Chapter 1: Risk Definition

Definition

A risk is a potential problem, a situation that, if it materializes, may adversely affect the project. Risks that materialize are no longer risks, they are problems.

All projects have risks, and all risks are ultimately handled: 1). Some disappear, 2). some develop into problems that demand attention, and 3). a few escalate into crises that destroy projects. **The goal of risk management is to ensure that risks never fall into the third category.**

There are four steps to managing risks: **identify them, categorize them, mitigate them, and manage them.**

1.1 Identifying Risk

Identifying Risks

Although all projects are different, the same risks – those listed in Table 1.1 tend to recur. The list in Table 1.1 is not exhaustive, and in identifying the risks for a project, you must continually ask, **"What can possibly go wrong?"**

If there is one risk that is universally the most dangerous for all projects, it is the following:

> *Corporate management views the project manager's risk analysis as alarmist and will not take the risks seriously until they materialize.*

The only way to mitigate this risk is to document all other risks, identify the actions you take, and keep a management informed, especially as the risk becomes more probable. *It is only by stressing your risk analysis, by making explicit recommendations, and by insisting that management understand the risks that you can avoid having to say, "See, I told you so."*

Common Risks

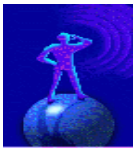
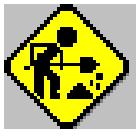
1.2 Common Risks

Staff, equipment, client, scope, technology, delivery and physical

Table 1.1 lists common risks that most projects will encounter; They form a starting point for developing a catalog of risks. However, the list is not exhaustive; most project managers will find several more risks that they can add, and project experience will tend to increase this number. When you are assessing the risks for your projects, always refer to a list such as this. Otherwise, you run the project

management risk that not all project risks are identified.

Table 1.1: Sample list of project risks

	***Staff Risks*** Key staff will not be available when needed. Key skill sets will not be available when needed. Staff will be lost during the project.
	***Equipment Risks*** Required equipment will not be delivered on time, Access to hardware will be restricted. Equipment will fail.
	***Client Risks*** Client resources will not be made available as required. Client staff will not reach decisions in a timely manner. Deliverables will not be reviewed according to the schedule. Knowledgeable client staff will be replaced by those less qualified.
	***Scope Risks*** Requirements for additional effort will surface. Changes of scope will be deemed to be included in the project. Scope changes will be introduced without the knowledge of project management.
	***Technology Risks*** The technology will have technical or performance limitations that endanger the project. Technology components will not be easily integrated. The technology is new and poorly understood.
	***Delivery Risks*** System response time will not be adequate. System capacity requirements will exceed available capacity. The system will fail to meet functional requirements
	***Physical Risks*** The office will be damaged by fire, flood, or other catastrophe. A computer virus will infect the development system. A team member will steal confidential material and make it available to competitors of the client.

Categorizing Risks

1.3 Categorizing Risks

To describe the risk as extreme, high, low or minimal

There are numerous statistical methods for defining degree of risks, but the simplest categorization, and therefore the most effective, **is to describe risks as extreme, high, medium, low, or minimal**.

The degree of risk depends upon two characteristics: the probability that the risk will occur, and its impact on the project if it does.

Probability and impact are both categorized as **high, medium, and low,** and their relationship, as illustrated in Table 1.2 indicates the degree of risk.

Consider two risks: that a team member will resign during the project and that a fire will consume the office, destroying the installation and all the work that has been done. Both risks are of medium degree. In the first case, although the probability is high, the impact is low: You assume that the team member will give adequate notice and can be easily replaced. The second risk has a high – in fact, potentially devastating – impact, but the probability is low and the risk is easily mitigated by ensuring proper off-site backup.

You categorize risks so that you can identify those that are the most dangerous and therefore require the most attention. It is the extreme and high risks that need your attention first.

Table 1.2: Categorization of degree of risk

Probability	Impact		
	High	Medium	Low
High	Extreme	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Minimal

Mitigating Risks

1.4 Mitigating Risks

By reducing its probability, its impact or both

You mitigate a risk by reducing its probability, its impact, or both. Since every project is unique, so are the mitigating actions. However, some principles apply across projects and risks.

1. **Remove excuses:** When the project depends on someone (such as a supplier, client, or line manager) to provide something (such as staff, equipment, or material) in accordance with a schedule, **ensure that the provider knows the schedule, knows what is expected, and understands the consequences of a slippage.** For major providers, such as the client, make up a schedule giving the exact dates when the project will require resources. If

you have exact dates when the project will require client resources. If you are not able to give an exact date now, give a date by which you will be able to.

You remove excuses by providing visibility into the project, an active process in which provides are forced to understand what is expected of them. For example, if you have ordered a piece of equipment with a two-month lead time to be delivered by a specified date, just putting a required date on the purchase order is not enough. **Four weeks before delivery, call the sales representative to verify the schedule. Three weeks prior, call to clarify, for example, the power requirements. At two weeks, call to clear up a technical question. One week ahead of time, call to establish shipping procedures**. *With each call, of course, you will ask if there are any problems that could delay delivery, and you will emphasize how critical timely delivery is. After this series of calls, the supplier has no excuses to fall back on.* There is no guarantee, of course, that the equipment will actually be delivered on time, but by actively reminding the supplier of the schedule, you have reduced the probability of a late delivery.

2. **Demand visibility:** *when the project depends on someone delivering something and there is a process that the provider must follow before delivery,* **you must understand at least the milestones of the process**. For example, if a piece of equipment must be manufactured, identify the checkpoints in the manufacturing process, have the sales representative attach dates to each checkpoint, and call on those dates to ensure that the milestones have been met and there are no delays.

If the process is repetitive, such as client review and approval of project documents, understand the process. **What happens to a document when it is received? Who reviews it? How are individual reviews reconciled? Is there a final authority for approval? Who? What is the priority of the project for the reviewers?** With this understanding, you will be able to suggest changes in the process that will speed things up, if there are delays.

3. **Help people communicate:** When there is a surprise, the project manger is frequently the last to know, even though the informal communications network (or "rumor mill") among team members and users contains various tidbits and snippets of information that provide inklings of problems to come. **Helping people to communicate increases the probability that useful information will find its way to you.**

The communications network can provide advance warning that an employee is dissatisfied and looking elsewhere, that the performance of a system may be slower than required, that software components may not integrate smoothly, or that covert scope changes are being

smuggled into the system. In other words, the rumor mill is a prime course of information about emerging risks.

The key rule to using the rumor mill is, "Don't shoot the messenger." No matter how painful the information, thank the deliverer; otherwise, like the jilted spouse, you will be the last to know.

4. **Plan fallbacks:** *If the technology does not perform adequately, what can be done to improve it? If a critical team member is lost to the project, how will those skills be replaced? If the building burns down, how does the project recover? Fallbacks are your plans for when the worst happens.*

Fallbacks must be capable of being put into action, either now or when they are needed, and they must be capable of being handled within the budget, schedule, and functionality of the project. If this is not the case, they are not fallbacks; they are wishes with nothing to anchor them but the fervent hope they will never have to be exercised.