BENCHMARKING RISK MANAGEMENT CAPABILITY

© Dr David Hillson FAPM APMP MIRM MIMgt
Manager of Consultancy,
Project Management Professional Services Limited
7 Amersham Hill, High Wycombe, Bucks HP13 6NS, UK

ABSTRACT

The value of proactive risk management is hard to deny, and many organisations are working hard to implement risk processes across all aspects of their business. But how can they tell how well they are doing? What frameworks exist to enable them to assess risk management capability objectively?

In order to develop effective risk management, organisations need to be able to measure their current capability, define realistic and achievable targets for improvement, and design action plans to bridge the gap.

Benchmarking offers the opportunity to determine current capability against agreed frameworks, and also provides a structured route to improvement. A number of such frameworks have been developed recently, covering various aspects of risk management. Some measure the inherent risk in the business. Others address the maturity of organisational risk management capability, while a third group look at personal management of risk.

This paper considers risk benchmarking models covering these three areas, all of which are in the public domain, and explores how such frameworks might be useful in developing improved risk management capability.

INTRODUCTION

Successful projects deal effectively with risk, maximising benefits while minimising uncertainty. Guidelines and standards are being produced to define best practice, and organisations wishing to develop or improve in-house risk management processes can look to a number of sources for assistance. Risk management within projects has developed in recent years into an accepted discipline, with its own language, techniques and tools. Most textbooks in project management now include sections on risk management, and there is a growing library of reference texts specifically devoted to the subject in its own right. The value of a proactive formal structured approach to managing uncertainty has been widely recognised, and many organisations are seeking to introduce risk processes in order to gain the promised benefits.

There is currently broad consensus on the fundamentals of project risk management, with a mature and agreed process, supported by a comprehensive infrastructure. The core elements of project risk management are in place, and many organisations are reaping the benefits of implementing risk processes within their projects and wider business. There are however a number of areas where risk management needs to develop in order to build on the foundation which currently exists (see references

1 and 2 for a discussion of possible areas for development). One of the most important of these is the ability to measure effectiveness in managing risk.

Organisations need to know where they stand in relation to competitors and best practice, to enable them to maximise their competitive advantage and stay ahead, exploiting current developments in risk management as they arise. But how can an organisation know whether its risk processes are adequate? What measures exist to enable a business to compare its management of risk with best practice or against its competitors? Is there an accepted benchmark for organisational risk capability? 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.

A number of models have been developed in recent years to meet these needs, ranging from a simple "risk calculator" through to a fully developed "maturity model". These approaches allow an organisation to assess its current risk processes against agreed criteria, set realistic targets for improvement, produce action plans for developing or enhancing risk capability, and measure progress towards improvement targets. Other approaches permit benchmarking of personal approach to risk, exposing risk attitude and enabling risk-balanced teams to be built.

This paper outlines the structure of several models for benchmarking organisational and personal risk management capability, and shows how they can be used to develop best practice risk management processes. Three types of benchmarking framework can be distinguished, which aim to :

- measure inherent risk in the business
- address the maturity of organisational risk management capability
- consider personal management of risk

Representative models from each category are discussed in the following sections, illustrating the benefits that can be gained from attempting to measure organisational and personal risk management capability.

INHERENT RISK

It is clear that the effectiveness of risk management within an organisation will be directly related to the degree of risk exposure faced by the business. Some organisations have attempted to develop screening tools to determine the riskiness associated with particular ventures or projects, using criteria such as project size, complexity, value, novelty, constraints etc. Such tools however tend to be based on known sources of risk which have occurred previously in the history of the organisation, and focus on these to the exclusion of novel areas. An alternative to this can be found in proprietary models which have been developed by some consultancy companies, offering standardised diagnostic tests for risk exposure. The weakness of these proprietary approaches arises from their generic nature, attempting to force all situations into a single framework.

One benchmarking model for measuring inherent risk which has been positively received is that developed by Simons[3], known as the "Risk Exposure Calculator". This

assesses internal pressures within an organisation which give rise to increased risk, identifying "pressure points" within three areas :

- growth
- culture
- information management

The "Risk Exposure Calculator" subdivides each of these three areas into three further specific issues which can generate risk to an organisation, as follows :

- *growth* pressure points :
  - pressures for performance
  - rate of expansion
  - inexperience of key employees
- *culture* pressure points :
  - rewards for entrepreneurial risk-taking
  - executive resistance to bad news
  - level of internal competition
- *information management* pressure points :
  - transaction complexity and velocity
  - gaps in diagnostic performance measures
  - degree of decentralised decision-making

The description of the model[3] details each of these nine criteria, and rates each on a scale of 1 to 5. Scores are totalled within each pressure area (growth/culture/information management), and a grand total is produced. The overall figure places the organisation into one of three zones :

- The *safety zone* : Organisations in this zone are "probably safe from unexpected errors or events that could threaten the health of the business". However, recognising that not all risk is bad, Simons suggests that companies in the safety zone should question whether their risk exposure score is too low, and challenges them to consider taking some calculated gambles.
- The *caution zone* : Simons expects most companies to fall in this middle zone, which may indicate insufficient granularity in the model. However he suggests that the detailed scores should be examined to see whether there are any "hot-spots" of risk exposure, i.e. high scores in one or two of the three risk dimensions, to indicate areas of possible concern.
- The *danger zone* : Here Simons says that "alarm bells should be ringing and fast action should follow". The degree of risk faced by the company is probably unacceptable and unsafe, and he recommends using "whatever means are available to protect your business from disaster".

The approach embodied in the "Risk Exposure Calculator" is simple and easy to apply. It diagnoses risk exposure in several key areas and permits an organisation to evaluate the challenges faced in their business, which risk management needs to address. Use of this framework (or any other model of inherent risk in the business) will not reduce risk, but it will indicate areas of particular exposure, and allow management to focus their efforts on the areas most at risk.

ORGANISATIONAL RISK MANAGEMENT CAPABILITY

An increasing number of organisations wish to reap the benefits of proactive management of uncertainty in their projects by developing or improving in-house project risk management processes. It is however important for the organisation to be able to determine whether its risk processes are adequate, using agreed measures to compare its management of risk with best practice or against its competitors.

One framework which has been successfully used in the UK is the *Risk Maturity Model* (RMM)[4,5], which was developed as a benchmark for organisational risk capability. This describes four increasing levels of maturity, summarised as follows :

- The *Naïve* risk organisation (RMM Level 1) 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.
- At RMM Level 2, the *Novice* risk organisation has begun to experiment with 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.
- The level to which most organisations aspire when setting targets for risk management capability is captured in RMM Level 3, the *Normalised* risk organisation. At this level, management of risk is built into routine business processes and risk management is implemented 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 fully achieved in all cases.
- Many organisations would probably be happy to remain at Level 3, but the RMM defines a further level of maturity, termed the *Natural* risk organisation (Level 4). Here the 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.

Each RMM level is characterised in terms of four attributes, namely *culture*, *process*, *experience* and *application*. These allow an organisation to assess its current risk processes against agreed criteria, set realistic targets for improvement, and measure progress towards enhanced risk capability.

Since its original publication[4], the RMM has been used by several major UK organisations to benchmark their risk processes, and there has been considerable interest in it as a means of assisting organisations to introduce effective project risk management. Other professional bodies are considering the development of benchmarks for risk management based on the principles of maturity models[6,7], and a number of consultancies are also producing their own frameworks. This seems likely to become an important area for future development, as organisations seek assurance that their approach to risk management is both effective and improving.

PERSONAL RISK MANAGEMENT CAPABILITY

Considerable work has been done in the area of heuristics[8], to identify the unconscious rules used when making judgements under conditions of uncertainty. There is however less insight into risk attitudes and their effect on the validity of the risk process[9]. If risk management is to retain any credibility, this aspect must be addressed and made a routine part of the risk process. A reliable means of measuring risk attitudes needs to be developed, which can be administered routinely as part of a risk assessment in order to identify potential bias among participants. Accepted norms for risk attitudes could be defined, allowing individuals to be assessed and placed on a spectrum of risk attitude, perhaps ranging from risk-averse through risk-neutral to risk-tolerant and risk-seeking. Once potential systematic bias has been identified it can then be countered, leading to more reliable results and safe conclusions. The impact of risk attitude on perception of uncertainty should be explored to allow the effects to be eliminated.

A further result of the inclusion of a formal assessment of behavioural characteristics in the risk process would be the ability to build risk-balanced teams. This would permit intelligent inclusion of people with a range of risk attitudes in order to meet the varying demands of a project environment. For example, it is clearly important for a project team to include people who are comfortable with taking risks, since projects are inherently concerned with uncertainty. It is however also important that these people are recognised and that their risk-taking tendency should be balanced by others who are more conservative and safety-conscious, in order to ensure that risks are only taken where appropriate.

Work is in progress in this area[10,11], but it is important that this should be fully integrated into mainstream project risk management, rather than remaining a specialist interest of psychologists and behavioural scientists. The standard risk process must take full account of all aspects of human behaviour if it is to command any respect and credibility.

One model which is simple to use and accurate in its results has been developed by Hillson based on work by Hall[12], who has defined a series of questions to reveal the underlying approach to decision-making under conditions of uncertainty. These diagnose the preferred approach(es) to risk when an individual is faced with having to make a decision when uncertain. Scores are calculated in three aspects of risk attitude, namely *risk-averse*, *risk-seeking* and *risk-neutral*. An individual may have a high score in just one area, showing their preferred way of handling uncertainty. Scoring high in two or even all three areas indicates a person with several styles of response available, who must choose the most appropriate. A low score in any area suggests a type of response with which the person is uncomfortable. Being aware of this may help to identify types of decision where input is required from another person, preferably someone with a different risk style.

The three basic risk attitudes diagnosed by this model are summarised below :

- *Risk-averse* : This indicates a conservative risk attitude with a preference for secure payoffs. People who are risk-averse make good middle managers, administrators and engineers. Key characteristics include being practical, accepting, and showing common sense. Risk-averse people enjoy facts more

than theories, and support established methods of working. They excel at activities which involve remembering, persevering and building.

- *Risk-seeking* : These show a preference for speculative payoffs, and make good entrepreneurs and negotiators. Risk-seeking people are adaptable and resourceful, enjoy life and are not afraid to take action. They are good at activities which require performing, acting and taking risks.
- *Risk-neutral* : This attitude prefers future payoffs. People who are risk-neutral make good executives, system architects and group leaders. They think abstractly and creatively and envisage the possibilities. They enjoy ideas and are not afraid of change or the unknown. Risk-neutral people are good at learning, imagining and inventing.

The importance of understanding risk attitude is clear, since people have such a profound effect on the effectiveness of any risk process. Use of models such as the one outlined above will assist in revealing underlying risk attitudes, enabling systemic bias to be exposed and corrected.

CONCLUSION

The short history of project risk management has been a success story to date, with widespread application across many industries, and development of a core best practice with a strong supporting infrastructure. Although project risk management has matured into a recognised discipline, it has not yet reached its peak and could still develop further[1,2]. In particular, organisations need to measure their progress in developing effective risk management, in terms of the challenge they face, and the capabilities they can deploy to meet that challenge, both organisational and personal.

Project risk management must not remain static if it is to fulfil its potential as a significant contributor to project and business success. Neither can organisations be content with their existing abilities to manage risk. Measuring their current position against accepted frameworks, and using the results to develop improvement plans, will ensure that organisations maximise the benefits of project risk management.

This paper has outlined several approaches to benchmarking risk management capability. Adoption of these techniques and application of the results will provide an understanding of current risk management capability within accepted frameworks, allowing definition of a structured path for progression towards enhanced maturity of risk management. We need to understand how much risk we face in our business and projects (through use of models of inherent risk). We also need to know how well equipped we are to handle risk (using models of organisational risk capability) and how individuals will react to the challenge of risk (measuring personal risk attitudes). Only when we are able to match the capability to the challenge can we be sure that risk management will be effective.

REFERENCES

1. Hillson D.A. (1998) "Project risk management : future developments", Int J Project & Business Risk Mgt, 2 (2), 181-196
2. Hillson D.A. (1999) "Risk management for the new millennium", Session 7.7.4, Proceedings of the Ninth Annual International Symposium of the International Council on Systems Engineering (INCOSE), 6-11 June 1999, pages 1291-1294
3. Simons R. (1999) "How risky is your business?", Harvard Business Review, May-June 1999, 85-94
4. Hillson D.A. (1997) "Towards a Risk Maturity Model", Int J Project & Business Risk Mgt, 1 (1), 35-45
5. "The Risk Maturity Model was a concept of, and was originally developed by, HVR Consulting Services Limited in 1997. All rights in the Risk Maturity Model belong to HVR Consulting Services Limited."
6. "Organisational Project Management Capability Maturity Model (OPM3)" project, PMI Standards Committee, Project Management Institute, 130 South State Road, Upper Darby, PA 19082, USA.
7. 11th Software Engineering Process Group Conference : SEPG99, Atlanta, 8-11 March 1999 (themes include risk capability maturity models)
8. Kahneman D., Slovic P. & Tversky A. (eds.) "Judgement under uncertainty : Heuristics and biases", CUP, Cambridge, 1982
9. Oldfield A. & Ocock M. (1997) "Managing project risks : the relevance of human factors", Int J Project & Business Risk Mgt, 1 (2), 99-109
10. Greenwood M. (1998), "Measuring risk behaviour : An introduction to the Risk Behaviour Profiler", Int J Project & Business Risk Mgt, 2 (3), 273-288
11. Research by L Millward and L Hopkins (personal communication, 1997), Centre for Employee Research, Guildford, Surrey, UK.
12. Hall, E.M. (1998) "Managing risk – Methods for software systems development", pub. Addison Wesley Longman Inc, 1998, ISBN 0-201-25592-8, pages 38-39.

AUTHOR'S BIOGRAPHY

Dr David Hillson is Manager of Consultancy with Project Management Professional Services Limited, based in Buckinghamshire (UK), with responsibility for all aspects of consultancy work. He has a particular interest in risk management consultancy and training. His speciality is risk technology transfer, assisting organisations to develop in-house risk processes, and he is a regular conference speaker on risk.

David is a Fellow of the UK Association for Project Management (APM), and is co-editor of the APM's "*Project Risk Analysis & Management (PRAM) Guide*". He is immediate past Chairman of the APM Risk Management SIG. He is also an active member of the Project Management Institute (PMI) and was part of the team rewriting the risk chapter of the PMBoK®. David is an elected member of the UK Institute of Risk Management, and the Institute of Management, and contributes to the Risk Management Working Group of the International Council on Systems Engineering (INCOSE).