Management of Risk: Guidance for Practitioners
By Office of Government Commerce (OGC), UK, © 2007
(A book review by R. Max Wideman)

Introduction

Management of Risk (MoR)*: Guidance for Practitioners* is a new guide by the Office of Government Commerce (OGC), UK, the same people who publish *PRINCE2* with which many readers will be familiar. By way of introduction, the Foreword tells us:

> "All of us manage risks in our daily lives almost unconsciously – assessing the speed of traffic when crossing the road, taking out insurance policies, making everyday decisions, weighing up options. However, in business, risk and risk management can sometimes be seen as specialist subjects, requiring expertise outside 'normal' management experience. In other circumstances, risk can be ignored altogether or the view taken that risk can be avoided by maintaining the status quo. Spending time developing risk management strategies is sometimes perceived as mere pointless bureaucracy. In this rapidly changing world, a status quo is unrealistic, and failure to identify and explore new opportunities is a risk in itself.
> . . .
> This guide provides an accessible framework for taking informed decisions on managing risk throughout the organization, from designing policy and strategy to dealing with threats and opportunities in your day-to-day operations and services."[1]

So, at first glance, both from the title and the Foreword, one might think that this publication is not relevant to project management on this web site. Indeed, in the Table of Contents, only the final chapter even mentions programs and projects. However, throughout the text, as well as risks to the Line of Business operations, the authoring team clearly had "projects" very much in mind whether at the project, program or portfolio levels.

For example, "Risk" itself is defined as "An uncertain event or set of events that, should they occur, will have an effect on the achievements of objectives."[2] That sounds to us very much like a project. In many places the content follows traditional project risk management philosophy, including such risk tools as Issue Log,[3] Risk Register,[4] and reference to the project life cycle.[5] Even "stakeholder" is defined as: "Any individual, group or organization that can affect, be affected by, or perceived to be affected by, an initiative (program, project, activity or risk)."[6]

So, in fact this text is a solid "How-to" treatise on managing risks associated with an organization's initiatives (aka projects). And as such, taking into account the perspective from which it is written, it might well have been better titled as "Management of ***Project Portfolio*** Risk". Either way, we believe that this book is one of the first of its kind, and something that we have been looking for. For those who might want to draw a comparison with the Project Management Institute's ("PMI") publications, remember that this *Management of Risk: Guidance for Practitioners* is a "How-to", whereas PMI essentially publishes standards, i.e. "What-is".

The MoR framework is based on four core concepts namely: Principles; Approach; Processes; and Embedding & Reviewing. These are shown arranged diagrammatically in Figure 1.

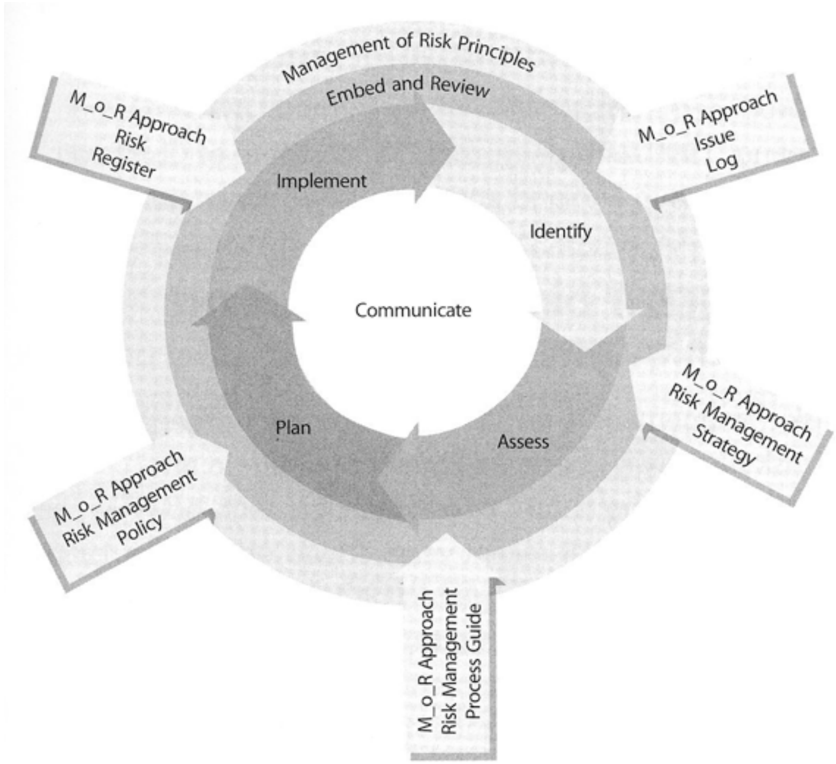

Figure 1: The MoR framework[7]

Thus, according to the MoR guide:

> "It provides a route map for risk management, bringing together principles, an approach, a set of inter-related processes and pointers to more detailed sources of advice on risk management techniques and specialisms. It also provides advice on how these principles, approach and processes should be embedded, reviewed and applied differently depending on the nature of the objectives at risk."[8]

As an interesting footnote, but completely true to form, the authoring team treated the very production of this MoR document as a project – complete with a quality assurance and change control panel.[9]

Book Structure

As you might expect from the foregoing, the Management of Risk guide has just six chapters. However, six appendices and a glossary provide considerable amplification of the chapter content altogether as follows:

1. Introduction
2. Management of risk principles
3. Management of risk approach
4. Management of risk process
5. Embedding and reviewing management of risk
6. Perspectives

Followed by:

Appendix A: Provides 10 risk document outlines and describes their purpose and content
Appendix B: Describes 50 risk management techniques, including several less well known

Appendix C: Introduces a health check tool to identify areas that might be improved
Appendix D: Provides a five-level maturity model and compares it to other established models
Appendix E: Introduces some management of risk specializations
Appendix F: Provides considerations in selecting risk management software tools
Further information: Gives a list of references

Chapter 1 introduces some key terminology, always a good idea, and explains what risk management is; why it is important to organizations; and where and when it should be applied. It also provides an introduction to the subjects of corporate governance and internal control. Chapter 2 introduces eleven management-of-risk principles intended to be high-level, universally applicable guidelines for aiding and influencing risk management practices.

These principles include such items as Stakeholder Involvement; Roles and Responsibilities; and Supportive Culture. These are wrapped around by a twelfth principle of Continual Improvement. Each of these principles are described, followed by a listing of Supporting Factors. According to the guide, these principles are derived from corporate governance and recognize that risk management is a subset of an organization's internal controls. If that is true, then it may be presumed that project management is likewise a subset of corporate development management.

Chapter 3 presents the management of risk approach, which consists of the Risk Management Policy, Process Guide, Strategy and Risk Register. It explains the main risk management concepts that need to be considered in establishing these documents. Interestingly, it also includes different ways of looking at probability and impact that should help to shed light on how to interpret these variables in practical project environments. Chapter 4 describes the main steps of the management of risk process. It contains practical pointers for identifying, assessing, and controlling risks.

Chapter 5 describes and provides guidance on how an organization can introduce and embed risk management, and then measure the success and maturity of its risk management. We have some difficulty with this chapter because we don't believe that "maturity" is an end in itself and that therefore the success of risk management, of any kind, should not be measured on this metric. But we'll get to that later. Chapter 6 explains when and how management of risk principles, concepts and processes should be applied throughout the organization, from the strategic, program, project and operational perspectives.

What we liked

The Management of Risk guide defines Risk Management as:

> "The systematic application of principles, approach and processes to the tasks of identifying and assessing risks, and then planning and implementing risk responses."[10]

If that sounds familiar, it is. The only thing missing is the word "Project".

The MoR states that:

> "Risk management should be most rigorously applied where critical decisions are being made. Decisions about risk will vary depending on whether the risk relates to long-, medium- or short-term goals."[11]

MoR illustrates these term views as shown in Figure 2. We particularly like this figure because it illustrates that each of these perspectives relates to one of the three major management components of any organization that are:

1. Senior executives responsible for corporate governance of the entire organization taking the long-term view
2. Program/project management responsible for delivery on new initiatives and taking the mid-term new product delivery view, and
3. Operations Line of Business responsible for generating the benefits from the available products.

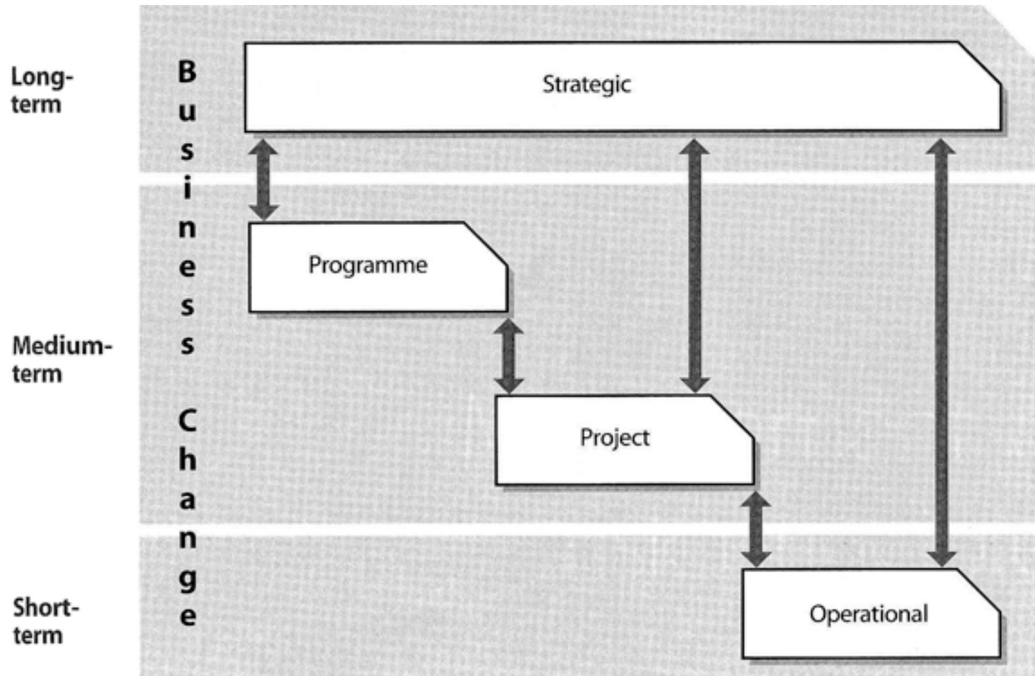

Figure 2: Organizational perspectives[12]

Chapter 4, Management of risk process, adopts the now well-established input-process-output model but with some elaboration as shown in the generic Figure 3.

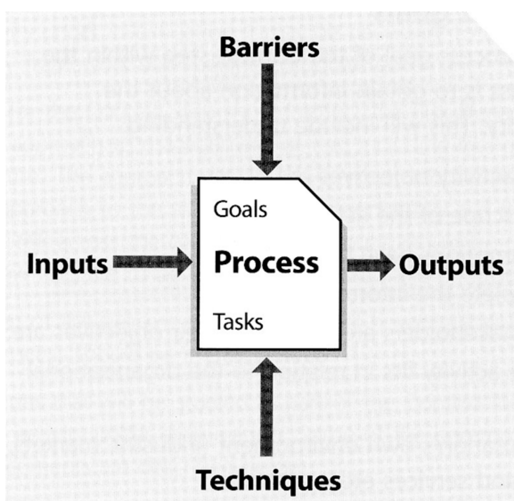

Figure 3: Generic process elements – inputs, outputs, barriers and techniques[13]

As an example, this model is used to illustrate the stage of risk identification as shown in Figure 4.

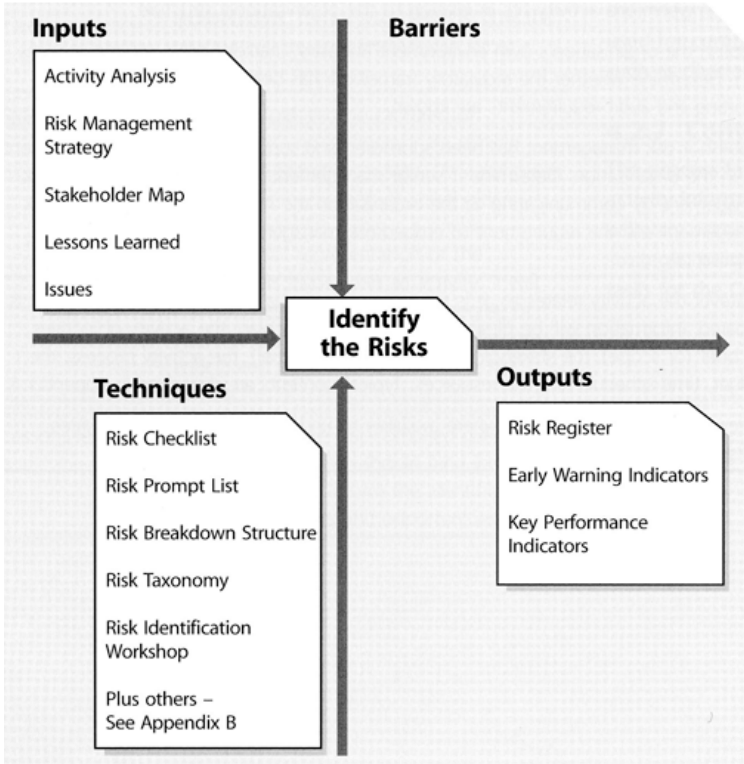

Figure 4: Risk identification process definition and information flows[14]

By way of comparison, compare this to the Project Management Institute's model shown in Figure 5.

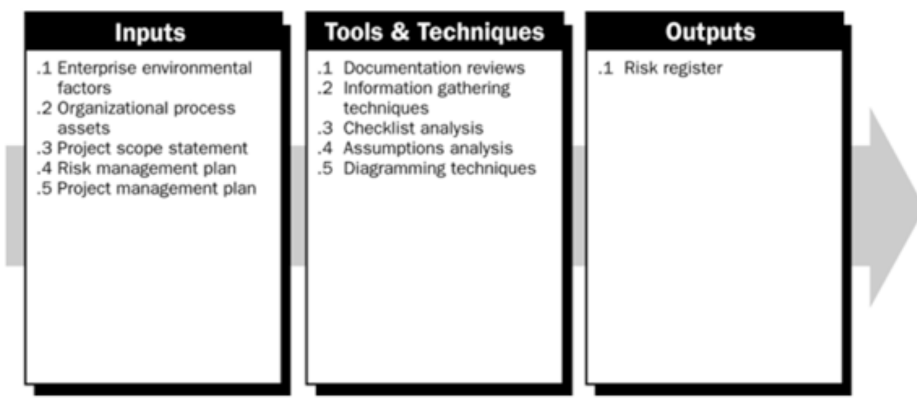

Figure 5: Risk identification – inputs, tools & techniques, and outputs[15]

Why is risk management important? According to the authors, because:

> "A certain amount of risk taking is inevitable if an organization is to achieve its objectives . . . Taking and managing risk is the very essence of business growth.[16]

The authors cautiously suggest that effective risk management is likely to improve performance against objectives by contributing to such things as:

- Better service delivery
- More focus internally on doing the right things properly
- Fewer sudden shocks
- Reduced waste and fraud
- Better management of contingent and maintenance activities, and so on

The authors also point out that:

> "Many of these benefits are applicable to both the private and public sectors. Whereas corporations focus mainly on shareholder returns and the preservation of shareholder value, the public sector's role is to implement programs cost-effectively, in accordance with government legislation and polices to achieve value for money."[17]

Oh, how we wish that our politicians understood that just as well!

In fact the authors recount that:

> "In the private sector change has been instigated in the UK, across Europe and within the US by new regulatory environments driven for instance by the:
> - Combined Code on Corporate Governance 2006 (UK)
> - Basel II Accord 2004 (Bank of International Settlements, Switzerland)
> - Sarbenese-Oxley 2002 (Public Company Accounting Reform and Investor Protection Act, US)"[18]

In our humble view, given the current chaotic financial environment (mid-2008), the US Sarbenese-Oxley act as one example has done little to avert the severest risk of all – the financial collapse of major investment banking institutions. While the regulators were busy harassing high profile business people, the boys in the sub-prime mortgage trenches were busy whooping it up using highly questionable corporate-endorsed marketing practices.

A legitimate question, therefore, is whether or not a strong dose of "Management of Risk" would have averted much of the turmoil and the collapse of major long-standing institutions that should have known better? Obviously, risk management is a hard sell to both public and private corporations. However, one cannot help but think that a stronger dose of plain economics might not have been more appropriate.

Downside

Chapter 5 discusses embedding and reviewing management of risk and observes that:

> "When an organization implements or develops its risk management capability, the organization should measure this development, the benefits it brings to the organization, and therefore its success"[19]

Very true indeed! However, the authors have not exactly defined what they mean by the term "success".

Rather, they suggest a number of "Success Factors" that are introduced by this caveat:

> "There are a number of essential elements to identify when measuring success, which will probably be different for each organization.
> . . .
> Rather than discuss general success factors in detail, each organization should identify specific success factors for themselves at the outset of the management of risk program and define these measurable benefits that can then be monitored and managed as part of the benefits management activities within a program management practice (see the MSP publication)."[20]

[Please pause for breath! MSP, by the way stands for *Managing Successful Programmes*, a companion OGC document.]

But then follows a long list of high-level success factors that includes such typical items as:[21]

- Visible sponsorship, endorsement and support from senior management

- Regular communication on risk management within the organization
- Inclusion of risk management and a review of key risks on the board agenda
- An appointed board member responsible for risk management
- A clearly defined risk management process
- Inclusion of risk management responsibilities in job descriptions and personal objectives
- Benchmarking of risk management awareness

To us, this looks like a valuable list of activities to institute the management of risk in an organization, but activity and documentation is not an end in itself. In our view, the measure of real success is in the real benefits that the risk management program brings to the organization. The issue is payoff, contribution to the bottom line, whether shareholder value, cost effectiveness, or value for money. The last thing any organization wants is a gravy train for increased bureaucracy.

Summary

Chapter 6 returns to a discussion of the four management perspectives as displayed in Figure 6. We think this chart neatly summarizes the purpose of this guide – the application of management of risk from strategic, program, project and operational viewpoints and the consequent interactions.

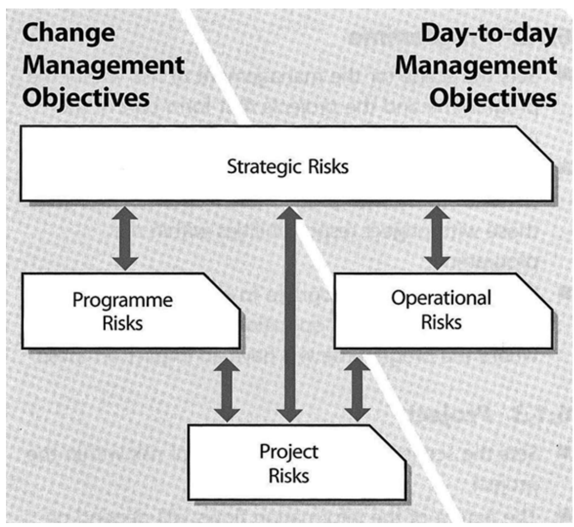

Figure 6: Inter-relationships between different organizational perspectives[22]

The ***strategic perspective*** is concerned with ensuring overall business strategy, vitality and viability and sets the scene for the management of risk across the entire organization. The ***program management perspective*** is concerned with transforming business strategy into new ways of working that represent significant changes that deliver measurable benefits to the organization. It sets the scene for the management of risk within the program and the projects that form part of the program.

The ***project perspective*** is concerned with delivering predefined outputs to an appropriate level of quality, and with potential benefits, within an agreed time, cost and scope constraints. It sets the scene for the management of risk within the project. The ***operational perspective*** maintains a view of the people, processes, and technologies that support ongoing business-as-usual or business service delivery activities of the organization. It is concerned with maintaining appropriate levels of services to existing and new customers and sets the scene for the management of risk within particular operational (service delivery) areas. These are all in relation to customer expectations whether those customers are internal to the organization (e.g. the human resources department), or external.[23]

What ever else, *Management of Risk: Guidance for Practitioners* provides a valuable source of practical information in the application of program and project risk management. It also provides insight into the much broader perspective of the whole organization for all those at whatever level in the hierarchy that, one way or another, are involved with projects.

R. Max Wideman
Fellow, PMI

---

[1] *Management of Risk: Guidance for Practitioners,* Office of Government Commerce (OGC), UK, 2007, p vii
[2] Ibid, p156
[3] Ibid, pp1, 155
[4] Ibid, 30-32, 157
[5] Ibid, p91
[6] Ibid, p158
[7] Ibid, Figure 1.1 on p1
[8] Ibid.
[9] Ibid, p viii
[10] Ibid, p1
[11] Ibid, p5
[12] Ibid, Figure 1.3 on p5
[13] Ibid, Figure 4.3, p37
[14] Ibid, Figure 4.5, p42
[15] A Guide to the Project Management Body of Knowledge, Third Edition, Project Management Institute, Figure 11-6, p246.
[16] *Management of Risk: Guidance for Practitioners,* Office of Government Commerce (OGC), UK, 2007, p2
[17] Ibid.
[18] Ibid, p3
[19] Ibid, p58
[20] Ibid, p59
[21] Ibid.
[22] Ibid, Figure 6.1, p66
[23] Ibid, p65-79