fact that the Project RMM helped me to identify insights into my own previous project experience was encouraging. The model is not intended to be just a measuring tool. Identifying priorities for process improvement is a fundamental part of its purpose. As clients started to ask for the model to be used to assess their projects, it was encouraging to see that they were similarly pleased with the recommendations for process improvement that were identified. HVR staff also started to use the model for process self-assessment purposes when working on clients' projects.

Since 1999, the model has been continuously updated and improved. The main sources of information used to do this have been experience from the application of the model and advances in the project risk management literature. The current model is based on 50 questions. In the early days, the number of questions increased quite quickly as practice showed that increased differentiation was needed to cover certain issues.

However the number of questions has stabilised, with an increase of only one in the last five years.

The words used in the model have also evolved. Words are used to identify the scope of each question and to describe criteria to be met for alternative answers. This part of the model's content has to be written concisely, yet cover all reasonable possibilities. It also has to avoid being inappropriately prescriptive whilst, nevertheless, setting unambiguous criteria. Over the years, a number of people have been adept at identifying gaps or ambiguities that they can exploit to obtain higher scores. Closure of these loopholes is one of the key reasons for keeping the model's content under continuous review. However, since it has been now used for approximately 250 assessments, the model should have become reasonably robust.

Changes to the model have made high scores slightly more difficult to achieve. Despite having been questioned by some users for 'moving the goalposts', this is something for which I do not apologise. If the art of project risk management is progressing, then so should the Project RMM. Besides, continuous improvement is described as being part of achieving the highest capability levels in similar maturity models. Projects and organisations that stand still over a long period of time should thus not expect to retain the highest level of assessment. With each change, the model is recalibrated against previous project assessments to ensure that it has not become unfair.

Gradual evolution of the Project RMM can be expected to continue. Despite all the work to develop the model to date, it is, inevitably, imperfect. As with any interesting non-trivial subject, project risk management engenders passionate debate amongst the leading academics and practitioners. Disagreements between leaders in the field exist and provide important fuel for improvement. I have been in the fortunate position of being part of this process myself. However, as a result, I am also aware that concepts of what constitutes best practice continue to be contested and to evolve. With regards to the current version of the Project RMM, I have spent ten years updating the model on the basis of both practical experience with assessments and a close involvement in the development of professional standards.

In 2004, HVR was bought by QinetiQ, a leading UK-listed engineering technology and services company. QinetiQ and HVR have reputations for being at the cutting edge of development in their fields, and the ongoing development of the Project RMM has continued to be supported. The model has recently been incorporated into the AWARD toolset owned by QinetiQ and used for the purposes of tender assessment and project approval. It is also, of course, QinetiQ's support and commitment to continuous development that has made it possible to publish this book and its accompanying disc.

The primary purpose of this book is to explain to readers how the Risk Maturity Model should be used. Whilst anyone would be able to take out the disc and skip to 'Software User Instructions' (see pp. 235–41), readers are strongly advised to read other sections of the book before putting it to use! The parts of the book most directly relevant to its purpose are Chapters 1 'Project Risk Maturity Model', 5 'Risk Maturity Model Data Collection', and 6 'Stakeholders'. Chapter 6 and the following five chapters are designed to provide readers with insight into the purpose of each RMM Question and the reasons for its wording. The wording of each question is important, since it defines the criteria to be used for assessments. Thus, Chapters 6 to 11 are the ones to which anyone involved with RMM assessments is likely to refer most frequently.

Chapters 2 and 3 have been designed to provide useful background material for readers. Part of their purpose is to address a problem faced by all risk management practitioners: the lack of agreement on what constitutes best practice. Chapter 2 clarifies the position taken on a number of related issues by defining the model's scope and boundaries. It also identifies features of a risk management process that are important to what the model implicitly treats as being best practice, that is, a Level 4 risk management capability. For example, the chapter differentiates between the concept of overall project risk and the idea of managing risks on a risk-by-risk basis. Managing overall project risk (and its link with quantitative analysis) is a key concept for what is required to achieve RMM Level 4.

Two other major points identified by Chapter 2 are that a mature project risk management process requires risks to be understood broadly as being attributable to conditions of uncertainty (that is, lack of certainty) and that it should be based on a top-down iterative process in its early stages. These are important points that differentiate the model's concept of what is usually required for Level 4 capability from some forms of common practice.

In practice the idea of use of a top-down iterative approach to risk management process is often not well understood. Chapter 3 therefore provides a worked example to illustrate what this can involve. Since a number of the RMM questions refer to the principle of using a top-down process, readers who are less familiar with this should find that Chapter 3 provides useful context.

Chapter 4 is a case study which shows how the RMM has been systematically used for project assessments by a major organisation. This chapter provides evidence that the model works in practice and that its use is likely to improve the performance of projects. It also includes discussion of issues that should be addressed by anyone who is responsible for rolling out an assessment programme of this nature.

Where appropriate, examples have been used to illustrate the points made by the book. There are approximately 45 examples, each describing the circumstances of a different project organisation. Most are derived from real life. However, for reasons that include ease of explanation and the protection of confidentiality, some examples are fictional. Whilst they are fictional, they are nevertheless based on lessons learned from real life. For clarity, fictional examples are described by this book in the present tense, whereas examples derived more directly from real life are described in the past tense.

Inevitably with a work of this nature, there are many people who I would like to thank. The first person on my list has to be David Hillson, both for writing the foreword for this book and for originating the Risk Maturity Model principles. He has also been responsible for a number of other ideas that have influenced this book including his work on opportunity management and risk descriptions.

The most prominent academic sources of inspiration for this book are Chris Chapman and Stephen Ward. You will find their ideas referenced in various places. I have been fortunate enough to have worked with both of them on risk management guides published by the Association for Project Management (APM). In addition, Chris Chapman kindly reviewed Chapter 3, which has a similar narrative structure to the ten tales in the second of his books co-authored with Stephen Ward.

Working on APM risk management guides has given me invaluable contacts with a range of other project risk management professionals including practitioners, consultants, risk tool developers and academics. In particular, I had the pleasure of leading the group

Contents

List of Figures

List of Tables

Introduction to the Project Risk Maturity Model

1 The Project Risk Maturity Model

A Risk Maturity Model (RMM) is a tool designed to assess risk management capability. The Project RMM software provided with this book will allow its user to assess the capability of the risk management process being applied on any project. It will also allow capability improvements to be assessed and for the capabilities of different projects to be compared. However, assessing risk management capability is not a simple task. Obtaining reliable results requires an assessor (or auditor) who has insight into the subtleties of project risk management; what is best practice for one project might be inappropriate to another.

This book has been written to describe the issues facing anyone tasked with assessing project risk management capability. Whilst it is possible for any owner of the Project RMM software to load it onto their computer and start their assessment process forthwith, following the guidance in this book should provide them and their organisation with a sounder basis for believing the results.

By way of introduction, the rest of this chapter describes how the Project RMM has been constructed and how its results should be interpreted. Subsequent chapters then describe the issues that assessors should understand before putting the RMM into action or making recommendations for process improvement. The section 'Software User Instructions' at the end of the book (pp. 235–42), provides user instructions for how the Project RMM software should be installed and used.

The Project Risk Maturity Model (RMM)

The Project RMM was first developed by HVR Consulting Services in 1999. Its four-level capability structure, illustrated in Figure 1.1 is derived directly from the structure developed by David Hillson (1997) who used it to establish a generic Risk Maturity Model framework. The matrix for assessments identified by Hillson's paper published in the *International Journal of Project and Business Risk Management* has been reproduced in Appendix A.

In order to adapt the Hillson Risk Maturity Model for project-specific purposes, the following additional sources were used:

* Standard risk management guides, most notably the *Project Risk Analysis and Management (PRAM) Guide* (1997) published by the Association for Project Management (APM).
* The project risk management literature published in academic journals and books.
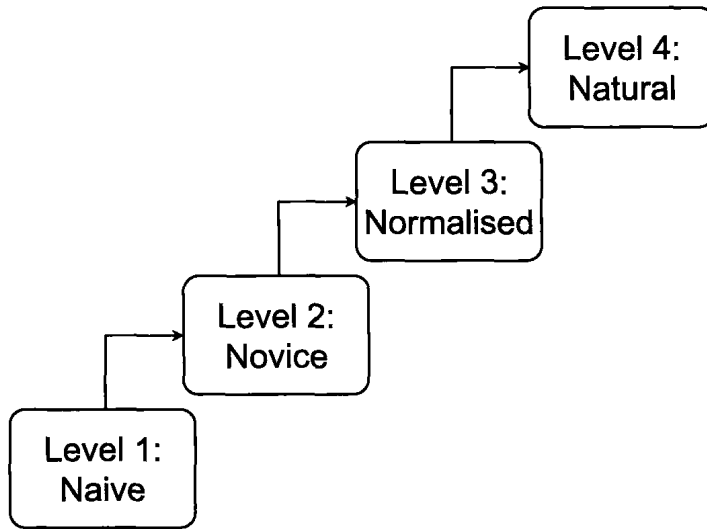
Figure 1.1   Risk maturity model levels

- The Turnbull Guidance[1] (1999) – *Internal Control: Guidance for Directors on the Combined Code.*
- The experience, dating back to 1987, of risk management consultants working for HVR Consultancy Services.

Since its creation the Project RMM has continued to evolve in response to lessons learned from its application. To date, it has been used for approximately 250 assessments on projects with an estimated combined value in excess of £60 Billion. Changes have also been made in response to new literature on the subject. Later chapters in this book identify the sources that have been the most influential. The software on the CD ROM included with this book is the latest version (version no. 6.0.0) of the model, updated in 2010.

The definitions of each level of project risk management capability are:

LEVEL 1 – NAÏVE

Although a project risk management process may have been initiated, its design or application is fundamentally flawed. At this level, it is likely that the process does not add value.

LEVEL 2 – NOVICE

The project risk management process influences decisions taken by the project team in a way that is likely to lead to improvements in project performance as measured against

---

1   N. Turnbull et al., *Internal Control: Guidance for Directors on the Combined Code,* hereafter referred to as the Turnbull Guidance or the Turnbull Report.

its objectives. However, although the process may add value, weaknesses with either the process design or its implementation result in significant benefits being unrealised.

LEVEL 3 – NORMALISED

The project risk management process is formalised and implemented systematically. Value is added by implementing effective management responses to significant sources of uncertainty that could affect the achievement of project objectives.

LEVEL 4 – NATURAL

The risk management process leads to the selection of risk-efficient strategic choices when setting project objectives and choosing between options for project solutions or delivery. Sources of uncertainty that could affect the achievement of project objectives are managed systematically within the context of a team culture conducive to optimising project outcomes.

Advancing through Project RMM Maturity Levels

RMM Level 1 could describe a project that is not implementing any process for managing risk. This would include projects that claim to be implicitly managing risk by virtue of the effectiveness of other project management processes such as planning (thus ignoring the fact that deterministic project management processes such as planning are not designed to manage the implications of uncertainty). However, since it would be unusual for projects to undergo RMM assessments when they have no formal risk management process, the more common cause of RMM Level 1 assessment results is a fundamental flaw with the design or application of the process. In practice, most problems at this level amount to failures of application. Whilst a risk management process might have been initiated, allowing any of its critical components to lapse into disuse will result in the overall process adding no value, hence producing a Level 1 assessment.

Once a project has taken professional advice or followed standard guidance to initiate its process, moving to a Level 2 RMM capability should be a relatively easy target to achieve. Level 2 does not set a particularly demanding standard. In effect, it requires that the value added by applying the risk management process should be greater than the cost and other resource implications of its application. Thus, even a relatively light application of the process can be sufficient to achieve this level.

The step-change difference between Level 2 and Level 3 RMM capability is mainly attributable to two factors: the discipline of implementing the process consistently across the whole project and the quality with which key skills are applied in practice.

A project will be able to achieve RMM Level 3 with the simple common-practice approach of using a risk register to underpin routine reviews of the implications of risks and the effectiveness and implementation of the responses designed to manage them. Although this is a simple process, there are a number of important skills involved in exploiting its potential to the full. For example, risks must be understood in a way that clarifies all relevant and significant sources of uncertainty. Failure to do this will impair the effectiveness of risk responses. Similarly, there are key skills involved in making sure