How to manage the risks you didn't know you were taking

Dr David Hillson, **PMI Fellow, PMP, HonFAPM, FRSA, FIRM, FCMI, CMgr, MIOD**

The Risk Doctor Partnership, david@risk-doctor.com

Abstract

When most people talk about risk in projects, they are thinking only about uncertain future events that would have a negative effect on achievement of project time and cost objectives. However the definition of risk in the risk chapter of *A Guide to the Project Management Body of Knowledge* (Project Management Institute, 2013) includes much more than mere threats to the project schedule or budget, and other risk standards agree. If we limit our view of risk to look at only one part of the risk picture, we will not be proactively managing all the risks that might affect the success of our project, and we will end up taking risks without knowing it.

This paper explores the other types of risk that are usually missed from the typical risk process. Drawing on leading thinking and current best practice, we explore the full range of project risks that need to be managed, starting from the proto-definition of risk as "*uncertainty that matters*" (Hillson, 2003, 2009).

Risks that *matter* include those with positive effects as well as those with negative effects (opportunities as well as threats). They can also affect any project objective, not just time or cost.

In addition, *uncertainty* in projects arises from much more than future uncertain events ("stochastic risks"). Other sources of uncertainty include variability ("aleatoric risk"), ambiguity ("epistemic risk"), and emergence ("ontological risk").

With illustrative examples of each type of risk, and practical response strategies for managing them, this paper helps us to identify all types of risk that might affect our projects, and offers ways for us to tackle them effectively.

The problem with the typical project risk management approach

It is widely accepted that effective management of risk is a key contributor to project success. All projects plan to succeed and meet all their objectives. However, when the project is underway, other things arise that were not expected and not included in the project plan. These factors have the potential to affect the project in a variety of ways, and if they are left unmanaged they could jeopardise the chances of project success. If we were able to scan the future and identify these factors in advance, then for some of them at least, we should be able to pre-plan, prepare and position ourselves to be ready if they were actually to occur. In many cases we can take effective action in the present which will influence whether these factors occur at all, or to change their potential impact on the project. Such proactive identification, assessment and action in relation to potential factors that might affect us is called **risk management**. Unmanaged risk results in project failure. The more effectively we can scan the future to identify and manage risks proactively, the better chance we have of succeeding in meeting our project objectives.

This is why project management standards such as *A Guide to the Project Management Body of Knowledge* (PMBoK® Guide) (Project Management Institute, 2013) include risk management as a core competence for project management professionals.

Unfortunately, despite the effort and attention given to managing risk in projects, it is still commonplace for projects to fail to meet all their objectives in full. One reason for this must be a failure to address all risks, since unexpected and unplanned factors are still occurring that drive the project off course. This in turn is caused by severe limitations in the way risk is understood. A narrow view of the meaning of risk inevitably produces ineffective management of risk.

What is risk? First principles

A simple starting point for understanding the nature of risk is the proto-definition "*Risk is uncertainty that matters*" (Hillson, 2003, 2009). While this is not a formal definition of risk, it is sufficiently robust to provide important insights that can shape our understanding of what risk really means.

Originally published as a part of the 2014 PMI Global Congress Proceedings – Phoenix, Arizona, USA

The view of risk as "uncertainty that matters" has been adopted by many standards bodies as a starting point for developing a more detailed risk definition, as illustrated in Exhibit 1.

SOURCE OF DEFINITION	"UNCERTAINTY…"	"…THAT MATTERS"
A Guide to the Project Management Body of Knowledge [PMBoK® Guide] (Project Management Institute, 2013)	"An uncertain event or condition…"	"…that, if it occurs, has a positive or negative effect on a project's objectives."
APM Body of Knowledge (Association for Project Management, 2012)	"An uncertain event or set of circumstances…"	"…that, should it or they occur, would have an effect on achievement of one or more project objectives."
Management of Risk [M_o_R]: Guidance for Practitioners (UK Office of Government Commerce, 2010)	"An uncertain event or set of events…"	"…that, should it occur, will have an effect on the achievement of objectives."
Risk Management – Principles and guidelines (ISO 31000:2009)	"Effect of uncertainty…"	"…on objectives."
Risk Analysis & Management for Projects [RAMP] (Institution of Civil Engineers et al, 2014)	"A possible occurrence…"	"…which could affect (positively or negatively) the achievement of the objectives for the investment."

Exhibit 1: Defining risk as "uncertainty that matters" (from Hillson, 2009)

This consensus among standards bodies should provide a firm foundation for project practitioners to implement effective risk management based on a sound agreed view of the nature of risk. Unfortunately when most project practitioners are asked to expand on their understanding of risk as "uncertainty that matters", they interpret "uncertainty" to mean "future events that may or may not occur", and "matters" means "would have a negative effect on project budget or schedule." This leads to a limited perspective that the only risks faced by projects are "*uncertain future events that, if they occurred, would have a negative effect on the project budget and/or schedule.*" Comparing this with the official definitions of risk in Exhibit 1 (see the PMI definition for example), the limitations are immediately obvious. The PMI definition says that project risk is:

- "*An uncertain event **or condition**…*" (i.e. not just uncertain events, but other types of uncertainty)
- "*…that, if it occurs, has a **positive or negative** effect…*" (i.e. not just negative effects)
- "*…on a project's **objectives***" (i.e. not just budget and/or schedule objectives)

This is important because **any uncertainty that matters** needs to be identified, assessed and managed, if we are to give our projects the best chance of succeeding.

The remainder of this paper outlines the other types of uncertainty that could affect projects, and the other ways in which they might matter, with examples and suggested responses.

Different types of "mattering"

Taking the proto-definition of risk as "*uncertainty that matters*", we can start by considering the question of how uncertainties might "*matter*". The typical perspective is that project risks are "*uncertain future events that, if they occurred, would have a negative effect on the project budget and/or schedule.*" This needs to be expanded to include other types of effect that uncertainty might have on our project objectives.

One obvious expansion of this limited perspective is to recognise that risk can affect other project objectives, not just time or cost. Risks that occur can have an impact on technical performance, human health and safety, regulatory compliance, customer satisfaction, corporate reputation, etc. Each of these project objectives is at risk, and we need to identify, prioritise and manage uncertainties that could affect them, as well as those that relate to project budget or schedule.

One tool that reminds project practitioners to consider all types of potential impact from risk is the Risk Impact Breakdown Structure, or RIBS (Hillson, 2007). RIBS is defined as "*An impact-oriented grouping of project risks that organises and defines the total risk exposure of the project. Each descending level represents an increasingly detailed definition of risk impacts on the project*" (Hillson, 2007). An example RIBS is shown in Exhibit 2, with four Level 1 impact types (Time, Cost, Scope/Quality, and Other Objectives). Each of these is

Originally published as a part of the 2014 PMI Global Congress Proceedings – Phoenix, Arizona, USA

decomposed into a number of Level 2 impact types. All projects will include Time, Cost and Scope/Quality at Level 1, since these represent the familiar "triple constraint". Further Level 1 RIBS elements should be added depending on the specific objectives of the project, such as Reputation, Regulatory Compliance, Business Benefits, Safety etc., and also depending on the level of detailed analysis required to support effective management of risk.

RIBS LEVEL 0	RIBS LEVEL 1	RIBS LEVEL 2
0. IMPACT ON PROJECT	1. TIME IMPACT	1.1 Project duration
		1.2 Phasing
		1.3 Interim milestones
		1.4 Float
		1.5 Delivery schedule
		1.6 Useful product life
		1.7 Obsolescence
	2. COST IMPACT	2.1 Profitability
		2.2 Margin
		2.3 Cashflow
		2.4 Resourcing
		2.5 NPV
		2.6 ROI
		2.7 Whole-life costs
		2.8 Cost of ownership
		2.9 Liquidated damages
		2.10 Contingency reserve
		2.11 Payback period
	3. SCOPE/QUALITY IMPACT	3.1 Performance
		3.2 Functionality
		3.3 Reliability
		3.4 Maintainability
		3.5 Expansion potential
		3.6 Security
	4. IMPACT ON OTHER OBJECTIVES	4.1 Safety
		4.2 Regulatory compliance
		4.3 Reputation
		4.4 Supply chain
		4.5 Business case
		4.6 …

Exhibit 2: Example Risk Impact Breakdown Structure (RIBS) (from Hillson, 2007)

Another important expansion of the typical view of the effects of risk is to consider risks with positive upside impacts, for example uncertainties that would produce cost or time savings, performance enhancements, safety improvements etc. (Hillson, 2003). This broad view of risk to encompass both threat (downside risk with negative impact) and opportunity (upside risk with positive impact) is widespread in risk standards (for example Project Management Institute, 2013; Association for Project Management, 2012; ISO 31000:2009). A particularly clear example is given by the PMI definition:

- An uncertain event or condition that, if it occurs, has a *positive or negative effect* on a project's objectives (Project Management Institute, 2013)

In summary, if risk is "*uncertainty that matters*", then "*mattering*" includes both *positive and negative* impacts (not just threats), and can affect *any project objective* (not just time and cost).

Different types of "uncertainty"

Having addressed the "*mattering*" side of the proto-definition of risk as "*uncertainty that matters*", we now turn to the "*uncertainty*" side. The limited common view of project risks as "*uncertain future events that, if they occurred, would have a negative effect on the project budget and/or schedule*" needs to be expanded beyond events to include other types of uncertainty that might affect project objectives.

Originally published as a part of the 2014 PMI Global Congress Proceedings – Phoenix, Arizona, USA

The need for this broader understanding of uncertainty is covered clearly in risk standards, including the PMBoK Guide (risk is "an uncertain event *or condition*…", Project Management Institute, 2013) and the APM Body of Knowledge (risk is "an uncertain event *or set of circumstances*…, Association for Project Management, 2012). The international risk standard ISO 31000:2009 also states in Principle 4 that "Risk management explicitly addresses *all uncertainty*". What is meant by these references to non-event types of uncertainty?

It is possible to define four types of uncertainty, each of which could affect a project's ability to achieve its objectives, but only one of which is about future uncertain events. In summary, these four types are as follows:

1. Event risk
2. Variability risk
3. Ambiguity risk
4. Emergent risk

Event risk

The first type of risks are **future possible events**, which are sometimes called "stochastic uncertainty" or "event risk". An event risk is something that has not yet happened and it may not happen at all, but if it does happen then it has an impact on one or more objectives. Most risks identified in the typical Project Risk Register are event risks. Examples of event-based threats and opportunities include:

- A key supplier may go out of business during the project
- The client might change the requirement after design is complete
- New regulatory constraints might be imposed
- We may lose a key resource at a critical time in the project
- The client may allow incremental deliveries
- A subcontractor may propose enhancements to our standard operating processes

These types of event risk are addressed in the typical project risk process, with well-established techniques for identifying, assessing and managing them. Event risks can also be represented explicitly in quantitative risk analysis models using stochastic branches (Hillson, 2003; Hillson & Simon, 2012), as shown in Exhibit 3.

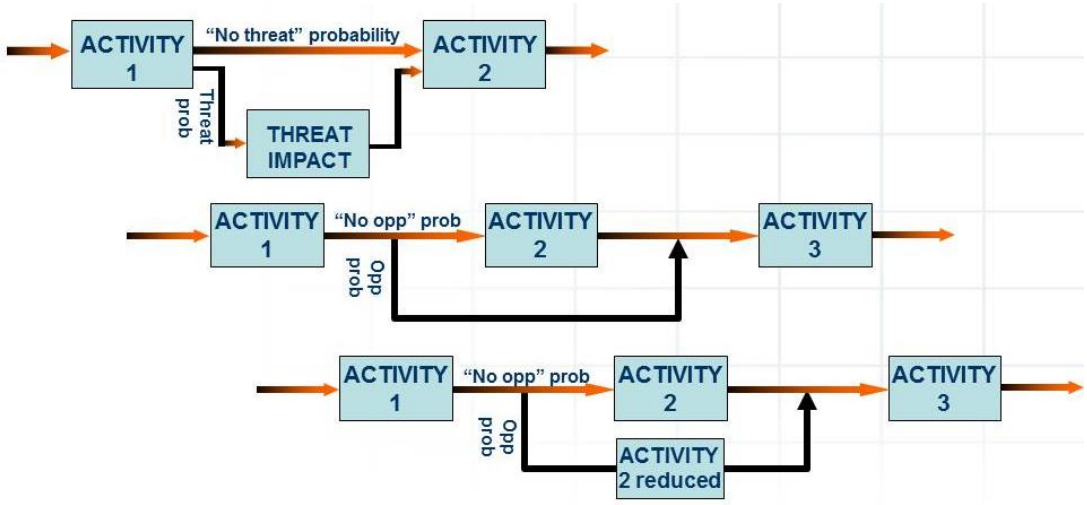

Exhibit 3: Stochastic branches to model threat and opportunity event risks (from Hillson, 2003)

Variability risk

Secondly, some risks arise from **variability** (also called "aleatoric uncertainty"), where some aspect of a planned task or situation is uncertain. The name is taken from the Latin word *alea*, which is a game of chance with dice where there are a set number of possible outcomes but we don't know which one will actually occur. A common example from the project arena is the situation where we plan to run a 15-day trial, but the actual duration could in fact be anywhere between 10-25 days. The probability of running the trial is 100%, but its duration is uncertain. Other variable parameters include cost, resource requirement, productivity, defect rate, performance, etc. Example variability risks include:

Originally published as a part of the 2014 PMI Global Congress Proceedings – Phoenix, Arizona, USA

- Productivity may be above or below target
- The number of errors found during testing may be higher or lower than expected
- Unseasonal weather conditions may occur during construction phase
- Exchange rates could vary beyond the range used to build our quotation

Variability risks typically result in a potential spread of possible values for some parameter relating to a planned event or activity, covering outcomes that are both higher and lower than expected. This presents a problem if we try to manage variability risks using the standard risk process. How can a range of possible outcomes be represented by a single "risk event"? If the variability includes both upside and downside, is the risk a threat or an opportunity or both? What do we do if the range of potential impact is very wide (for example a supplier may deliver late, by one day, one week, one month, or one year)? Should the risk be split into several?

The best way to analyse variability risks is in a quantitative risk analysis model using Monte Carlo simulation (Vose, 2008; Hulett, 2011). The standard probability distributions used in these models (triangular, lognormal, beta, gamma, weibull etc.) are all built using a range of values from a credible minimum to a credible maximum, with various intermediate values such as mean or most-likely (see Exhibit 4). These ranges are specifically designed to reflect the degree of uncertainty in key parameters such as time, cost, resource requirement, profitability etc., which makes them ideal for describing variability risks.

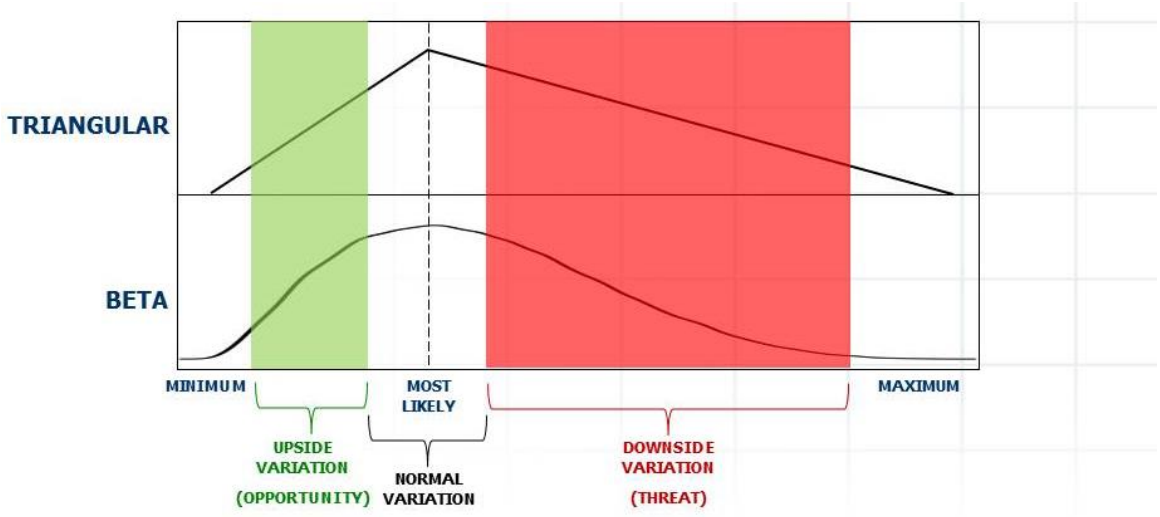

Exhibit 4: Using distributions to model variability risk

Once variability risks have been identified and their potential impact on project outcomes has been analysed in a risk model, responses can be designed to manage them. Responses to variability risks can address the range of possible variation, seeking to narrow the min-max spread by reducing or avoiding those threats that drive the worst-case values, and by exploiting or enhancing the opportunities that contribute to the best-case outcome. Alternatively responses can aim to shift the entire range towards the upside, by targeting the risks that influence the expected-value outcome.

Ambiguity risk

The third type of non-event risks are those relating to **ambiguity**. These are also known as "epistemic uncertainty", from the Greek word *episteme* meaning knowledge, since they describe uncertainties arising from lack of knowledge or understanding. Areas of the project where imperfect knowledge might affect our ability to achieve project objectives include:

- Elements of the requirement or technical solution
- Use of new technology
- Market conditions
- Competitor capability or intentions
- Future developments in regulatory frameworks
- Inherent systemic complexity in the project

Originally published as a part of the 2014 PMI Global Congress Proceedings – Phoenix, Arizona, USA

Ambiguity risks are addressed through exploration and experimentation, seeking first to define the scope and boundaries of those areas where we have a deficit of knowledge or understanding. The aim is to transform ambiguity risks into "known-unknowns".

Having understood where lack of knowledge might cause a problem, we can then take action to fill the gap, perhaps by obtaining expert external input, or by benchmarking our approach against best-practice, so that we can learn from the experience of others.

A second strategy to tackle ambiguity risk is through incremental development, prototyping or simulation. These allow us to take small steps within the scope of our existing limited knowledge, gradually extending the boundaries of our understanding. It is important with these approaches to ensure clear acceptance criteria for our project deliverables, so that each incremental step is directed towards achieving the overall project goals.

Emergent risk

Lastly, we have risks that emerge from our blind-spots. The technical name for these risks is "ontological uncertainty", but they are more commonly known as "Black Swans" (Taleb, 2007) or "emergent risks". They arise from limitations in our conceptual frameworks or world-view. These are risks which we are unable to see because they are outside our experience or mindset, so we don't know that we should be looking for them.

Another popular term for emergent risks is "unknown unknowns", which are things that we do not know but where we are unaware of our ignorance. In fact "unknown unknowns" can be divided into two types, one of which is a true emergent risk ("Black Swan") and the other is not.

1. The first group are "unknown-but-knowable unknowns". There are some uncertainties that we currently do not know, but which we could find out about. This is where the risk process can help, through creative risk identification, exploration and education. The aim is to expose those unknowns that could be known, so that we can deal with them effectively using a standard risk management approach. They are not true Black Swans because we could know about them if our predictive or discovery processes were better.
2. Secondly there are "unknown-and-unknowable unknowns". These are much more difficult to deal with, since by definition we can never discover them unless and until they happen. They are genuine emergent risks, which we could not predict with even the best risk process.

It is hard to give examples of typical emergent risks in projects, since by definition they are things outside of our current mindset or cognisance. In general terms, emergent risks arise from game-changers and paradigm-shifters, such as the release of disruptive inventions or products, or the use of cross-over technology from previously unforeseen sources. Previous high-profile emergent risks (both positive and negative) at the global level include the development of the commercial internet in 1982 and the current prevalence of social media use, the fall of the Berlin Wall in 1989 and subsequent collapse of communism, the 9/11 terrorist attack in New York in 2001 leading to enhanced aviation security, or the global financial crisis of 2008 followed by more stringent regulation.

Traditional risk management cannot manage emergent risks, since it only targets uncertainties that can be seen in advance and which we can prepare for or address proactively. At the strategic level, business continuity addresses "unknowable unknowns" by identifying areas of vulnerability then building in sufficient organisational resilience to cope with the impact of the unexpected, wherever it comes from. Business continuity also looks for early warning indicators or trigger events to tell us that something is different from normal. Finally, business continuity uses environmental scanning to help us discover potential emergent risks before they strike. It is possible to apply the same approaches at project, programme or operational levels.

In particular, attention should be given to developing strong "project resilience". Resilience can be defined as "*the capacity to maintain core purpose and integrity in the face of external or internal shock and change*", sometimes known as "*bounce-back-ability*." This requires each project to have:

- The right level of *contingency* built into its budget and schedule for currently-unknown emergent risks, in addition to a specific *risk budget* for known risks.
- Project *processes* that are flexible enough to cope with emergent risk while maintaining overall direction towards project goals, including strong change management.
- An *empowered project team* with *clear objectives*, who are trusted to get the job done within agreed limits, without needing approval for every small deviation from the original plan.
- Frequent targeted *project reviews* which review early warning signs and triggers in order to identify emergent risks as early as possible and allow proactive action to be taken.

Originally published as a part of the 2014 PMI Global Congress Proceedings – Phoenix, Arizona, USA

Conclusion and next steps

The idea that risk is "*uncertainty that matters*" has been central to risk management thinking and practice for decades. The commonly-adopted interpretation of this to mean that risk is limited to "*uncertain future events that, if they occurred, would have a negative effect on the project budget and/or schedule*." Unfortunately, this limited view of risk has necessarily resulted in a limited application of risk management to a mere subset of all the uncertainties that matter. Clearly any uncertainty that could affect our ability to achieve our objectives needs to be managed.

"*Uncertainty that matters*" has been elaborated in this paper to show that "*mattering*" includes both upside and downside impacts (opportunities as well as threats), and that any project objective can be affected by risk (not just project schedule or budget). We have also shown that "*uncertainty*" covers much more than just future events that may or may not occur. Four types of uncertainty can be distinguished, each of which could affect the ability of a project to succeed in meeting its objectives. These four include event risks ("stochastic uncertainty"), variability risks ("aleatoric uncertainty"), ambiguity risks ("epistemic uncertainty"), and emergent risks ("ontological uncertainty"). Exhibit 5 illustrates this more complete understanding of risk, expanding both the "uncertainty" side and the "mattering" dimension.

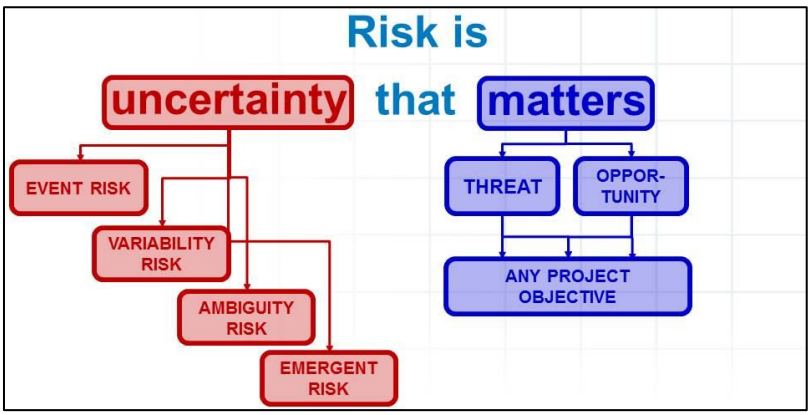

Exhibit 5: "Uncertainty that matters" expanded

If we recognise that the risk management effectiveness is a key determinant of project success or failure, then we will also accept that we must identify, assess and manage *any* uncertainty that matters. This poses challenges at two levels.

1. Firstly for the *profession*, it is important that risk standards and guidelines should clearly describe all types of risk, including those arising from the four sources of uncertainty described here, recognising that the impacts of risk can be positive or negative, and they can affect any project objective. Many of the current risk standards reinforce the view that risk is only about events with negative consequences to time and cost. Even where their definitions of risk are broader, then the detailed supporting processes usually fail to deal adequately with non-event risks or upside risks. Future editions of risk standards should address these shortcomings, otherwise they will prove inadequate to the task of promoting effective management of all risks.
2. Secondly for *practitioners*, we should start to implement these ideas immediately on our projects and in our organisations. Our risk workshops and checklists should prompt project stakeholders to think about all types of risk. Our risk processes and risk language should be inclusive of non-event risks, and should encourage proactive identification and management of opportunities, as well as defining impact scales for each project objective. While risk standards remain behind the curve, risk management practice can lead the way, demonstrating the value of a broader approach that encompasses all types of risk. When major organisations and leading practitioners begin to modify their approach to managing risk, the professional bodies and standards organisations will follow.

Risk management is too important to leave to chance, as it has a strong positive correlation with project success. Clearly risk management must manage risk, and we can only manage those risks that we can identify. A limited concept of risk inevitably leads to ineffective management of risk, as we will overlook other types of risk that lie outside our perspective and they will remain unmanaged. But the converse is also true: a broader concept of risk will support more effective risk management, ensuring that risk management manages **all** "uncertainties that matter".

Originally published as a part of the 2014 PMI Global Congress Proceedings – Phoenix, Arizona, USA

References

Association for Project Management. (2004) *Project Risk Analysis & Management (PRAM) Guide (second edition).* High Wycombe, Bucks UK: APM Publishing.

Association for Project Management. (2012) *Body of Knowledge (sixth edition).* High Wycombe, Bucks UK: APM Publishing.

Hillson, D. A. (2003) *Effective Opportunity Management for Projects: Exploiting Positive Risk.* Boca Raton, US: Taylor & Francis.

Hillson, D. A. (2007) *Understanding risk exposure using multiple hierarchies.* PMI Global Congress 2007 EMEA, Budapest, Hungary.

Hillson, D. A. (2009) *Managing Risk in Projects*. Farnham, UK: Gower.

Hillson D. A. & Simon P. W. (2012) *Practical Project Risk Management: The ATOM Methodology (second edition).* Vienna, US: Management Concepts.

Hulett D. T. (2011) *Integrated Cost-Schedule Risk Analysis*. Farnham, UK: Gower.

Institution of Civil Engineers, Institute and Faculty of Actuaries. (2014) *Risk Analysis & Management for Projects (RAMP) (third edition).* London UK: ICE Publishing.

ISO 31000:2009. *Risk Management – Principles and Guidelines*. Geneva, Switzerland: International Organization for Standardization.

Project Management Institute. (2009) *Practice Standard for Project Risk Management.* Newtown Square, PA: Project Management Institute.

Project Management Institute. (2013) *A Guide to the Project Management Body of Knowledge (PMBoK® Guide), (5th ed.).* Newtown Square, PA: Project Management Institute.

Taleb N. N. (2007) *The Black Swan: The impact of the highly improbable*. London UK: Allen Lane/Penguin.

UK Office of Government Commerce (OGC). (2010) *Management of Risk: Guidance for Practitioners (third edition).* London, UK: The Stationery Office.

Vose D. (2008) *Risk Analysis – A Quantitative Guide (third edition).* Chichester, UK: Wiley.

Originally published as a part of the 2014 PMI Global Congress Proceedings – Phoenix, Arizona, USA