Reprinted courtesy of Enterprise Risk magazine and the Institute of Risk Management

Through a glass darkly

BY ELMAR KUTSCH

The very standards and practices used to manage risks could be blinding organisations to their biggest threats

All over the world, companies and governments spend billions of dollars on what is euphemistically called risk management – gathering information about the future state and effect of their environment. Risk management is big business and becoming ever larger despite the worldwide downturn. For example, despite recent cost cutting and staff reductions, banks and broker dealers plan to increase their spending by $100 billion a year implementing risk governance frameworks by 2025. Risk management has been at the heart of organisations and standards in programmes that are promoted globally to increase the chance of success.

In many industries, such as healthcare, aeronautics, finance or aviation, the practice of risk analysis and management is deemed critical for sound decision-making about the unknown. The prescribed tools and techniques are enshrined in several best practice risk management standards including, to mention just a few, BS 31100:2021 risk management – code of practice and guidance for the implementation (published by the British Standards Institute); PMBOK® Guide (with risk management defined as a core process, published by the Project Management Institute (PMI)); and the APM Body of Knowledge (with risk management defined as a core process, published by the Association for Project Management (APM)).

Four major stages

The principal activity of risk management can be subdivided into four major stages: planning, identification, analysis and response.

First, we can apply risk management planning to define what activities should be taken to approach project and other risks. Second, risk identification allows us to single out risks that may affect the project objectives, thereby addressing the question of what can go wrong.

Third, by using risk analysis we evaluate quantitatively or qualitatively the likely impact of risks as well as the likelihood of occurrence – in other words, how likely it is that the threat will materialise and how serious it will be. The resulting risk analysis is often visualised as a risk matrix (see *A typical risk matrix*). This provides a simple analysis that enables managers to focus their responses on those risks with a high probability and high impact.

> **Best practice risk management standards indirectly claim to be self-evidently effective**

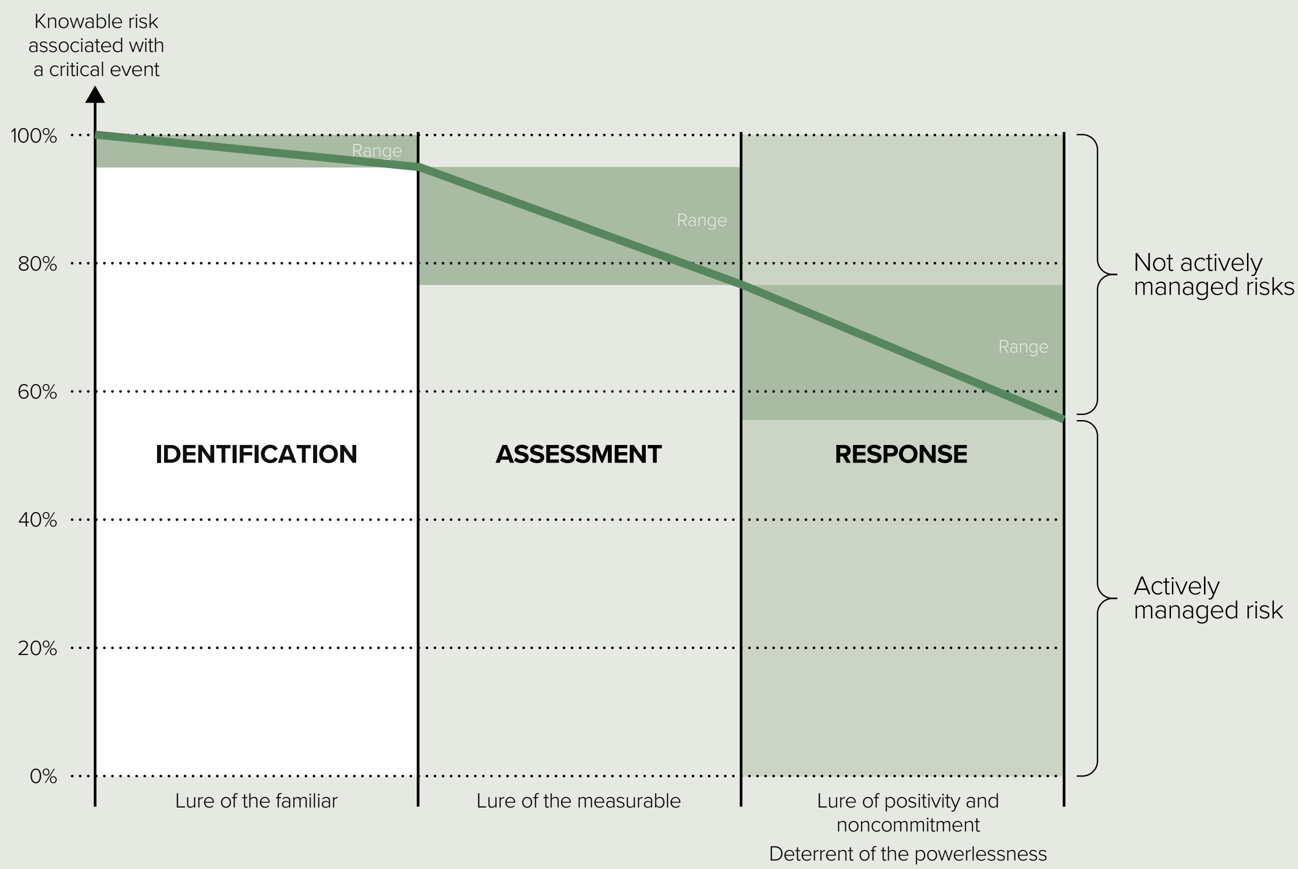
The fourth and final stage is to create a risk response – what will we do about it – that helps us to develop procedures and techniques to mitigate the defined risks. It enables organisations to keep track of these, identify new

A TYPICAL RISK MATRIX

IMPACT

LIKELIHOOD	Negligible	Minor	Moderate	Major	Catastrophic
Almost certain	Moderate	High	Extreme	Extreme	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Possible	Low	Moderate	High	High	Extreme
Unlikely	Low	Moderate	Moderate	High	High
Rare	Low	Low	Low	Moderate	Moderate

EXTENT OF DISENGAGEMENT



threats during the project and implement risk response plans.

As introduced and promoted by organisations such as PMI or APM, best practice risk management standards indirectly claim to be self-evidently effective. In this respect, writers such as Terry Williams have argued that project management includes risk management as a core process. In an article from 2005, he writes it "is presented as a set of procedures that are self-evidently correct: following these procedures will produce effectively managed projects; project failure is indicative of inadequate attention to the project management procedures."

However, research into the adoption of risk management practices indicates that we not only pay inadequate attention to it but also tend to disengage from such a supposedly self-evidently correct process altogether, with some serious consequences. The extent of disengagement from probabilistic risk management shows the extent to which knowable risks were left unmanaged by project managers in information systems projects – see *Extent of disengagement*. On average, 44 per cent of all risks that were discovered, understood and ascertained were not actively managed. This degree of disengagement from a purportedly universally applicable process is concerning.

> **On average, 44 per cent of all risks that were discovered, understood and ascertained were not actively managed**

The reasons for disengagement from a process that is being conveyed and promoted as unmistakably right are manifold. They can be summarised as three lures and one deterrent, which are spelt out below.

The lure of the familiar

Taboos reflect a moral or cautionary restriction placed on the action to know what is inappropriate. The risk management process requires risk managers to expose threats in order to analyse and respond

> **We tend to ignore difficult-to-measure risks, not because they are not useful or, indeed, have a significant probable impact, but because they are not 'easy' to assess**

to them. However, the exposure may also create anxiety among stakeholders, and negative thoughts may therefore be suppressed. As a result, we may limit the degree to which we identify new risks to those they are familiar with, confident about and already in control of. At the same time, we may exclude those risks from our attention that are unrecognisable to us.

The lure of the measurable

Risks are often ignored because they are deemed out of scope. Back in 1989, James Short wrote, "All too often such measures rest upon what can easily be counted, rather than on what is meaningful to those who are at risk, …".

Those risks that attract more attention than others may be unusually visible, sensational and easy to imagine. Risk actors tend to focus on the better-known and readily resolvable risks, obvious

DO YOU ACTIVELY MANAGE RISKS?

How well do the following statements characterise risk management in your project/programme? For each item, select one box only that best reflects your conclusion:

Lure of the familiar	NOT AT ALL		TO SOME EXTENT		TO A GREAT EXTENT
Our focus includes risks that we have not encountered in the past	1	2	3	4	5
The unfamiliar attracts our attention like nothing else	1	2	3	4	5
We encourage cross-functional perspectives to identify risks	1	2	3	4	5

Lure of the measurable	NOT AT ALL		TO SOME EXTENT		TO A GREAT EXTENT
We question the accuracy of risks	1	2	3	4	5
We like to be challenged in our risk estimates	1	2	3	4	5
We attend to those risks that are difficult to assess	1	2	3	4	5

Lure of optimism	NOT AT ALL		TO SOME EXTENT		TO A GREAT EXTENT
We look to identify as many risks as possible	1	2	3	4	5
Acknowledging risks does not question our competence to plan	1	2	3	4	5
We are encouraged to embrace risks as an opportunity	1	2	3	4	5

Lure of indecisiveness	NOT AT ALL		TO SOME EXTENT		TO A GREAT EXTENT
Ownership of risks does not constrain our freedom to act	1	2	3	4	5
Making a decision now is better than doing it later	1	2	3	4	5
We only defer decisions to risk if more information is required	1	2	3	4	5

Deterrent of powerlessness	NOT AT ALL		TO SOME EXTENT		TO A GREAT EXTENT
We feel empowered to deal with risks	1	2	3	4	5
We have access to a variety of responses to manage risks	1	2	3	4	5
We are experienced enough to deal with the risk at hand	1	2	3	4	5

SCORING: Add the numbers. If you score higher than 55, your are actively seeking to keep the risk gap low. If you score between 54 and 30, the danger of risks not being managed is moderate. Scores lower than 30 suggest the potential for a wider risk gap. Please question your risk management practices.

risks or those being perceived as legitimate. Hence, we tend to ignore difficult-to-measure risks, not because they are not useful or, indeed, have a significant probable impact, but because they are not "easy" to assess.

Lure of positivity and noncommitment

Due to the lack of statistical data for predicting future risks, we need to rely on subjective estimates. However, other stakeholders may not believe in the credibility of these estimates. So, during the risk identification phase, stakeholders might disagree over which risks are considered untrue or fictional. To avoid tensions that result from ambiguity, we may find that we just exclude those risks in contention from further management.

Deterrent of powerlessness

The lure of the familiar, the measurable, and positivity and noncommitment already reduce the chance for a risk to be proactively managed before it materialises. A further potential block is the deterrent of feeling powerless. Having a risk identified, analysed and associated with a response to it does not mean that that response can be enacted.

Despite having more knowledge at our disposal, we increasingly fail to pay attention to risks that ultimately matter. Instead, we tend to selectively concentrate on good-weather risks while ignoring others. This is symptomatic of an apparently universal problem – a risk gap – a gulf between what risks we should, and must, pay attention to and what risks we actually end up managing. Ultimately, we need to ask ourselves whether it is riskier to apply more of a particular process component, or refrain from doing it.

Hyper-rational

Proactive probabilistic risk management, with its assumptions of hyper-rationality, excludes many aspects of managerial behaviour. On the one hand, some stakeholders' preference lies in identifying, analysing and responding in advance. Other stakeholders appear to wait until risk resolves itself so to react to materialising risks only. Clive Smallman summarised the apparent emphasis of risk actors on reactive risk management: "It is hardly surprising that reactive risk management is dominant at the present time; it is, apparently, more certain and easier to manage and cost than the holistic approach."

Does this mean that the process of probabilistic risk management is doomed, given that it only helps us to manage 56 per cent of all knowable risks actively? These numbers may well indicate that, in many cases, the process of probabilistic risk management ends up a "tick-box exercise", with limited impact on mitigating risk. As one manager I interviewed told me: "… it becomes an administrative process and as long people feel there is a risk register somewhere and lip services paid to it on a reasonably frequent basis that they are managing risk."

Sanity check

If you like to do a quick sanity check on your engagement with probabilistic risk management, please complete the questionnaire *Do you actively manage risks?* Suppose you find yourself caught in the act of disengaging from such a process. Could you integrate more of your thinking and doing beyond the realm of probabilistic risk management into a more holistic routine of proactively managing risks?

For example, to address the lure of the familiar head-on, we should venture outside our zone of familiarity and make sense of those risks we have not yet experienced. This also helps us to offset the lure of the measurable. The more we think beyond what we are familiar with, the more we appreciate that our risk measurements become increasingly guesswork, and are inexact and inaccurate. Consequently, with increasing ambiguity comes a greater unease to take a risk for granted: we are more likely to challenge the degree of positivity we associate with them. Ultimately, we look at what truly constitutes a risk – and our erroneous perception of reality that has not yet materialised. The recognition of unfamiliarity, inexactness and inaccuracy, in combination with an appreciation of powerlessness, is an effective stimulant to do something about risk instead of disengaging from it.

Ultimately, it is not a question of whether or not to apply this supposedly straightforward, hyper-rational approach process. Instead, we should complement it with our tacit, at times illogical, counterintuitive but lived way of engaging with risks.

“ Proactive probabilistic risk management, with its assumptions of hyper-rationality, excludes many aspects of managerial behaviour

Elmar Kutsch is associate professor in risk management at the School of Management, Cranfield University. His most recent book is published by Routledge: *Organisational resilience: navigating paradoxical tensions*. IRM members can receive a 20 per cent discount on the print edition using code EFL01 by end of June.