CHAPTER

8

Managing Project Risk

CHAPTER OVERVIEW

Chapter 8 focuses on project risk management. After studying this chapter, you should understand and be able to:

- Describe the project risk management planning framework introduced in this chapter.
- Define risk identification and the causes, effects, and integrative nature of project risks.
- Apply several qualitative and quantitative analysis techniques that can be used to prioritize and analyze various project risks.
- Describe the various risk strategies, such as insurance, avoidance, or mitigation.
- Describe risk monitoring and control.
- Describe risk evaluation in terms of how the entire risk management process should be evaluated in order to learn from experience and to identify best practices.

GLOBAL TECHNOLOGY SOLUTIONS

The Husky Air project team filed into the GTS conference room, and everyone took a seat at the conference table. No one seemed to know why this urgent meeting had been called, but they knew from Tim Williams' e-mail that they were about to hear some interesting news.

Tim walked into the room and shut the door behind him. Everyone could tell by the expression on his face that the news was not going to be good. Tim took a seat at the head of the table. "Thank you all for being here on such short notice," he said. "As you all know, I had a meeting with our client this morning to go over the project plan we prepared." The look on Tim's face grew more serious, and the tension began to thicken. He paused, then continued, "Husky Air's management has informed me that they are feeling the effects of the downturn in the economy. The company is getting hit from two

sides. First, there has been an increase in fuel costs. Second, with the continuing demand for airline pilots, several of its more experienced charter pilots have left to take jobs with the scheduled airlines. With costs up and revenues down, cash flow is a concern."

The project team members looked at each other with puzzled expressions. Sitaramin spoke up, "Tim, how will this affect *our* project?"

Tim looked down at faces of the team members gathered around the table. "When I met with them this morning, a few of the managers were inclined to cancel the project," he said. "However, because we focused on the value that this project is expected to bring to the organization, they decided that the project was too valuable to just cancel outright. But because cash flow is a problem, they need to reduce the cost of the project. After much discussion, it was agreed that we would trim the project's scope in order to decrease the project's budget. The good news is that Husky Air's management believes that the increase in fuel costs will be temporary and they are in the process of recruiting new pilots. However, it may be a few months before they are back on solid financial ground. If that happens, they want us complete the rest of the scope as we had originally planned. In the meantime, we'll have to get back to work and come up with a revised schedule and budget."

Ted, the project's telecommunication specialist, asked, "What about our contract with Husky Air? Can't we hold them to the contract they signed?"

"I just got off the phone with our company's lawyer," Tim answered. "She said that our contract allows either party to cancel the project if they can not fulfill the terms of the agreement. There's a significant financial penalty, of course, but Kellie and I decided that it was in everyone's best interest to renegotiate the contract based on a newly defined scope. We feel legal action is not the best way to build and maintain a good, long-term relationship with our client. Kellie did a quick financial analysis and believes we can still make a profit without having to downsize our project team. Besides, we have leads for several other projects with new clients so all of our eggs are not in one basket."

"Well at least I can still make the payments on my new car!" joked Pat. Everyone in the room laughed.

Sitaramin asked, "Tim, maybe we should think seriously about what else could affect our project?"

Tim looked around the table at the other team members. They seemed to be in agreement with the suggestion. Pat spoke up, "Sitaramin's right. What we need to do is come up with a risk management plan."

Tim laughed, "Okay, it looks like we're in for another brainstorming session. I just hope we have enough color markers. Any suggestions as to how we should get started?"

Even though the team had received bad news just a few minutes earlier, they were energized by thought of tackling another problem together. Yan suggested they focus on identifying different risks and the potential impact they might have on the project. This process would help them come up with strategies for handling risks and reduce the likelihood of surprises. Then, the team could develop a learning cycle to identify the facts, assumptions to be tested, and things to find out. The lessons learned could be documented and made part of the GTS knowledge base. Pat thought that was a good idea, and he suggested that they also identify triggers or flags that warn them when a particular risk might be imminent. This system would allow them to monitor the project's risk throughout the project life cycle and reduce the likelihood of being surprised again.

Tim rolled up his sleeves and walked over to the whiteboard. "Okay, everyone, slow down so I can write these ideas down," he said. "Now, how do you propose we get started?" Tim grinned and thought to himself how much he enjoyed working with this group of people.

Things to Think About:

1. Was the financial downturn of Husky Air a problem that the GTS team could have foreseen and avoided?
2. Can all risks to a project be identified and managed?
3. In addition to identifying threats, why should project stakeholders also look for opportunities?

INTRODUCTION

In the last chapter you learned how to develop a baseline project plan. This project plan is based on a number of estimates that reflect our understanding of the current situation, the information available, and the assumptions we must make. The fact that we must estimate implies a degree of uncertainty in predicting the outcome of future events. Although no one can predict the future with 100 percent accuracy, having a solid foundation, in terms of processes, tools, and techniques, can increase our confidence in these estimates.

Unfortunately, things seldom go according to plan because the project must adapt to a dynamic environment. Project risk management is becoming an important sub-discipline of software engineering. It focuses on identifying, analyzing, and developing strategies for responding to project risk efficiently and effectively (Jones 1994). It is important, however, to keep in mind that the goal of risk management is not to avoid risks at all costs, but to make well-informed decisions as to what risks are worth taking and to respond to those risks in an appropriate manner (Choo 2001).

Project risk management also provides an early warning system for impending problems that need to be addressed or resolved. Although risk has a certain negative connotation, project stakeholders should be vigilant in identifying opportunities. Although many associate uncertainty with threats, it is important to keep in mind that there is uncertainty when pursuing opportunities, as well.

It is unfortunate that many projects do not follow a formal risk management approach (Jones 1994). Because of their failure to plan for the unexpected, many organizations find themselves in a state of perpetual crisis characterized by an inability to make effective and timely decisions. Many people call this approach *crisis management or fire fighting* because the project stakeholders take a reactive approach or only address the project risks after they have become problems. Several common mistakes to managing project risk include:

- *Not Understanding the Benefits of Risk Management*—Often the project spon sor or client demands results. They may not care how the project team achieves its goal and objectives—just as long as it does! The project manager and project team may rely on aggressive risk taking with little understanding of the impact of their decisions (Lanza 2001). Conversely, project risks may also be optimistically ignored when, in reality, these risks may become real and significant threats to the success of the project. Unfortunately, risks are often schedule delays, quality issues, and budget overruns just waiting to hap pen (Wideman 1992). Risks can result in sub-par productivity and higher than average project failure rates (Kulik 2000).
- *Not Providing Adequate Time for Risk Management*—Risk management and the ensuing processes should not be viewed as an add-on to the project plan ning process, but should be integrated throughout the project life cycle (Lanza 2001). The best time to assess and plan for project risk, in fact, is at the earliest stages of the project when uncertainty for a project is the highest.

Catastrophic problems or surprises may arise that require more resources to correct than would have been spent earlier avoiding them (Choo 2001). It is better to reduce the likelihood of a risk or be capable of responding to a particular risk as soon as possible in order to limit the risk's impact on the project's schedule and budget.

- *Not Identifying and Assessing Risk Using a Standardized Approach*—Not having a standardized approach to risk management can overlook both threats and opportunities (Lanza 2001). Consequently, more time and resources will be expended on problems that could have been avoided; opportunities will be missed; decisions will be made without complete understanding or information; the overall likelihood of success is reduced; and catastrophic problems or surprises may occur without advanced warning (Choo 2001). Moreover, the project team may find itself in a perpetual crisis mode. Over time, crisis situations can have a detrimental effect on team morale and productivity.

Capers Jones (1994) suggests that effective and successful project risk management requires:

- *Commitment by all stakeholders*—To be successful, project risk management requires a commitment by all project stakeholders. In particular, the project sponsor or client, senior management, the project manager, and the project team must all be committed. For many organizations, a new environment and commitment to following organizational and project processes may be required. For many managers, the first impulse may be to shortcut or sidestep many of these processes at the first sign that the project is in trouble. A firm commitment to a risk management approach will not allow these impulses to override the project management and risk management processes that the organization has in place.
- *Stakeholder Responsibility*—It is important that each risk have an owner. This owner is someone who will be involved in the project, who will take the responsibility to monitor the project in order to identify any new or increasing risks, and who will make regular reports to the project sponsor or client. The position may also require the risk owner to ensure that adequate resources be available for managing and responding to a particular project risk. Ultimately, however, the project manager is responsible for ensuring that appropriate risk processes and plans are in place.
- *Different Risks for Different Types of Projects*—In a study that looked at IT project risks, Jones (1994) found that patterns of risk are different across different types of IT projects. The results of this study are summarized in Table 8.1. The implication is that each project has its own unique risk considerations. To attempt to manage all projects and risks the same way may spell disaster.

The remainder of this chapter will incorporate many of the processes and concepts outlined in the Project Management Body of Knowledge (PMBOK) that define the processes of risk management. More specifically, these processes include:

- *Risk Management Planning*—Determining how to approach and plan the project risk management activities. An output of this process is the development of a risk management plan.
- *Risk Identification*—Deciding which risks can potentially impact the project. Risk identification generally includes many of the project stakeholders and requires an understanding of the project's goal, as well as the project's scope, schedule, budget, and quality objectives.

8.1 Various Software Risks for IT Projects

MIS Software Risks		*Systems Software Risks*		*Commercial Software Risks*		*Military Software Risks*		*Contract or Outsourced Software Risks*		*End-User Software Risks*	
Creeping user requirements	80%	Long schedules	70%	Inadequate user documentation	70%	Excessive paper work	90%	High maintenance costs	60%	Non-transferable application	80%
Excessive schedule pressure	65%	Inadequate cost estimates	65%	Low user satisfaction	55%	Low productivity	85%	Friction between contractor & client personnel	50%	Hidden errors	65%
Low quality	60%	Excessive paper work	60%	Excessive time to market	50%	Long schedules	75%	Creeping user requirements	45%	Unmaintainable software	60%
Cost overruns	55%	Error-prone modules	50%	Harmful competitive actions	45%	Creeping user requirements	70%	Unanticipated acceptance criteria	30%	Redundant application	50%
Inadequate configuration control	50%	Canceled projects	25%	Litigation expense	30%	Unused or unusable software	45%	Legal ownership of software & deliverables	20%	Legal ownership of software & deliverables	20%

SOURCE: T.C. Jones, *Accessment and Control of Software Risks*, 1994.

Qualitative Risk Analysis—Focusing on a qualitative analysis concerning the impact and likelihood of the risks that were identified.

Quantitative Risk Analysis—Using a quantitative approach for developing a probabilistic model for understanding and responding to the risks identified.

Risk Response Planning—Developing procedures and techniques to reduce the threats of risks, while enhancing the likelihood of opportunities.

Risk Monitoring and Control—Providing an early warning system to monitor identified risks and any new risks. This system ensures that risk responses have been implemented as planned and had the effect as intended.

IT PROJECT RISK MANAGEMENT PLANNING PROCESS

To manage risk, we first need to have a definition *of risk.* Although *Webster s* dictionary defines risk as *"hazard; peril; or exposure to loss or injury, "* the PMBOK defines **project risk as:**

> An uncertain event or condition that, if it occurs, has a positive or negative effect on the project objectives. (127)

The PMBOK definition provides an important starting point for understanding risk. First, project risk arises from uncertainty. This uncertainty comes from our attempt to predict the future based on estimates, assumptions, and limited information. Although project risk has a downside resulting from unexpected problems or threats, project risk management must also focus on positive events or opportunities. Therefore, it is important that we understand what those events are and how they may impact the project beyond its objectives. It is also important that we understand not

A WILD FRONTIER

Very few companies have a fully integrated approach to managing their information technology and business risks together. The companies that do tend to manage and monitor their IT risks with a fragmented approach. A survey conducted by Arthur Andersen & Co. and The Economist Intelligence Unit found that more than two-thirds of the 150 chief executive offices, chief financial officers, and chief information officers admit that IT risks are not that well-understood in their companies. In fact, only one-third of the companies have methods to determine risk. A common problem cited was that few companies try to anticipate problems once systems are implemented. For example, security is a common threat to many electronic business systems; however, few companies can actually say what impact security problems and threats would have on their customers. As it turns out, crisis management is much more expensive and embarrassing than risk management.

SOURCE: Adapted from Thomas Hoffman, Risk Management Still a Wild Frontier, *Computerworld*, February 16, 1998. http://www.com-puterworld.com/news/1998/story/0,11280,29808,00.html

only the nature of project risks but also how those risks interact and impact other aspects of the project throughout the life of a project. The PMBOK defines project risk management as:

> The systematic process of identifying, analyzing, and responding to project risk. It includes maximizing the probability and consequences of positive events and minimizing the probability and consequences of adverse events. (127)

This PMBOK definition of risk management suggests that a systematic process is needed to effectively manage the risk of a project. In this section, an approach for risk management planning is introduced. It is illustrated in Figure 8.1.

The framework presented in Figure 8.1 outlines seven steps for managing IT project risk. Each of these steps will be discussed in more detail throughout the chapter.

Risk Planning

Risk planning is the first step and begins with having a firm commitment to the entire risk management approach from all project stakeholders. This commitment ensures that adequate resources will be in place to properly plan for and manage the various risks of the IT project. These resources may include time, people, and technology. Stakeholders also must be committed to the process of identifying, analyzing, and responding to threats and opportunities. Too often plans are disregarded at the first sign of trouble, and instinctive reactions to situations can lead to perpetual crisis management. In addition to commitment, risk planning also focuses on preparation. It is important that resources, processes, and tools be in place to adequately plan the activities for project risk management. Systematic preparation and planning can help minimize adverse effects on the project while taking advantage of opportunities as they arise.

Risk Identification

Once commitment has been obtained and preparations have been made, the next step entails identifying the various risks to the project. Both threats and opportunities must be identified. When identifying threats to a project, they must be identified clearly so that the true problem, not just a symptom, is addressed. Moreover, the causes and effects of each risk must be understood so that effective strategies and responses can

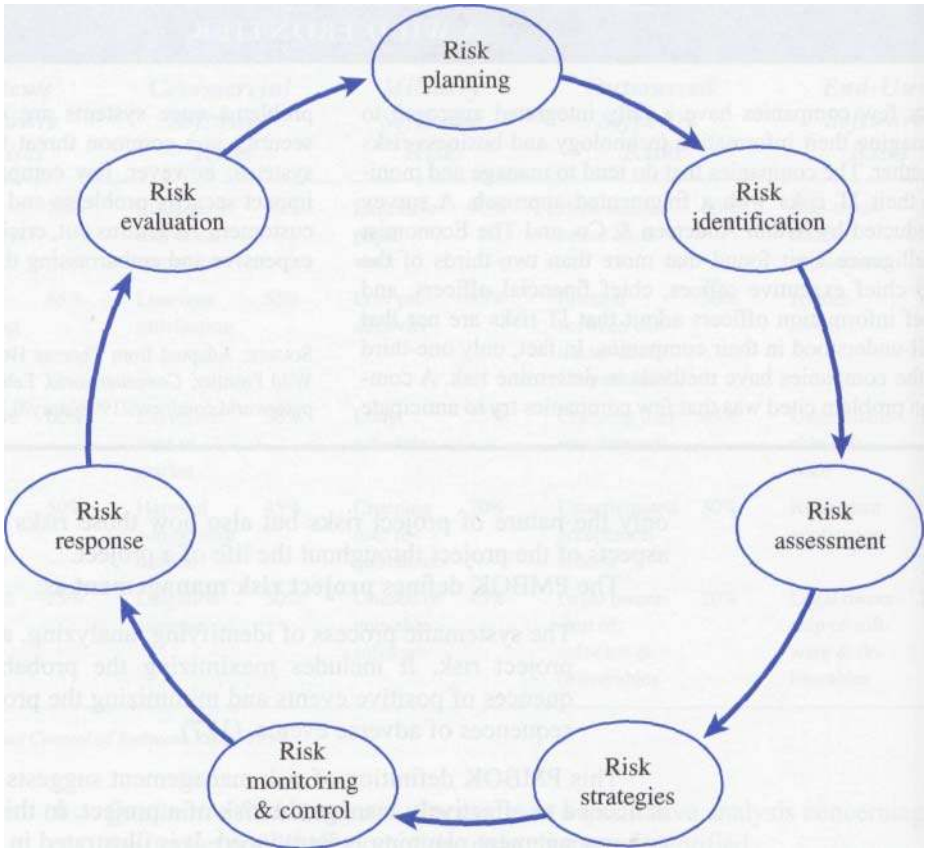


Figure 8.1 IT Project Risk Management Processes

be made. A framework for understanding the sources and nature of IT project risks will be introduced in the next section; however, it is important to keep in mind that project risks are rarely isolated. Risks tend to be interrelated and affect the project and its stakeholders differently.

Bisk Assessment

Once the project risks have been identified and their causes and effects understood, the next step requires that we analyze these risks. Answers to two basic questions are required: What is the likelihood of a particular risk occurring? And, what is the impact on the project if it does occur? Risk assessment provides a basis for understanding how to deal with project risks. To answer the two questions, qualitative and quantitative approaches can be used. Several tools and techniques for each approach will be introduced later. Assessing these risks helps the project manager and other stakeholders prioritize and formulate responses to those risks that provide the greatest threat or opportunity to the project. Because there is a cost associated with responding to a particular risk, risk management must function within the constraints of the project's available resources.

Risk Strategies

The next step of the risk planning process is to determine how to deal with the various project risks. In addition to resource constraints, an appropriate strategy will be

determined by the project stakeholders' perceptions of risk and their willingness to take on a particular risk. Essentially, a project risk strategy will focus on one of the following approaches:

- Accept or ignore the risk.
- Avoid the risk completely.
- Reduce the likelihood or impact of the risk (or both) if the risk occurs.
- Transfer the risk to someone else (i.e., insurance).

In addition, triggers or flags in the form of metrics should be identified to draw attention to a particular risk when it occurs. This system requires that each risk have an owner to monitor the risk and to ensure that resources are made available in order to respond to the risk appropriately. Once the risks, the risk triggers, and strategies or responses are documented, this document then becomes the risk response plan.

Risk Monitoring and Control

Once the salient project risks have been identified and appropriate responses formulated, the next step entails scanning the project environment so that both identified and unidentified threats and opportunities can be followed, much like a radar screen follows ships. Risk owners should monitor the various risk triggers so that well-informed decisions and appropriate actions can take place.

Risk Response

Risk monitoring and control provide a mechanism for scanning the project environment for risks, but the risk owner must commit resources and take action once a risk threat or opportunity is made known. This action normally follows the planned risk strategy.

Risk Evaluation

Responses to risks and the experience gained provide keys to learning. A formal and documented evaluation of a risk episode provides the basis for lessons learned and lays the foundation for identifying best practices. This evaluation should consider the entire risk management process from planning through evaluation. It should focus on the following questions:

- How did we do?
- What can we do better next time?
- What lessons did we learn?
- What best practices can be incorporated in the risk management process?

The risk planning process is cyclical because the evaluation of the risk responses and the risk planning process can influence how an organization will plan, prepare, and commit to IT risk management.

IDENTIFYING IT PROJECT RISKS

Risk identification deals with identifying and creating a list of threats and opportunities that may impact the project's goal and/or objectives. Each risk and its characteristics are documented to provide a basis for the overall risk management plan.

An IT Project Risk Management Framework

Identifying and understanding the risks that will impact a project is not always a straightforward task. Many risks can affect a project in different ways and during different phases of the project life cycle. Therefore, the process and techniques used to identify risks must include a broad view of the project and attempt to understand a particular risk's cause and impact among the various project components. Figure 8.2 provides a framework for identifying and understanding the sources and impacts of IT project risks.

At the core of the IT project risk framework is the MOV, or measurable organizational value. The MOV is the goal of the project that defines the measurable value the organization expects from the project. It is both a measure and definition of project success.

The next layer of the framework includes the project objectives in terms of scope, quality, schedule, and budget. Although these objectives are not by themselves sufficient conditions for success, together they do play a critical role in supporting the MOV.

The third layer focuses on the sources of IT project risk. Risks can arise as a result of the various people or stakeholders associated with a project, legal considerations,

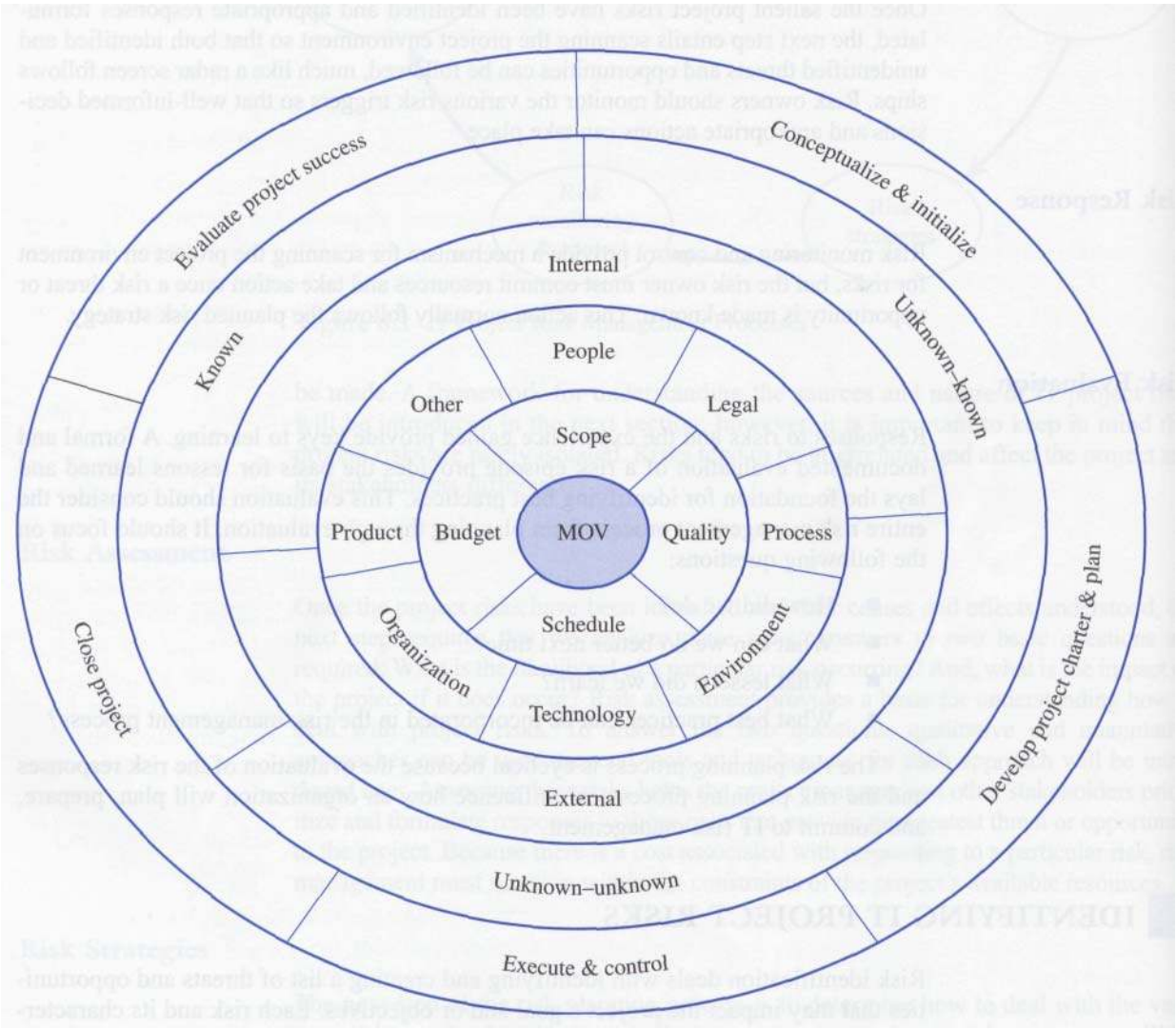


Figure 8.2 IT Project Risk Framework

the processes (project and product), the environment, the technology, the organization, the product, and a catchall category called *other*.

The next layer focuses on whether the sources of risk are internal or external to the project. It is important to make this distinction because a project manager is responsible and accountable for all project risks internal to the project. For example, if a project team member is not adequately trained to use a particular technology, then the project's objectives—scope, schedule, budget, and quality—may be impacted. In turn, this lack of training may inhibit the project from achieving its goal or MOV. Once this project risk has been identified along with its impact, the project manager can avoid or mitigate the risk by sending this particular project team member to training or by assigning certain critical tasks to a more experienced or skillful team member. On the other hand, a project manager may not be responsible for external risks. For example, a project manager would not be responsible or accountable if the project was cancelled because the organization sponsoring the project went bankrupt.

The distinction between internal and external risks is not always clear. For example, even though a particular hardware or software vendor may be external to the project, the project manager may still be responsible if that vendor is unable to deliver required technology resources. If the project manager chose that particular vendor, he or she would then be responsible or accountable for that risk. In short, a project manager will (or should) have control over internal risks, but not external risks. That distinction does not mean the project manager can ignore external risks. These risks can have a significant impact on the project, as well as the project manager's employment!

The fifth layer of the IT project risk management framework includes three different types of risks: **known risks, known-unknown risks,** and **unknown-unknown risks.** Wideman (1992) defines known risks as events that are going to occur. In short, these events are like death and taxes—they will happen and there is no uncertainty about it. On the other hand, known-unknowns are identifiable uncertainty. For example, if you own a home or rent an apartment, you know that you will receive a bill next month for the utilities you use. The precise amount you will owe the utility company will be unknown until you receive the actual bill. Unknown-unknown risks are residual risks or events that we cannot even imagine happening. For example, it was not too long ago that people had never even heard about the Internet. How could they comprehend the impact it would have on many of us? Unknown-unknown risks are really just a way to remind us that there may be a few risks remaining even after we may think we identified them all. In general, these are the risks that we identify after they have occurred.

The outer layer provides a time element in terms of the project life cycle. It may help us determine or identify when risks may occur, but also remind us that they may change over the life of the project. Although risk management is an important concern at the beginning of a project, the IT project risk management framework reminds us that we must be vigilant for opportunities and problems throughout the project life cycle.

Applying the IT Project Risk Management Framework

The GTS vignette at the beginning of the chapter can be analyzed using the process represented in Figure 8.1. For example, the risk faced by the GTS team could be defined as:

- A threat that occurred in the develop project charter and project plan phase.
- It was an unknown-unknown risk because it was identified after it occurred and, therefore, caught the GTS project team off guard.
- It was an external risk, and the project manager and project team should not be held responsible for the economic downturn experienced by Husky Air.

- The sources of risk to the GTS project include environment (economic), organizational (the client Husky Air) and people (if you would like to argue that Husky Air's management was lax in anticipating this problematic event).
- The impact on the GTS project was significant because it would affect the project's scope, schedule, and budget. Since Tim Williams was able to renegotiate the contract based on a trimmed scope, we can assume that quality would not be an issue. But if Husky Air's management insisted on maintaining the original scope, schedule, and budget, chances are good that quality would become an issue, especially if, for example, the scheduled testing time had to be shortened in order to meet the scheduled deadline.
- It is likely that the project's MOV would change as well because the project team would not complete the scope as originally planned. This, in turn, would determine the revised scope, schedule, and budget for the project.

This example shows how a risk can be understood after it occurs. The framework can also be used to proactively identify IT project risks. For example, a project team could begin with the project phases defined in the outer core of the framework. Using the project's work breakdown structure (WBS) and the individual work packages, the team could identify the risks for each of the work packages under the various project phases. Again, it is important that both threats and opportunities be identified. These risks could be classified as either known risks or known-unknown risks. The category of unknown-unknown risks should serve as a reminder to keep asking the question, What other threats or opportunities have we not thought about? Hopefully, the project team will do a more thorough job of identifying risks early in the project and reduce the likelihood of being surprised later.

The risks identified by the team can then be categorized as external or internal to the project. The internal risks are the direct responsibility of the project manager or team, while external risks may be outside their control. Regardless, both external and internal risks must be monitored and responses should be formulated.

The next step involves identifying the various sources of risk. Instead of trying to neatly categorize a particular risk, it may be more important to understand how the sources of risk are interrelated with each other. In addition, it may be a situation where precise definitions get in the way of progress. Instead of arguing or worrying about the exact source of a particular risk, it is more important the stakeholders understand the complex nature of a risk. Each risk-source category may mean different things to different stakeholders. Depending on the project, the stakeholders should be free to develop their own definitions and interpretations for each risk source category. They should also feel free to add categories, as needed.

After identifying the nature and characteristics of a particular risk, the project team can assess how a particular risk will impact the project. At this point, the team should focus on the project objectives that would be impacted if a particular risk occurred and, in turn, whether the project's MOV or goal would be impacted. Later on, these risks can be assessed to determine how the objectives will be impacted.

The above example shows how, working from the outside and then inward toward the center of the model, risks can be identified using the IT project risk framework. This procedure works well as a first pass and when using the project plan or WBS as a source of input. Many threats and opportunities may, however, be overlooked when relying only on the WBS.

The project team could start with the inner core of the IT risk framework and work outward. For example, the project team could identify how the MOV may be

affected in terms of threats or opportunities that affect the project's scope, schedule, budget, or quality. Working away from the center, the team could identify possible sources of risk and then categorize whether the risk is internal or external, known, known-unknown, or unknown-unknown (i.e., did we miss something?), and when during the project life cycle this particular risk might occur.

Tools and Techniques

Identifying risks is not always easy. Risks tend to be interrelated and identifying each and every risk may not be possible or economically feasible. People may not want to admit that potential problems are possible for fear of appearing incompetent. As a result, stakeholders may deny or downplay a particular risk. Still, people and organizations have different tolerances for risk, and what may be considered a normal risk for one stakeholder or organization may be a real concern for another. So, the stakeholders may concentrate on a particular risk (that may or may not occur) at the expense of other risks that could have the same impact on the project.

It is, therefore, important that the project manager and team guide the risk management process. Risk identification should include the project team and other stakeholders who are familiar with the project's goal and objectives. Using one or more of the following tools, the IT project risk framework introduced earlier in this section can provide direction for identifying the threats and opportunities associated with the project:

- *Learning Cycles*—The concept of learning cycles was introduced in Chapter 4. The project team and stakeholders can use this technique, whereby they identify facts (what they know), assumptions (what they think they know), and research (things to find out), to identify various risks. Using these three categories, the group can create an action plan to test assumptions and conduct research about various risks. Based on the team's findings, both risks and lessons learned can then be documented.
- *Brainstorming*—Brainstorming is a less structured activity than learning cycles. Here the team could use the IT risk framework and the WBS to iden tify risks (i.e., threats and opportunities) starting with the phases of the project life cycle and working towards the framework's core or MOV or working from the MOV outward toward the project phases. The key to brainstorming is encouraging contributions from everyone in the group. Thus, initially ideas must be generated without being evaluated. Once ideas are generated by the group as a whole, they can be discussed and evaluated by the group.
- *Nominal Group Technique (NGT)*—The NOT is a structured technique for identifying risks that attempts to balance and increase participation (Delbecq and Van de Van 1971). Using the NGT:

    a. Each individual silently writes her or his ideas on a piece of paper.
    b. Each idea is then written on a board or flip chart one at a time in a round-robin fashion until each individual has listed all of his or her ideas.
    c. The group then discusses and clarifies each of the ideas.
    d. Each individual then silently ranks and prioritizes the ideas.
    e. The group then discusses the rankings and priorities of the ideas.
    f. Each individual ranks and prioritizes the ideas again.

g. The rankings and prioritizations are then summarized for the group.

Delphi Technique—If the time and resources are available, a group of experts can be assembled—without ever having to meet face-to-face. Using the Delphi technique, a group of experts are asked to identify potential risks or discuss the impact of a particular risk. Initially, in order to reduce the potential for bias, the experts are not known to each other. Their responses are collected and made available anonymously to each other. The experts are then asked to provide another response based upon the previous round of responses. The process continues until a consensus exists. The advantage of using the Delphi technique is the potential for getting an insightful view into a threat or opportunity; but the process takes time and may consume a good portion of the project's resources.

Interviewing—Another useful technique for identifying and understanding the nature of IT project risks is to interview various project stakeholders. This technique can prove useful for determining alternative points of view; but the quality of the information derived depends heavily on the skills of the interviewer and the interviewees, as well as the interview process itself.

Checklists—Checklists provide a structured tool for identifying risks that have occurred in the past. They allow the current project team to learn from past mistakes or to identify risks that are known to a particular organization or industry. One problem with checklists is that they can lead to a false sense of security—i.e., if we check off each of the risks on the list, then we will have covered everything. Table 8.2 provides an example of items that may be included in a project risk checklist.

Table 8.2 Example of an IT Project Check List

Risk Checklist
✔ Funding for the project has been secured.
✔ Funding for the project is sufficient.
✔ Funding for the project has been approved by senior management.
✔ The project team has the requisite skills to complete the project.
✔ The project has adequate manpower to complete the project.
✔ The project charter and project plan have been approved by senior management or the project sponsor.
✔ The project's goal is realistic and achievable.
✔ The project's schedule is realistic and achievable.
✔ The project's scope has been clearly defined.
✔ Processes for scope changes have been clearly defined.

**SWOT Analysis*—*SWOT* stands for Strengths, Weaknesses, Opportunities, and Threats. Brainstorming, NOT, or the Delphi technique could be used to identify and understand the nature of IT project risks by categorizing risks using the frame work illustrated in Figure 8.3. The usefulness of using SWOT analysis is that it allows the project team to identify threats and opportunities as well as their nature in terms of project or organizational strengths and weaknesses.

**Cause-and-Effect Diagrams*—The most widely known and used cause-and-effect diagram is the fishbone, or Ishikawa, diagram developed by Kaoru Ishikawa to analyze the causes of poor quality in manufacturing systems. The diagram can also be used for understanding the causes or factors of a particular risk, as well as its effects. An example of an Ishikawa diagram is illustrated in Figure 8.4. The diagram shows the possible causes and effects of a key member of the team leaving the project. This technique itself can be used individually or in groups by using the following steps:

a. Identify the risk in terms of a threat or opportunity.

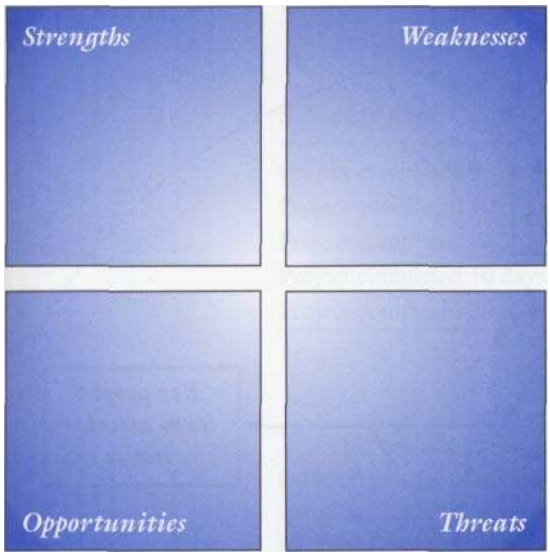


Figure 8.3 SWOT Analysis—Strengths, Weaknesses, Opportunities, and Threats

b. Identify the main factors that can cause the risk to occur.
c. Identify detailed factors for each of the main factors.
d. Continue refining the diagram until satis fied that the diagram is complete.

Past Projects—One of the themes in this text has been the integration of knowledge management to support the project management processes. Lessons learned from past projects can provide insight and best practices for identifying and understanding the nature of IT project risks. The usefulness of these lessons takes time and a commitment by the organization and project team to develop a base of knowledge from past projects. The value of this knowledge base will increase as the base does, allowing project teams to learn from the mistakes and successes of others.

RISK ANALYSIS AND ASSESSMENT

The framework introduced in the previous section provides tools for identifying and understanding the nature of risks to IT projects. The next step requires that those risks be analyzed to determine what threats or opportunities require attention or a response. Risk analysis and assessment provides a systematic approach for evaluating the risks that the project stakeholders identify. The purpose of **risk analysis** is to determine each identified risk's probability and impact on the project. **Risk assessment,** on the other hand, focuses on prioritizing risks so that an effective risk strategy can be formulated. In short, which risks require a response? To a great degree, this will be determined by the project stakeholders' tolerances to risk.

There are two basic approaches to analyzing and assessing project risk. The first approach is more qualitative in nature because it includes subjective assessments based on experience or intuition. Quantitative analysis, on the other hand, is based on mathematical and statistical techniques. Each approach has its own strengths and weaknesses when dealing with uncertainty, so a combination of qualitative and quantitative methods provides valuable insight when conducting risk analysis and assessment.

Qualitative Approaches

Qualitative risk analysis focuses on a subjective analysis of risks based upon a project stakeholder's experience or judgment. Although the techniques for analyzing project risk qualitatively can be conducted by individual stakeholders, it may be more effective if done by a group. This group process allows each stakeholder to hear other points of view and supports open communication among the various stakeholders. As a result, a broader view of the threats, opportunities, issues, and points of view can be discussed and understood.

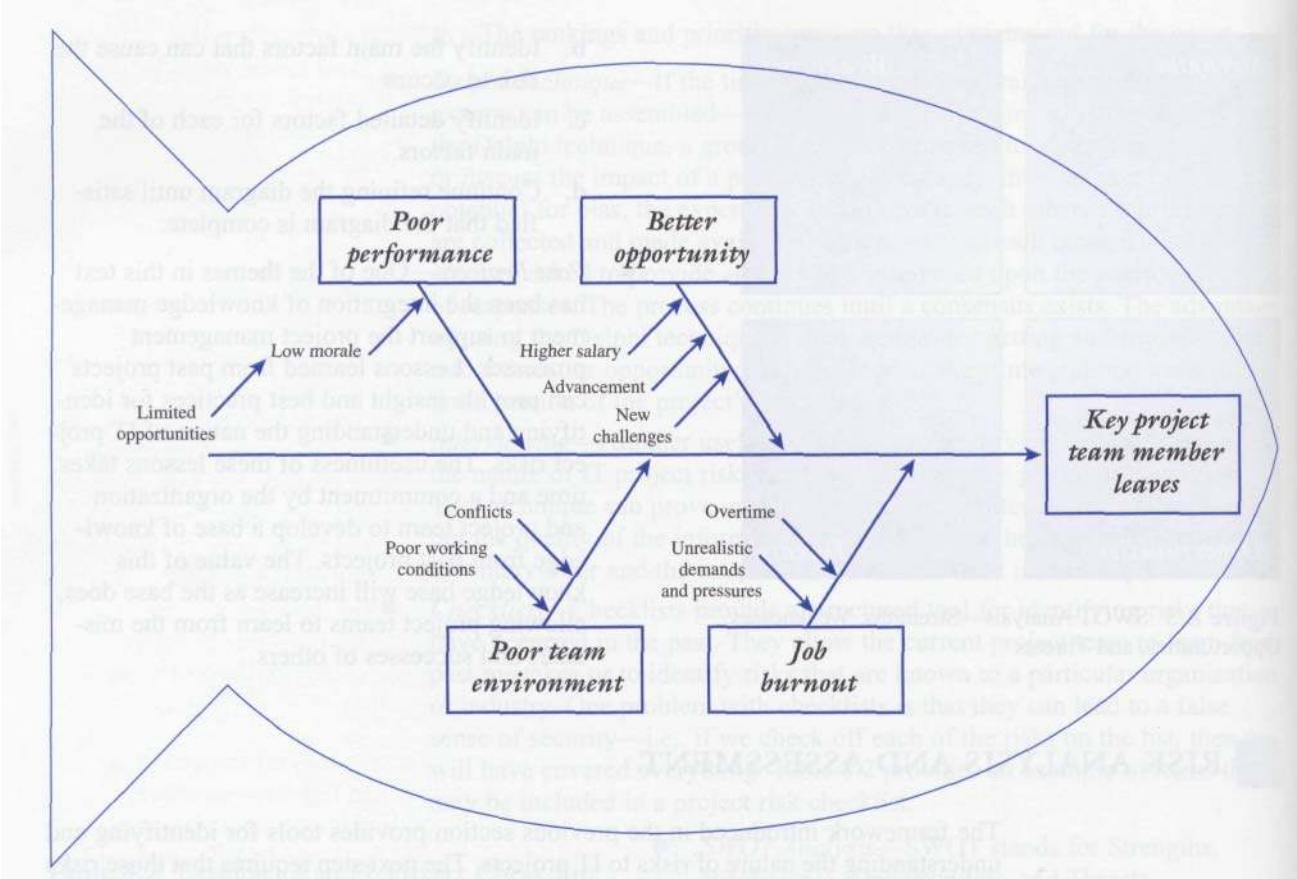


Figure 8.4 Cause and Effect Diagram

Expected Value The concept of **expected value** provides the basis for both qualitative and quantitative risk analysis. Expected value is really an average, or mean, that takes into account both the probability and impact of various events or outcomes. For example, let's assume that a project manager of a consulting firm would like to determine the expected return or payoff associated with several possible outcomes or events. These outcomes or events, in terms of possible schedule scenarios, determine the return or profit the project will return to the consulting firm. The project manger believes each outcome has a probability of occurring and an associated payoff. The project manager's subjective beliefs are summarized in a **payoff table** in Table 8.3.

As you can see from Table 8.3, the project manager believes that the project has a small chance of finishing twenty days early or twenty days late. The payoff for finishing the project early is quite high, but there appears to be a penalty for completing the project late. As a result, the expected value or return to the consulting firm is $88,000. Since each event is mutually exclusive (i.e., only one of the five events can occur), the probabilities must sum to 100 percent.

Decision Trees Similar to a payoff table, a **decision tree** provides a visual, or graphical, view of various decisions and outcomes. Let's assume that a project is going to overrun its schedule and budget. The project manager is contemplating reducing the time allocated to testing the application system as a way of bringing the project back within its original schedule and budget objectives.

Table 8.3 Expected Value of a Payoff Table

Schedule Risk	*A Probability*	*B Payoff (in thousands)*	*A • B Prob • Payoff (in thousands)*
Project completed 20 days early	5%	$ 200	$ 10
Project completed 10 days early	20%	$ 150	$ 30
Project completed on schedule	50%	$ 100	$ 50
Project completed 10 days late	20%	$ –	$ –
Project completed 20 days late	5%	$ (50)	$ (3)
	100%		

The project manager, then, is faced with a decision about whether the project team should conduct a full systems test as planned or shorten the time originally allocated to testing. The cost of a full test will be $10,000; but the project manager believes that there is a 95 percent chance the project will meet the quality standards set forth by the client. In this case, no additional rework will be required and no additional costs will be incurred. Since there is only a 5 percent chance the system will not meet the standards, the project manager believes that it would only require a small amount of rework to meet the quality standards. In this case, it will cost about $2,000 in resources to bring the system within standards.

On the other hand, the shortened test will cost less than the full test and bring the project back on track. But, if the project team limits the testing of the system, it will very likely lower the probability of the system meeting the quality standards. Moreover, a failure will require more rework and cost more to fix than if these problems were addressed during a full testing of the system. As you can see from Figure 8.5, a limited testing of the system will cost only $8,000, but the chances of the system failing to meet the quality standards increase. Moreover, the time and cost to complete the rework will be higher.

Even though the project manager still has a difficult decision to make, it now becomes a more informed decision. If the project team continues with the testing activities as planned, there is a very good chance that the system will not require a great deal of rework. On the other hand, reducing the time to test the system is more of a gamble. Although there is a 30 percent chance the limited testing will save both time and money, there is a high probability that the system will not pass or meet the quality standards. As a result, the required rework will make the project even later and more over its budget. If you were the project manager, what decision would you make?

Risk Impact Table We can create a **risk impact table** to analyze and prioritize various IT project risks. Let's use another example. Suppose a project manager has identified seven risks that could impact a particular project.

The left-hand column of Table 8.4 lists the possible risks that were identified using the IT project risk framework introduced in the last section. For simplicity, we will focus only on risks in terms of threats, but opportunities could be analyzed and assessed using the same technique.

The second column lists the subjective probabilities for each of the risks. In this case, the probabilities do not sum to 100 percent because the risks are not mutually exclusive. In other words, none, some, or all of the risk events could occur. A probability of zero indicates that a probability has absolutely no chance of occurring, while

a probability of 100 percent indicates an absolute certainty that the event will occur. The next column provides the potential impact associated with the risk event occurring. This also is a subjective estimate based on a score from 0 to 10, with zero being no impact and ten having a very high or significant impact on the project.

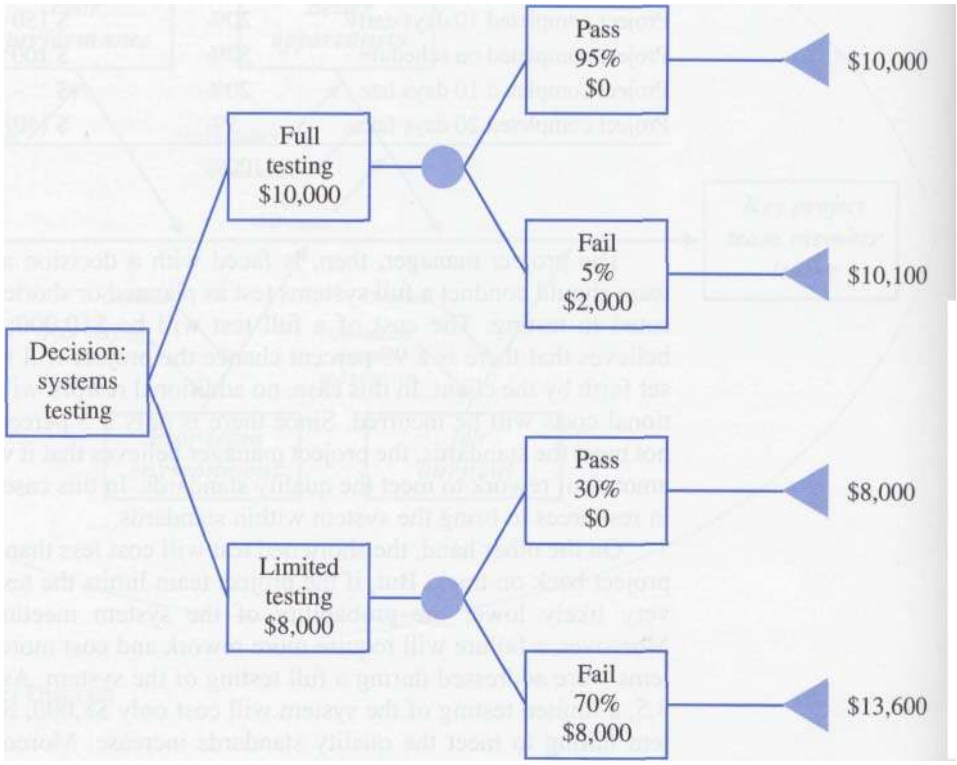


Figure 8.5 Decision Tree Analysis

Table 8.4 IT Project Risk Impact Analysis

Risk (Threats)	*0–100% Probability*	*0–10 Impact*	*P • I Score*
Key project team member leaves project	40%	4	1.6
Client unable to define scope and requirements	50%	6	3.0
Client experiences financial problems	10%	9	0.9
Response time not acceptable to users/client	80%	6	4.8
Technology does not integrate with existing application	60%	7	4.2
Functional manager deflects resources away from project	20%	3	0.6
Client unable to obtain licensing agreements	5%	7	0.4

Once a probability and an impact are assigned to each risk event, they are multiplied together to come up with a risk score. Although this score is based on the subjective opinions of the project stakeholders, it does provide mechanism for determining which risks should be monitored and which risks may require a response. Once a risk score is computed for each risk, the risks can be prioritized as in Table 8.5.

Table 8.5 shows that "Response time not acceptable to users/client" and "Technology does not integrate with existing application" are the two most significant risks to this project. The risk scores for all of the risks include the stakeholders risk tolerances and preferences since the subjective probabilities and impacts will reflect these tolerances and preferences.

The risk scores can be further analyzed using a risk classification scheme introduced by Robert Tusler (Tusler 1998). Figure 8.6 shows how the risk analysis can be used to classify the different risks.

As you can see in Figure 8.6, each risk from Table 8.4 is plotted against its probability and potential impact. Tusler suggests that risks can be classified according to the four quadrants:

- *Kittens*—Risks that have a low probability of occurring and a low impact on the project. These risks are rarely a source of trouble and, therefore, a great deal of time and resources should not be devoted to responding to these threats. Similarly, these types of opportunities are not worth pursuing since they offer little payback and have little chance of fruition.
- *Puppies*—Puppies are similar to kittens, but can become a source of prob lems very quickly because they have a high probability of occurring. Like the risks that they represent, puppies can grow into large troublesome dogs unless they are trained properly. Similarly, these types of risks must be watched so that corrective action can be taken before they get out of hand.
- *Tigers*—These types of risks have a high probability of occurring and a high impact. Similar to the dangerous animals they represent, they must be neutralized as soon as possible.
- *Alligators*—Alligators are not a problem if you know where they are, other wise, they can be. These risks have a low probability of occurring, but a high impact if they do. These types of risks can be avoided with care.

Table 8.5 Risk Rankings

Risk (Threats)	*Score*	*Ranking*
Response time not acceptable to users/client	4.8	1
Technology does not integrate with existing application	4.2	2
Client unable to define scope and requirements	3.0	3
Key project team member leaves project	1.6	4
Client experiences financial problems	0.9	5
Functional manager deflects resources away from project	0.6	6
Client unable to obtain licensing agreements	0.4	7

Quantitative Approaches

Quantitative approaches to project risk analysis include mathematical or statistical techniques that allow us to model a particular risk situation. At the heart of many of these models is the probability distribution. Probability distributions can be continuous or discrete.

Discrete Probability Distributions **Discrete probability distributions** use only integer or whole numbers where fractional values are not allowed or do not make sense. For example, flipping a coin would allow for only two outcomes— heads or tails. If you wanted to find the

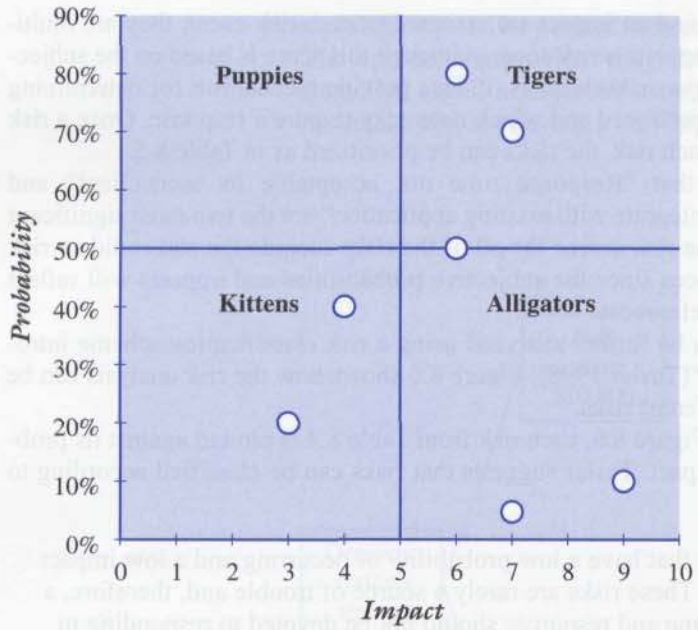


Figure 8.6 Tusler's Risk Classification Scheme

probability of flipping a fair coin into the air and having the outcome of the coin landing with the heads side up, just divide the number of favorable events (heads) by the number of total outcomes (heads or tails). This results in a ½ or 50 percent probability of the coin coming up heads. Since these events (heads or tails) are mutually exclusive and exhaustive (one and only one of these events will occur), the probability of tails is 50 percent (i.e., 100 percent − 50 percent = 50 percent). Probabilities must be positive and the sum of all of the event probabilities must sum to one.

If you were to flip a coin repeatedly a few hundred times and then record the outcomes, you would end up with a distribution similar to Figure 8.7.

Continuous Probability Distributions

Continuous probability distributions are useful for developing risk analysis models when an event has an infinite number of possible values within a stated range. Although in theory there are an infinite number of probability distributions, we will discuss three of the more common continuous probability distributions used in modeling risk. These include the **Normal Distribution, the PERT distribution,** and the **triangular distribution.** A quick overview shows how these distributions may be used to develop models for simulation or sensitivity analysis.

One of the most common continuous probability distributions is the normal distribution, or Bell Curve. Figure 8.8 provides an example of a normal distribution.

The normal distribution has the following properties:

- The distribution's shape is determined by its mean (μ) and standard deviation (σ). In Figure 8.8, this particular distribution has a mean of 0 and a standard deviation of 1. Other combinations of means and standard deviations will result in normal distributions with shapes that are either flatter or taller.

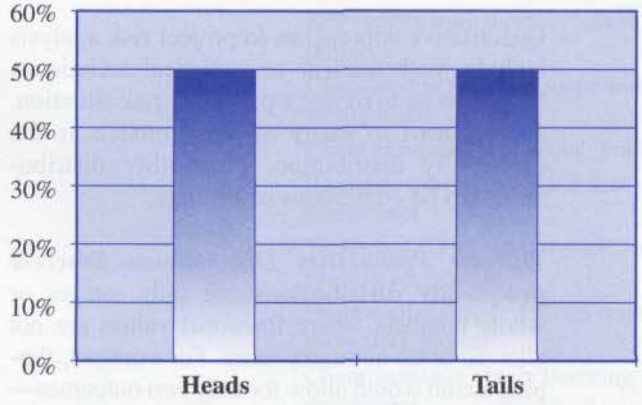
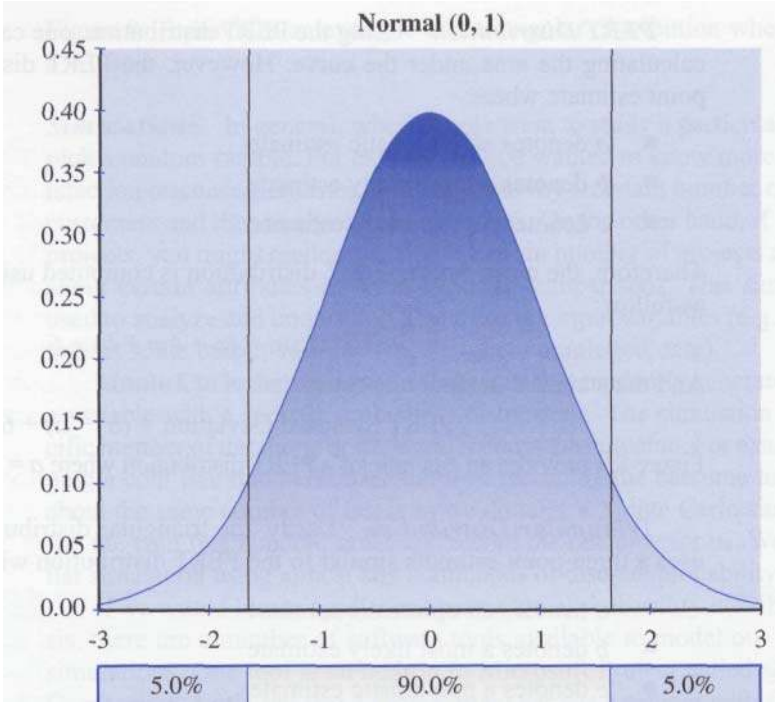


Figure 8.7 Binomial Probability Distribution

- Probability is associated with area under the curve. Therefore, the total area under the curve and the baseline that extends from negative infinity (− ∞) to positive infinity (+ ∞) is 100 percent. Subsequently, to find the probability of an event occurring between any two points on the baseline, just find the area between those two points under the curve. This is done by standardizing a given value for X using the formula: $z = (X - \mu) \div \sigma$ to obtain a z score. A table with the various z scores is then used to compute the probability for the area between any two z scores.



-1.6448 **Figure** 1.6448

8.8 Normal Distribution

- Since the normal distribution is symmetrical around the mean, an outcome that falls between $-\infty$ and the mean, μ, would have the same probability of falling between the mean, μ, and $+\infty$ (i.e., 50 percent).
- Since the distribution is symmetrical, the following probability rules of thumb apply
  - About 68 percent of all the values will fall between $\pm 1\sigma$ of the mean
  - About 95 percent of all the values will fall between $\pm 2\sigma$ of the mean
  - About 99 percent of all the values will fall between $\pm 3\sigma$ of the mean

Therefore, if we know or assume that the probability of a risk event follows a normal distribution, we can predict an outcome with some confidence. For example, let's say that a particular project task has a mean duration of ten days. Moreover, over time we have been able to determine that this particular task has a standard deviation of two days. The mean tells us that if we were to complete this particular task over and over again, we would expect to complete this task, on average, in ten days. If we always completed the task in ten days, there would be no variability and the standard deviation would be zero. If, however, the task sometimes took anywhere between six and fifteen days to complete, we would have some variability, and the standard deviation would be a value greater than zero. The more variability we have, the larger is the computed standard deviation.

Using the rules of thumb described above, we could estimate, for example, that we would be about 95 percent certain that the project's task would be complete within six to fourteen days ($\mu \pm 2\ \sigma = 10 \pm 2 \times 2$). In addition, we could also say that we would be about 99 percent confident that the task would be completed between four and sixteen days ($\mu \pm 3\sigma = 10 \pm 3 \times 2$).

PERT Distribution Using the PERT distribution, one can find a probability by calculating the area under the curve. However, the PERT distribution uses a three-point estimate where:

- a denotes an optimistic estimate
- b denotes a most likely estimate
- c denotes a pessimistic estimate

Therefore, the mean for the PERT distribution is computed using a weighted average as follow:

$$\text{PERT Mean} = (a + 4m + b) \div 6$$

And the standard deviation is computed:

$$\text{PERT Standard Deviation} = (b - a) \div 6$$

Figure 8.9 provides an example of a PERT distribution where $a = 2$, $m = 4$, and $b = 8$.

Triangular Distribution Lastly, the triangular distribution, or TRIANG, also uses a three-point estimate similar to the PERT distribution where:

- a denotes an optimistic estimate
- b denotes a most likely estimate
- c denotes a pessimistic estimate

However, the weighting for the mean and standard deviation are different.

$$\text{TRIANG Mean} = (a + m + b) \div 3$$

$$\text{TRAING Standard Deviation} = [((b - a)^2 + (m - a)(m - b)) \div 18]^{1/2}$$

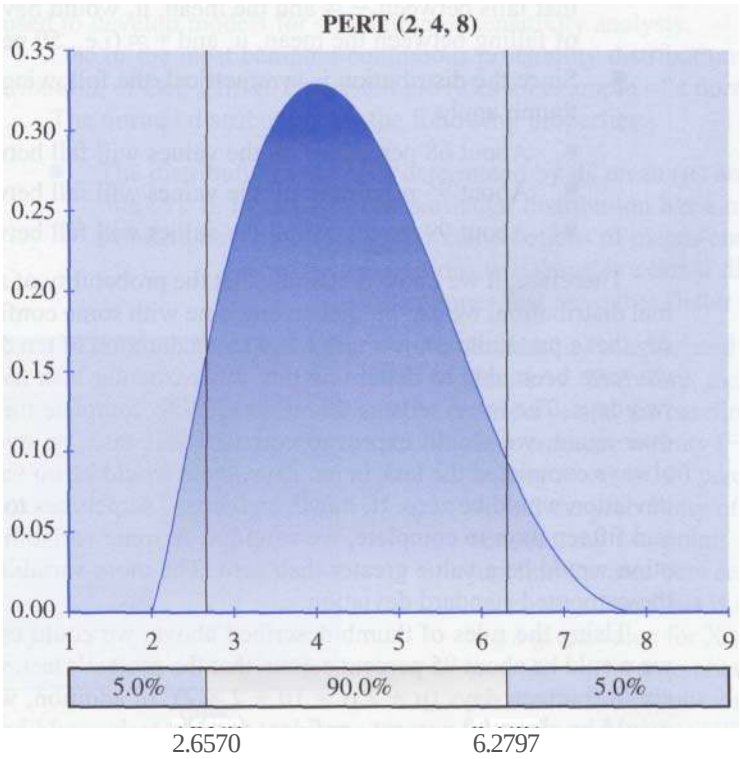


Figure 8.9 Example of a PERT Distribution

Figure 8.10 provides an example of a triangular distribution where $a = 4$, $m = 6$, and $b = 10$.

Simulations In general, when people want to study a particular phenomenon, they pick a random sample. For example, if you wanted to know more about customer satisfaction or consumer tastes, you could survey a certain number of randomly selected customers and then analyze their responses. On the other hand, if you wanted to study projects, you might randomly select a certain number of projects and then collect data about certain attributes in order to make comparisons. This same approach can be used to analyze and understand how different input variables (e.g., task durations) can impact some output variable (e.g., project completion date).

Monte Carlo simulation is a technique that randomly generates specific values for a variable with a specific probability distribution. The simulation goes through a specific number of iterations or trials and records the outcome. For example, instead of flipping a coin five hundred times and then recording the outcome to see whether we get about the same number of heads as we do tails, a Monte Carlo simulation can literally flip the coin five hundred times and record the outcome for us. We can perform a similar simulation using almost any continuous or discrete probability distribution.

If we would like to apply our knowledge of probability distributions to risk analysis, there are a number of software tools available to model our project and develop simulations. One tool is an add-on to Microsoft Project called @Risk™, by Palisade Corporation. Let's say that a project manager has a project with five tasks (A through E) and has created a project plan using Microsoft Project. As you can see from Figure 8.11, the project is estimated to be completed in sixteen days. However, each task has a level of uncertainty in terms of each task's estimated duration. Therefore, we can create a Monte Carlo simulation that will tell us how likely it is that the project will

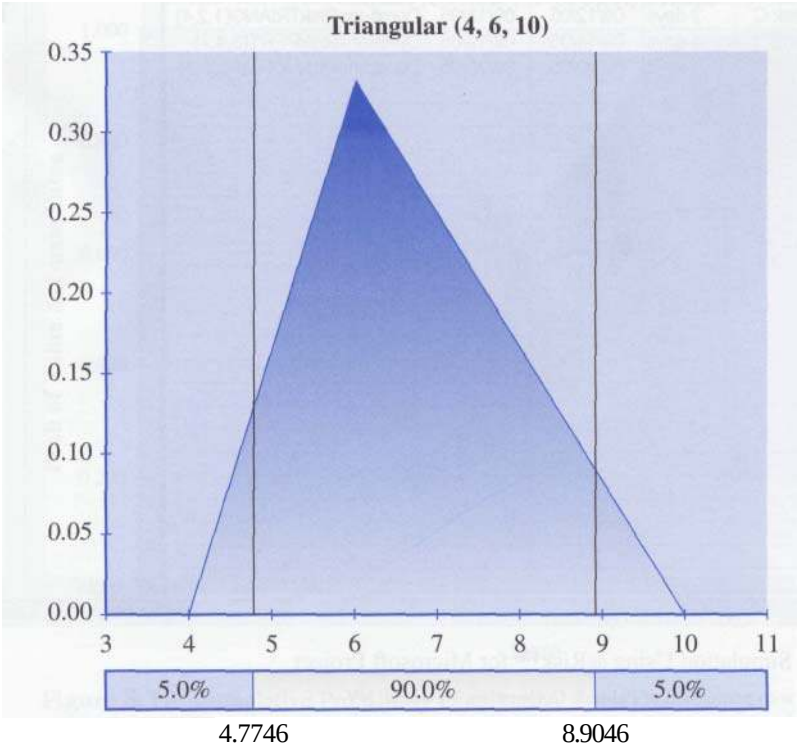


Figure 8.10 Example of a Triangular Distribution

be completed as planned. For example, Tasks A and D follow a PERT distribution, while Tasks B and C follow a triangular distribution. In addition, Task E follows a normal distribution. The distributions and values are listed in the @Risk Functions column created by the @Risk™ add-on.

The Monte Carlo simulation using @Risk™ was set to run five hundred iterations or trials. The output of this simulation is illustrated in Figure 8.12. Each bar in the histogram shows the frequency, or number of times, an iteration generated a particular completion date for the project based on the probability distributions for the five tasks.

Running the simulation using @Risk™, the project manager can assess the likelihood of the project finishing on September 26 (i.e., within the original sixteen-day estimate) by viewing a cumulative probability distribution (see Figure 8.13).

As you can see in Figure 8.13, the probability of completing the project on September 26—the end of the project manager's original sixteen-day estimate—is less than .200 or 20 percent.

In addition, the project manager can conduct a sensitivity analysis to determine the tasks that entail the greatest risk. Figure 8.14 illustrates a **tornado graph,** which summarizes the tasks with the most significant risks at the top. As the risks are ranked

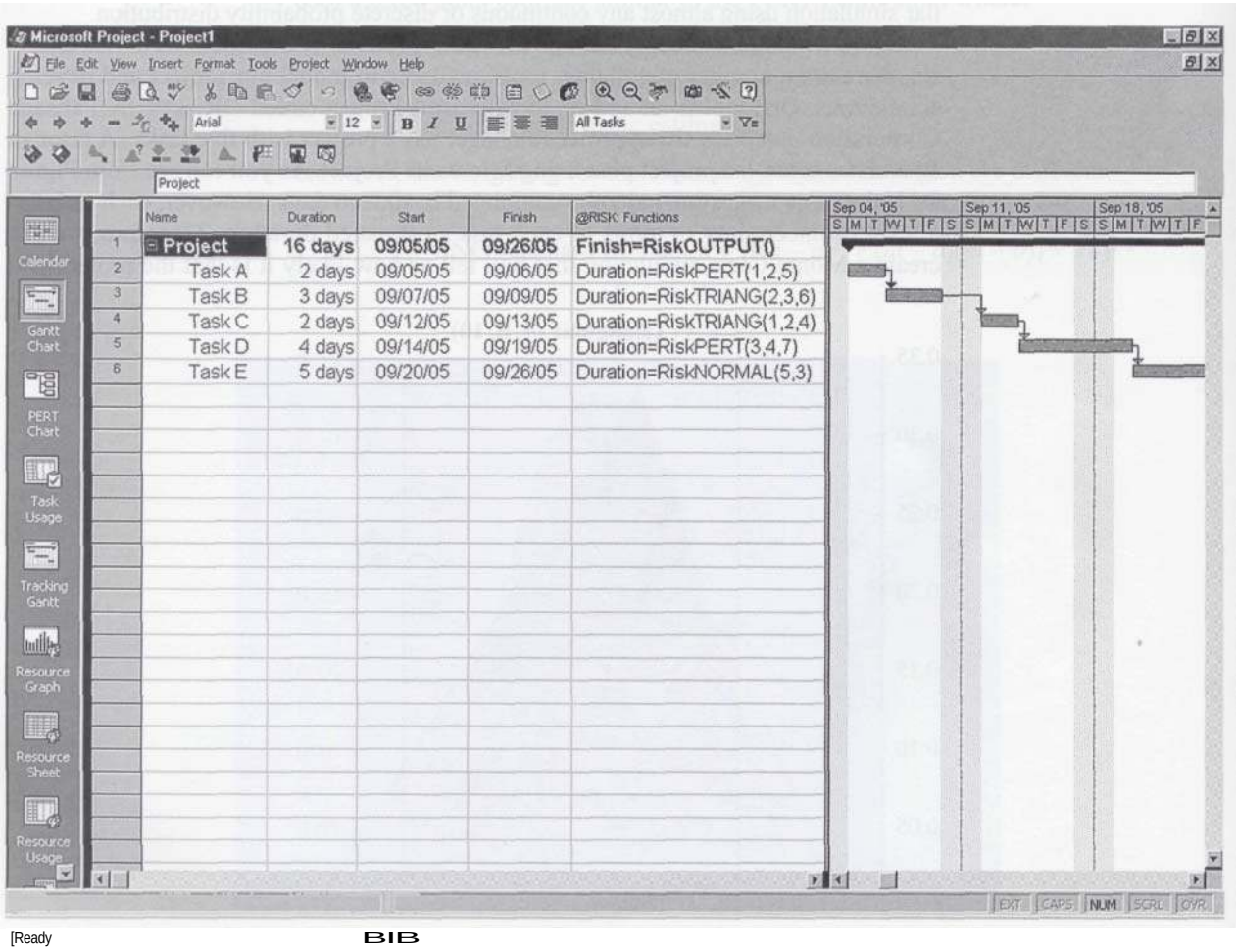


Figure 8.11 Risk Simulation Using @Risk™ for Microsoft Project

SOURCE: @Risk is used with permission of Palisade Corporation, Newfield, NY

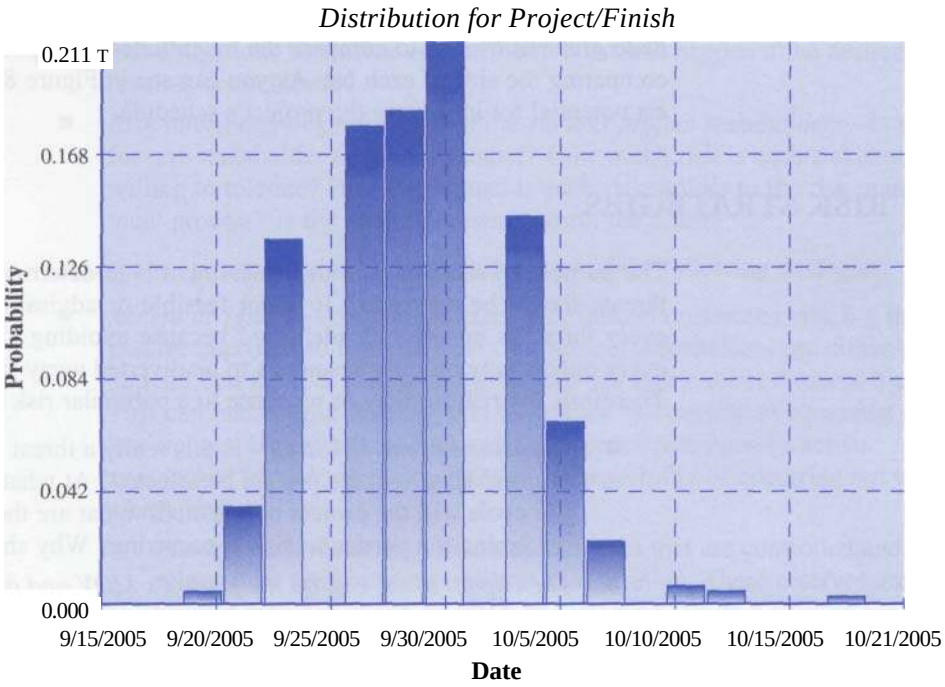


Figure 8.12 Output from Monte Carlo Simulation

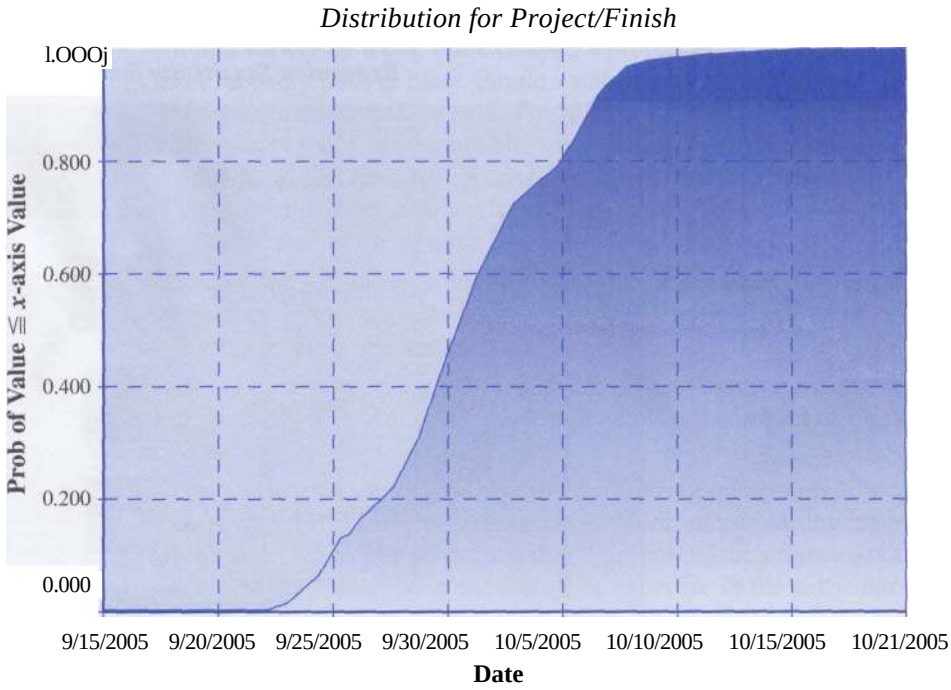


Figure 8.13 Cumulative Probability Distribution

from highest to lowest, the bars of the graph sometimes resemble a tornado. The tornado graph allows us to compare the magnitudes of impact for each of the tasks by comparing the size of each bar. As you can see in Figure 8.14, Task E has the greatest potential for impacting the project's schedule.

RISK STRATEGIES

The purpose of risk analysis and assessment is to determine what opportunities and threats should be addressed. It is not feasible or advisable to respond to each and every threat or opportunity identified because avoiding all threats or chasing after every opportunity requires resources to be diverted away from the real project work. Therefore, the risk strategy or response to a particular risk depends on:

- *The nature of the risk itself— Is* this really a threat to or opportunity for the project? How will the project be affected? At what points during the project life cycle will the project be affected? What are the triggers that would determine if a particular risk is occurring? Why should the risk be taken?
- *The impact of the risk on the project's MOV and objectives* — A risk has a probability and an impact on the project if it occurs. What is the likelihood of this occurring? And if this risk occurs, how will the project be affected? What can be gained? What could be lost? What are the chances of success or failure?
- *The project s constraints in terms of scope, schedule, budget, and quality requirements* — Can a response to a particular threat or opportunity be made within the available resources and constraints of the project? Will additional

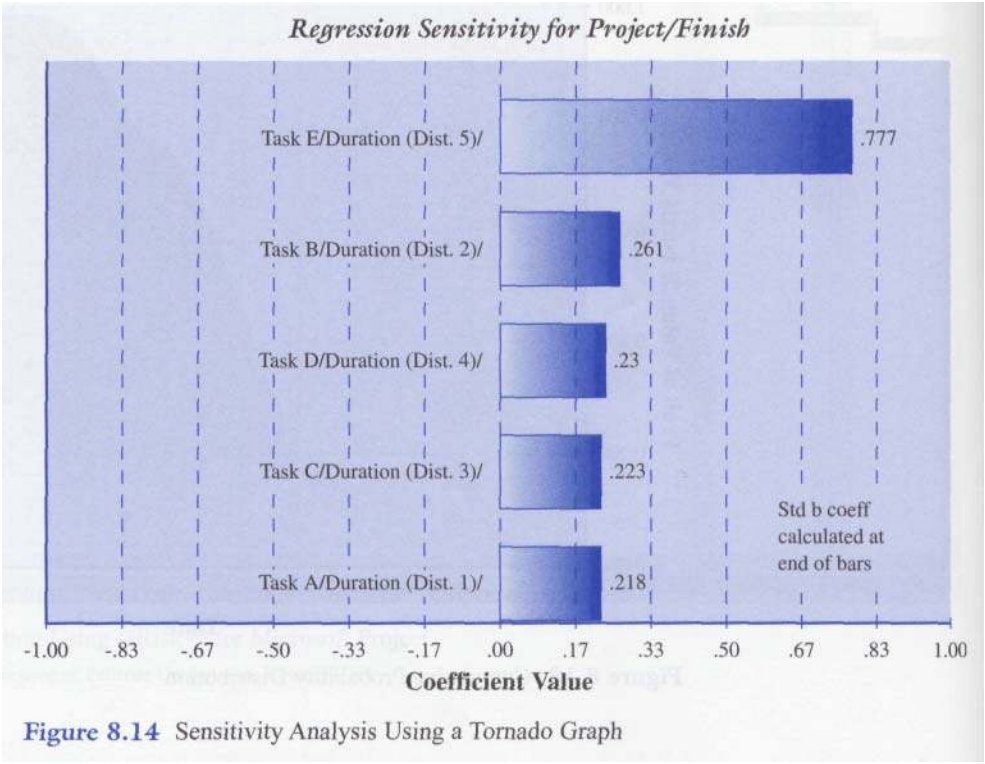


Figure 8.14 Sensitivity Analysis Using a Tornado Graph

resources be made available if a particular risk occurs? Can certain contractual obligations be waived or modified? What will happen if the desired result is not achieved?

- *Risk tolerances or preferences of the various project stakeholders*—Is a risk for one stakeholder a risk for another? How much risk is each stakeholder willing to tolerate? How committed is each stakeholder to the risk manage ment process? Is the potential reward worth the effort?

A response to a particular risk may follow one of the following strategies:

- *Accept or Ignore*—Choosing to accept or ignore a particular risk is a more passive approach to risk response. The project stakeholders can either be hopeful that the risk will not occur or just not worry about it unless it does. This can make sense for risks that have a low probability of occurring or a low impact. However, reserves and contingency plans can be active approaches for risks that may have a low probability of occurring but with a high impact.

  Management Reserves—These are reserves that are controlled and released by senior management at its discretion. These reserves are not usually included in the project's budget, but provide a cushion for dealing with the unexpected.

  * *Contingency Reserves*—A contingency reserve is usually controlled and released within specific guidelines by the project manager when a particular risk occurs. This reserve is usually included in the project's budget.

  Contingency plans—Sometimes called an alternative plan, or *Plan B,* this plan can be initiated in the event a particular risk occurs. Although these types of plans are viewed as plans of last resort, they can be useful in a variety of ways. For example, a project team should have a disaster recovery plan in place should a natural disaster, such as a hurricane or earthquake, occur. This plan may have procedures and processes in place that would allow the project team to continue to work should its present workplace become unusable or unavailable. This type of disaster recovery plan is only useful if it is up-to-date and communicated to the various project stakeholders.
- *Avoidance*—The avoidance strategy focuses on taking steps to avoid the risk altogether. In this case, an active approach is made to eliminate or pre vent the possibility of the threat occurring.
- *Mitigate*—The term *mitigate* means to lessen. Therefore, a mitigation risk strategy focuses on lessening the probability and/or the impact of threat if it does occur.
- *Transfer*—A transfer strategy focuses on transferring ownership of the risk to someone else. This transfer could be in the form of purchasing insurance against a particular risk or subcontracting a portion of the project work to someone who may have more knowledge or expertise in the particular area. As a result, this strategy may result in a premium, or added cost, to manag ing and responding to the risk.

Once the project risks and strategies are identified, they can be documented as part of the **risk response plan.** This plan should include the following:

- The project risk

- The trigger which flags that the risk has occurred
- The owner of the risk (i.e., the person or group responsible for monitoring the risk and ensuring that the appropriate risk response is carried out)
- The risk response based on one of the four basic risk strategies

The risk response plan can be developed using a template, such as the one illustrated in Figure 8.15.

RISK MONITORING AND CONTROL

Once the risk response plan is created, the various risk triggers must be continually monitored to keep track of the various IT project risks. In addition, new threats and opportunities may present themselves over the course of the project, so it is important that the project stakeholders be vigilant.

Risk monitoring and control should be part of the overall monitoring and control of the project. Monitoring and control focus on metrics to help identify when a risk occurs, and also on communication. The next chapter addresses how important it is to have a good monitoring and control system that supports communication among the various stakeholders and provides information essential to making timely and effective decisions.

Risk monitoring and control are analogous to a radarscope, as Figure 8.16 shows. Threats and opportunities present themselves at different times. Some are on the horizon, while others are closer to affecting the project's MOV and objectives.

Various tools exist for monitoring and controlling project risk. These include:

- *Risk Audits*—A knowledgeable manager or group can be useful for auditing the project team from time to time. The audit should focus on ensuring that the project manager and team have done a good job of identifying and ana lyzing project risks and on ensuring that proper procedures and processes are in place. Risk audits should be conducted by people outside the project team. Using outsiders provides a fresh perspective; the project team may be too close to the project and miss significant threats or opportunities.
- *Risk Reviews*—Risk audits should be conducted by individuals outside the project team; but risk reviews can be conducted internally. Throughout the project life cycle, the project stakeholders should hold scheduled, periodic risk reviews. These reviews should be part of each team meeting and part of the project team's learning cycles.
- *Risk Status Meetings and Reports*—Similar to risk reviews, a monitoring and control system should provide a formal communication system for monitoring and controlling project risks.

Risk	*Trigger*	*Owner*	*Response*	*Resources required*

Figure 8.15 Template for a Risk Response Plan

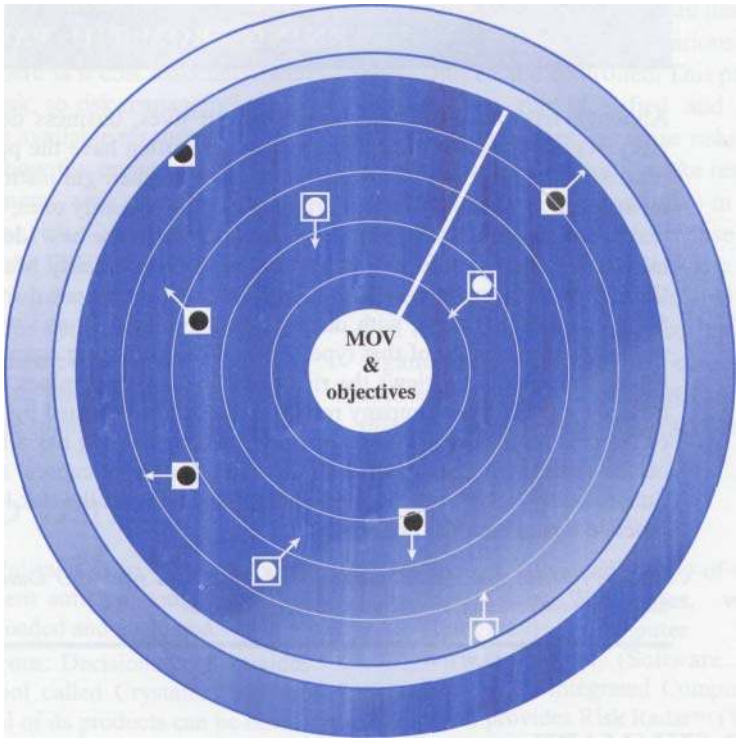


Figure 8.16 Project Risk Radar

RISK RESPONSE AND EVALUATION

The risk triggers defined in the risk response plan provide risk metrics for determining whether a particular threat or opportunity has occurred. A system for monitoring and controlling risk provides a mechanism for monitoring these triggers and for supporting communication among the various risk owners. The risk owners must be vigilant in watching for these triggers.

When a trigger occurs, the project risk owner must take appropriate action. In general, the action is responding to the risk as outlined in the risk response plan. Adequate resources must be available and used to respond to the risk.

The outcome of the risk response will either be favorable or unfavorable. Therefore, a great deal can be learned about the entire process of risk management (i.e., the preparedness of risk planning, identifying risks, analyzing and assessing risks, risk responses, and so forth). Lessons learned can lead to the identification of best practices that can be shared throughout the project organization. In summary, lessons learned and best practices help us to:

- Increase our understanding of IT project risk in general.
- Understand what information was available to managing risks and for mak ing risk-related decisions.
- Understand how and why a particular decision was made.
- Understand the implications not only of the risks but also the decisions that were made.
- Leam from our experience so that others may not have to repeat our mistakes.

LEARNING FROM THE PAST

Although risk pervades every aspect of our lives, business decisions can be particularly risky. As most people know, the greatest risks often have the potential for the highest payoffs. Although executives may use anything from their gut instincts to statistical and actuarial analysis to separate the smart risks from the foolhardy ones, in the end it conies down to making a decision. Unfortunately, most smart risks are best identified using hindsight, and taking risks that you do not understand is foolish. Fidelity Management Trust Company's Chief Risk Officer, James Lam, helped develop a risk event log in which every loss over $5,000 is entered, along with details about the incident and what controls are in place to reduce the probability of that type of loss from occurring again. At the end of each month, senior management reviews the risk event log and determines whether any additional controls are needed. The company reported that losses declined by 85 percent within two years of the creation of the risk log. Lam says that the risk log has allowed the company to focus on the right measures, understand the underlying root causes, and learn from its mistakes. Subsequently, other units within Fidelity have adopted the risk log, and it has become a best practice throughout the organization.

SOURCE: Adapted from Lauren Gibbons Paul, High Wire Acts, *CIO Enterprise Magazine,* June 15, 1998. http://www.cio.com/archive/enterprise/061598_risk.html

CHAPTER SUMMARY

This chapter introduced the processes and concepts of project risk management. Risk is an inherent component of IT projects because the project plan is based on a number of estimates that reflect our understanding of the current situation, the information available, and the assumptions that must be made. But, events seldom go according to plan, so the project must adapt to an ever-changing environment. Our inability to predict the future with 100 percent accuracy coupled with a dynamic environment create degrees of uncertainty or risk that must be addressed and managed throughout the project life cycle.

Although risk implies a negative connotation, project stakeholders must be vigilant in identifying opportunities presented by risk. The Project Management Body of Knowledge (PMBOK) points out that project risk management provides a systematic process for identifying, analyzing, and responding to project risks. A project risk management approach should focus on maximizing the probability and impacts of positive events while minimizing the probability and impacts of negative events.

In this chapter, two IT risk management frameworks were introduced. The first framework focused on the IT project risk management processes. These seven steps or processes include risk planning, risk identification, risk assessment, risk strategies, risk monitoring and controlling, risk response, and risk evaluation.

Risk planning begins with a firm commitment by all the project stakeholders to a risk management approach. A great deal of this commitment should be in terms of commitments to following the processes and to provide adequate resources when responding to risk events.

Risk identification should include identifying both threats and opportunities. Since most risks are interrelated and can affect the project in different ways, the project stakeholders should take a broad view of project risks. A second framework was introduced in this section to help understand the nature and influence of various IT project risks. This IT project risk framework is illustrated in Figure 8.2. It aids the project stakeholders in identifying and understanding the nature and influence of various risks.

Risk assessment allows the project stakeholders to determine what risks require a response. The goal of project risk management is not to avoid each and every risk at all costs, but to make well-informed decisions as to which risks are worth taking and which risks require a response. A well-informed decision requires an analysis of the probability of a particular risk occurring and its likely

impact. Several qualitative and quantitative approaches were introduced to help in analysis. It is, however, important to keep in mind that there is a cost associated with responding to a particular risk, so risk management must junction within the project's available resources.

Risk strategies define how the project stakeholders will respond to risk. In general, risk strategies include (1) accepting or ignoring the risk, (2) avoiding the risk, (3) mitigating or reducing the likelihood and/or impact of the risk, and (4) transferring the risk to someone else. A set of risk metrics should be defined to act as triggers, or flags, when a particular risk event occurs. The risks, the risk triggers, risk owners, and strategies should be formalized in a risk response plan.

Once the risk response plan has been completed and the project is underway, the various risks identified must be monitored and controlled. This process should include vigilance on the identified and unidentified threats and/or opportunities. As these risks present themselves, project risk owners should make resources available and respond to risk (Risk Response) in an appropriate manner, as outlined in the risk response plan.

Risk evaluation provides a key to learning and identifying best practices. A formal and documented evaluation of a risk response or episode can help an organization evaluate its entire risk management approach and provide insight for future project teams that may have to deal with a similar risk in the future.

| WEB SITES TO VISIT

www.palisade.com: Palisade Corp. provides many project risk management software tools. Free trial versions can be downloaded and evaluated. **www.decisioneering.com:** Decisioneering provides a risk management tool called Crystalball™. Free trial versions of several of its products can be downloaded and evaluated.

http://perso.wanadoo.fr/courtot.herve/links.htm: Project Risk Management Sites of Interest.

You can download a copy of this tool without cost from two Web sites, **www.iceincUSA.com** (Integrated Computer Engineering) and **www.spmn.com** (Software Program Managers Network): Integrated Computer Engineering, Inc. (ICE) provides Risk Radar™ (Version 2.02) as a free software product.

| REVIEW QUESTIONS

1. What leads to uncertainty in an IT project?
2. How does a project risk management approach pro vide an early warning signal for impending prob lems or issues?
3. What is meant by crisis management? And why do many organizations find themselves in this mode?
4. Describe some of the common mistakes in project risk management.
5. Briefly describe what is required for effective and successful project risk management.
6. What is project risk?
7. What is project risk management?
8. What are the seven IT project risk management processes?
9. What types of commitment are necessary for risk planning?
10. Why can identifying IT project risks be difficult?
11. What is a "known" risk? Give an example of one.
12. What is a "known-unknown" risk? Give an example of one.
13. What is an "unknown-unknown" risk? Give an example of one.
14. What is the difference between an internal and external risk? Give an example of each.
15. Describe some of the tools and techniques that can be used to identify IT project risks.
16. Describe the nominal group technique and how it can be applied to identifying IT project risks.
17. Describe how learning cycles can be used to iden tify IT project risks.
18. What is the Delphi Technique? How can this tech nique be used to identify IT project risks?
19. How can interviewing be used as a technique for identifying IT project risks? What are some of the advantages and disadvantages of using this technique?

20. How do checklists help in identifying IT project risk? Discuss the pros and cons of using this technique.
21. What is SWOT analysis? How can this technique be used to identify IT project risks?
22. What is a fishbone (Ishikawa) diagram? How can this tool be used to identify IT project risks?
23. What is the purpose of risk analysis and assess ment?
24. What is the difference between qualitative and quantitative risk analysis?
25. Describe the concept of expected value.
26. What is the purpose of a decision tree? What are the advantages and disadvantages of using a decision tree?
27. What is the purpose of a risk impact table?
28. What is the difference between a discrete proba bility distribution and a continuous probability distribution?
29. What are the rules of thumb that can be applied to a normal distribution?
30. Compare and contrast the normal distribution, the PERT distribution, and the triangular distribution.
31. What is a simulation? What value do simulations provide when analyzing and assessing IT project risks?
32. What is a Monte Carlo simulation? Describe a situ ation (other than the one used in this chapter) that could make good use of a Monte Carlo simulation.
33. Define and discuss the four risk strategies described in this chapter.
34. What is the difference between a management reserve and a contingency reserve?
35. What is a contingency plan?
36. Why can't a project team respond to all project risks?
37. What is a risk response plan? What should be included?
38. What are risk triggers or flags?
39. Why is having a risk owner a good idea? What role does a risk owner play?
40. What is risk monitoring and control?
41. Describe the three risk monitoring tools that were discussed in this chapter.
42. What is the purpose of evaluating a response to a particular risk?

EXTEND YOUR KNOWLEDGE

1. Using the Internet or the library, find an article about an IT project that failed. Using the IT project risk framework (Figure 8.2), identify the explicit or implicit risks that may have impacted this project.
2. Plan a trip to a show or a sporting event in another city. Define how you will get there and estimate how long it will take. Then define the risks that you might encounter and then construct a risk impact table. Afterwards, rank the risks and come up with a risk strategy for the three most significant risks.

BIBLIOGRAPHY

Choo, G 2001. It's A Risky Business, www.systemcorp.com/frame-site/downloads/choo_p.html Delbecq, A. and A. H. Van de Van. 1971. A Group Process Model for Identification and Program Planning. *Journal of Applied Behavioral Sciences 1:* 466-492. Jones, T. C. 1994. *Assessment and Control of Software Risks.* Upper Saddle River, N.J.: Yourdon Press/Prentice Hall. Kulik, P. 2000. What is Software Risk Management (And Why Should I Care?), www.klci.com

Lanza, R. B. 2001. Reviewing a Project Risk Management System. www.auditsoftware.net/infoarchive/articles/projmgmt/files/riskm gmt.htm Tusler, R. 1998. An Overview of Project Risk Management, www.net-comuk.co.uk/~rtusler/project/elements.html Wideman, R. M. 1992. *Project and Program Risk Management: A Guide to Managing Project Risks and Opportunities.* Newtown Square, Pa.: Project Management Institute.