

PMP Exam Tips on Risk Management, Fourth edition

Jim Owens PMP



Know your definitions, and make sure you have read the section in PMBOK, and are able to categorise risks.

Perry Como and Willie Nelson...

... both sung the song “Accentuate the positive”:

**“You gotta accent-u-ate the positive,
E-lim-inate the negative,
An' latch on To the affirmative.
Don't mess with Mister in-between!”**

Two types of risk.

1. Accentuate the positive

“Risk” sounds bad, no matter how you say it! When most people think of risk, they think of something negative, something that can go wrong and cause damage and cost money, hence the expression “Risky business”.

In project management, bad risk are known as “pure” risks, “insurable” risks or “threats” (I wonder why they don’t call them “impure risks”?)

There is a second type of risk, known as “business risks”, or “opportunities”, which carry the possibility of a reward (but one which you have to work for, with no guarantee of success). In reality, “business risks” are seldom pursued, or are underutilized (i.e. pursued half-heartedly), However both types of risk must be assessed and managed; especially in the PMP exam

And for the exam, remember the first two lines of the song, and in that order, because PMI optimistically puts the pursuit of opportunities first in definitions.

E.g.; “The objectives of Project Risk Management are to **increase the probability and impact of positive events**, and decrease the probability and impact of negative events in the project.” (PMBOK is always right, PMBOK is always right).

2. Eliminate the Negative

Risk management tends to be unpopular with “management” (in the exam “management” normally means senior management) and with project managers. Probably one of the main reasons for this is the fear that risk management might uncover risks significant enough to cause the project to be cancelled. Besides, risk management takes time and money – two scarce commodities in organizations.

Another reason that risk management can be unpopular with some management is that the in-depth nature of this technique, means that it may uncover risks that management would prefer to keep hidden. For example, in the areas of “creative accounting” or hazards to third parties or the environment (Spooky! – while I was typing “Environ..”, my cheap wireless keyboard skipped the “vi” and typed “Enron”!)

Certain projects may cause people to lose their homes, the environment to be polluted, the habitat of rare flora or fauna to be damaged, and so on, and some unscrupulous organizations would not want to alert anyone in case external/internal opposition or legal action might prevent a lucrative project from proceeding.

But risk is not an option in project management, it is a fact – and unlike fairies, you don’t have to believe in them for them to visit you. Every project that you manage will have risks associated with it; some large, some small, some important and some

trivial. You can do some things to reduce the likelihood of a risk happening and you can do things to reduce the impact on your project if the risk does occur.

You can remove some risks all the time, and you can remove all of the risks some of the time, but you can never remove all of the risks all of the time (sounds like something that Winston Churchill would say).

If projects involve risks (threats), why do people do them? It's simply because the expected benefits from completing the project outweigh the possible losses caused by the occurrence of the risks. If the reverse were true you would be mad to manage the project.

I'll make an obvious point here – if you know an ethical reason why a project should not proceed, then you are obliged by the PMI Code of Ethics and Professional Conduct, to speak up (and step down, if necessary).

So if you decide to manage a project to develop asbestos filter tips for cigarettes – don't say I didn't warn you!

To manage risks you have to determine two main things:

1. What the risks to the project are, and
2. What sort of risk "appetite" your client has.

Obviously the identification of risks must occur very early in the project planning stage, so you have the greatest ability to manage them. But there's no point in writing a report just to store it in a cupboard. The risk plan needs to be revisited regularly throughout the project, and also each time a "risk event" occurs. This review process may involve many stakeholders.

Your client's "risk appetite" will be revealed during stakeholder analysis. Be aware too that your organisation may have its own policies and procedures in place for risk, normally contained in the Enterprise Environmental Factors, so you'll have to work within them (unless you can present a compelling reason for doing otherwise – but you must obtain management approval in advance).

One downside of good risk management planning is that stakeholders may become complacent, thinking that everything's been dealt with. Remember that if you take out a fire insurance policy on your house, it doesn't mean that your house will never burn down. But more than that, you might even stop looking for risks because you're sure that "someone" is looking after everything. Another point to bear in mind is that insurance may not save your project from a risk. Even if it pays for the damage sustained by the insurable item, the delay caused by replacing the item might delay the entire project (especially if it's on the critical path), or even cause the project to be cancelled.

There's a rough analogy with a story I heard about a car in the 1950's that crashed and was seriously damaged after a bolt in the steering system snapped. When the driver submitted a claim, he was given a new bolt.

Tools and techniques for risk identification include:

- Documentation reviews (examines the quality and consistency of the project documents, along with the requirement)
 - **Brainstorming**
 - **Interviewing (aka Expert interviewing)**
 - **Delphi technique**
 - Root cause analysis
- } Probably the 3 most common, and in this order

- Checklist analysis
- Assumption Analysis
- Diagramming techniques
- SWOT analysis (Strengths, Weaknesses, Opportunities, and Threats)
- Expert judgment

There are two levels to risk analysis:

1. Qualitative:

subjective, usually employs words, such as “low”, “medium” and “high” rather than numbers (but simple number can be used, e.g. 0 to 5, to keep engineers happy).

2. Quantitative:

Important risks may be subjected to quantitative analysis (more precise numbers, data ranges, and historical information)

Monte Carlo simulations are typically associated with **quantitative** risk analysis.

For each risk you should determine:

1. The probability that it will occur,
2. The impact on the project,
3. When in the project it is likely to occur, and
4. How often it is likely to occur.

Four possible risk responses

(Five, if you include “resigning”)

■ **Avoidance**

This involves actually changing the project plan so that a particular risk can't happen (note however that changing the project plan may inadvertently introduce new risks, called “Secondary risks”, and changes to the scope must be agreed with the client and performed through Integrated Change Management).

■ **Mitigation**

Steps are taken to reduce the likelihood and/or the impact of an identified risk.

■ **Transference**

You pay someone to take the risk on your behalf. For example you get another company to manufacture a risky part of the project deliverable. But it is vital to realise that the risk still exists, it is only the responsibility that you have attempted to transfer.

I say “attempted” because now there is a (secondary) risk that:

- The other company may be late to deliver, or deliver unacceptable quality.
- You might end up in litigation with the other company over product scope arguments, or
- The other company may become bankrupt and unable to produce the component and unable to refund your money, or
- The other company may become bankrupt and *sue you* for bad business practices (unfair contract, etc).

For example, some organizations outsource their Business Continuity management in an attempt to transfer risk. But in the “Twin Towers” disaster, several complete Business Continuity companies were wiped out along with any chance of their client companies “continuing”.

- **Acceptance** You simply decide that you will accept the consequence of the risk if it occurs. This may be because you think:
 - There’s virtually no chance of it happening (e.g. an earthquake in London), or
 - The impact would be negligible, or
 - It is too expensive to deal with (e.g. cost of insurance may be more than the impact of the risk event).

Some of the risks are going to materialise as you progress with the project so you need a monitoring system to warn you of them (watch for “triggers”) and you’ll need a risk management plan so that you’ll know what to do when they happen.

Watch the outputs from the other management areas (e.g. earned value, quality control etc), as a warning sign of impending risk events.

Risk Categories Include

- **Technical, quality or performance risks** - such as reliance on unproven or complex technology, unrealistic performance goals, changes to the technology used or to industry standards during the project.
- **Project-management risks** - such as poor allocation of time and resources, inadequate quality of the project plan, poor use of project management disciplines.
- **Organizational risks** - such as cost, time, and scope objectives that are internally inconsistent, lack of prioritization of projects, inadequacy or interruption of funding, and resource conflicts with other projects in the organization.
- **External risks** - such as shifting legal or regulatory environment, labor issues, changing owner priorities, country risk, and weather. *Force majeure (act of god)* risks such as earthquakes, floods, and civil unrest generally require disaster recovery actions rather than risk management.
- **Historical information** - information on prior projects may be available from project files or published information through commercial or academic sources.

Other exam tips

- Risk identification should involve **all** stakeholders.
- Risks can be shown diagrammatically on an **RBS** (Risk Breakdown Structure) that looks like a WBS.
- Use **templates** where possible. If your organization has performed similar projects before, then check through the Organizational Process Assets for reports, RBS, checklists etc that you can reuse.
- In most of the Risk Management processes, the outputs of one process are the inputs to the next.
- Qualitative risk analysis is always required, quantitative analysis may not be.
- Qualitative risk analysis precedes, quantitative analysis (if used). Quantitative analysis is performed on only the higher risk categories.

- **Workarounds** are unplanned responses to emerging risks that were previously **unexpected** (as the risks are unknown until they occur so you can't possibly have a contingency plan in place). But they are also the unplanned responses to emerging risks that were previously **accepted**, (in which case you previously decided **not to have** a contingency plan).
- Risks (and assumptions) have to be constantly reviewed and communicated to stakeholders.
- Insuring against a risk does **not** prevent the risk from occurring.
- Passive acceptance means that you do nothing to plan for the risk. Active acceptance means that allocate reserves in the project and formulate a contingency plan.
- A **secondary risk** is one caused by the implementation of a response to another risk.
- **Contingency reserves** are for known unknowns.
- **Management reserves** are for unknown unknowns.

N.B. Some project managers may have different viewpoints or opinions to those expressed here – but PMI are marking your exam, so the PMBOK is *always* right and if I say anything that appears to contradict the PMBOK, then believe the PMBOK.

PS I've made every effort to get this right to help you in your exam – but if I've missed something please let me know.

Regards, Jim Owens PMP

Columnist with www.PMHub.net