



RISK DOCTOR BRIEFING

IMPLICIT AND EXPLICIT RISK MANAGEMENT



© May 2013, Dr David Hillson FIRM, HonFAPM, PMI Fellow

david@risk-doctor.com

Have you ever been asked “*How risky is your project?*” Most project managers find it hard to answer this question. Your Risk Register lists all the risks you’ve identified, and these are prioritised for attention and action, with responses and owners allocated to each risk. But how can a list of risks answer the “*How risky*” question? We need a different concept to describe the overall risk exposure of a project, which is different from the individual risks that need to be managed.

The Project Management Institute (PMI®) has addressed this in the *Practice Standard for Project Risk Management*, which has two distinct definitions of risk. The first is **individual risk** which is defined as “*an uncertain event or condition that, if it occurs, has a positive or negative effect on a project’s objectives.*” It also defines **overall project risk** as “*the effect of uncertainty on the project as a whole.*” The UK Association for Project Management (APM) also has two similar definitions of risk in its Body of Knowledge.

This dual concept of risk is important and useful when considering how to manage risk in projects. At one level the project manager is responsible for identifying, assessing and managing *individual risks*. At another higher level the project manager is also required to account to the project sponsor, the project owner and other stakeholders for the *overall risk of the project*. These two levels might be distinguished as **the risks in the project** and **the risk of the project**.

Managing risk requires action at both of these levels. But the typical project risk process only addresses the lower level of individual risks within the project, which are recorded in the Risk Register. It is far less common to consider the overall risk exposure of the project as a whole, or to have any structured approach to managing risk at that higher level. Clearly we’re missing something important here.

So how can overall project risk be identified, assessed and managed? The first place to address overall project risk is during the pre-project or concept phase, when the scope and objectives of the project are being clarified and agreed. Here the project sponsor or owner defines the benefits that the project is expected to deliver, together with the degree of risk that can be tolerated within the overall project. Each decision about the risk-reward balance involves an assessment of overall project risk, representing the inherent risk associated with a particular project scope and its expected benefits. At this level, overall project risk is managed implicitly through the decisions made about the scope, structure, content and context of the project.

Once these decisions have been made and the project is initiated, then the traditional project risk process can be used to address explicitly the individual risks that lie within the project. At key points within the project it will be necessary to revisit the assessment of overall project risk to ensure that the defined risk thresholds have not been breached, before returning to the ongoing task of managing individual risks within the project.

So two levels of risk management are important:

- **Implicit risk management** addresses **overall project risk** through decisions made about the scope, structure, context and content of the project
- **Explicit risk management** deals with **individual project risks** through the standard risk process to identify, assess, respond and review risks.

We need to understand and manage both of these types of risk if we want to answer the question “*How risky is your project?*”.

This two-level approach doesn’t just apply to projects. It can help senior management to understand the overall risk exposure of the business as well as particular risks that they need to address. The same is true for the risks associated with an operational portfolio or a functional department. In fact enterprise risk management (ERM) can only work properly if we address risk both **implicitly through our decision-making** and **explicitly through our risk processes**.