11

Project Risk Management

OPENING CASE

Cliff Branch was the president of a small information technology consulting firm that specialized in developing Internet applications and providing full-service support. The staff consisted of programmers, business analysts, database specialists, Web designers, project managers, and so on. The firm had 50 people and planned to hire at least 10 more in the next year. The company had done very well the past few years, but was recently having difficulty winning contracts. Spending time and resources to respond to various requests for proposals from prospective clients was becoming expensive. Many clients were starting to require presentations and even some prototype development before awarding a contract.

Cliff knew he had an aggressive approach to risk and liked to bid on the projects with the highest payoff. He did not use a systematic approach to evaluate the risks involved in various projects before bidding on them. He focused on the profit potentials and on how challenging the projects were. His strategy was now causing problems for the company because it was investing heavily in the preparation of proposals, yet winning few contracts. Several consultants who were not currently working on projects were still on the payroll. What could Cliff and his company do to get a better understanding of project risks? Should Cliff adjust his strategy for deciding what projects to pursue? How?

THE IMPORTANCE OF PROJECT RISK MANAGEMENT

Project risk management is the art and science of identifying, analyzing, and responding to risk throughout the life of a project and in the best interests of meeting project objectives. A frequently overlooked aspect of project management, risk management can often result in significant improvements in the ultimate success

of projects. Risk management can have a positive impact on selecting projects, determining the scope of projects, and developing realistic schedules and cost estimates. It helps project stakeholders understand the nature of the project, involves team members in defining strengths and weaknesses, and helps to integrate the other project management knowledge areas.

Good project risk management often goes unnoticed, unlike crisis management. With crisis management, there is an obvious danger to the success of a project. The crisis, in turn, receives the intense interest of the entire project team. Resolving a crisis has much greater visibility, often accompanied by rewards from management, than successful risk management. In contrast, when risk management is effective, it results in fewer problems, and for the few problems that exist, it results in more expeditious resolutions. It may be difficult for outside observers to tell whether risk management or luck was responsible for the smooth development of a new system, but project teams will always know that their projects worked out better because of good risk management.

All industries, especially the software development industry, tend to neglect the importance of project risk management. William Ibbs and Young H. Kwak performed a study to assess project management maturity. The 38 organizations participating in the study were divided into four industry groups: engineering and construction, telecommunications, information systems/software development, and high-tech manufacturing. Survey participants answered 148 multiple-choice questions to assess how mature their organization was in the project management knowledge areas of scope, time, cost, quality, human resources, communications, risk, and procurement. The rating scale ranged from 1 to 5, with 5 being the highest maturity rating. Table 11-1 shows the results of the survey. Notice that risk management was the only knowledge area for which all ratings were less than 3. This study shows that all organizations should put more effort into project risk management, especially the information systems/software development industry, which had the lowest rating of 2.75.[1]

Table 11-1: Project Management Maturity by Industry Group and Knowledge Area

KEY: 1 = Lowest Maturity Rating 5 = Highest Maturity Rating

KNOWLEDGE AREA	ENGINEERING/ CONSTRUCTION	TELECOMMUNICATIONS	INFORMATION SYSTEMS	HI-TECH MANUFACTURING
Scope	3.52	3.45	3.25	3.37
Time	3.55	3.41	3.03	3.50
Cost	3.74	3.22	3.20	3.97
Quality	2.91	3.22	2.88	3.26
Human Resources	3.18	3.20	2.93	3.18
Communications	3.53	3.53	3.21	3.48
Risk	**2.93**	**2.87**	**2.75**	**2.76**
Procurement	3.33	3.01	2.91	3.33

A similar survey was completed with software development companies in Mauritius, South Africa in 2003. The average maturity rating was only 2.29 for all knowledge areas, on a scale of 1-5, with 5 being the highest maturity rating. The lowest maturity rating in this study was also in the area of project risk management, with an average maturity rating of only 1.84. Cost management had the highest maturity rating of 2.5, and the authors of the survey noted that organizations in the study were often concerned with cost overruns and had metrics in place to help control costs. The authors also found that maturity rating was closely linked to the success rate of projects, and they noted the fact that the poor rating for risk management was a likely cause of project problems/failures.[2]

KLCI Research Group surveyed 260 software organizations worldwide in 2001 to study software risk management practices. Below are some of their findings:

- 97 percent of the participants said they had procedures in place to identify and assess risk.
- 80 percent identified anticipating and avoiding problems as the primary benefit of risk management.
- 70 percent of the organizations had defined software development processes.
- 64 percent had a Project Management Office.

Figure 11-1 shows the main benefits from software risk management practices cited by survey respondents. In addition to anticipating/avoiding problems, risk management practices helped software project managers prevent surprises, improve negotiations, meet customer commitments, and reduce schedule slips and cost overruns.[3]

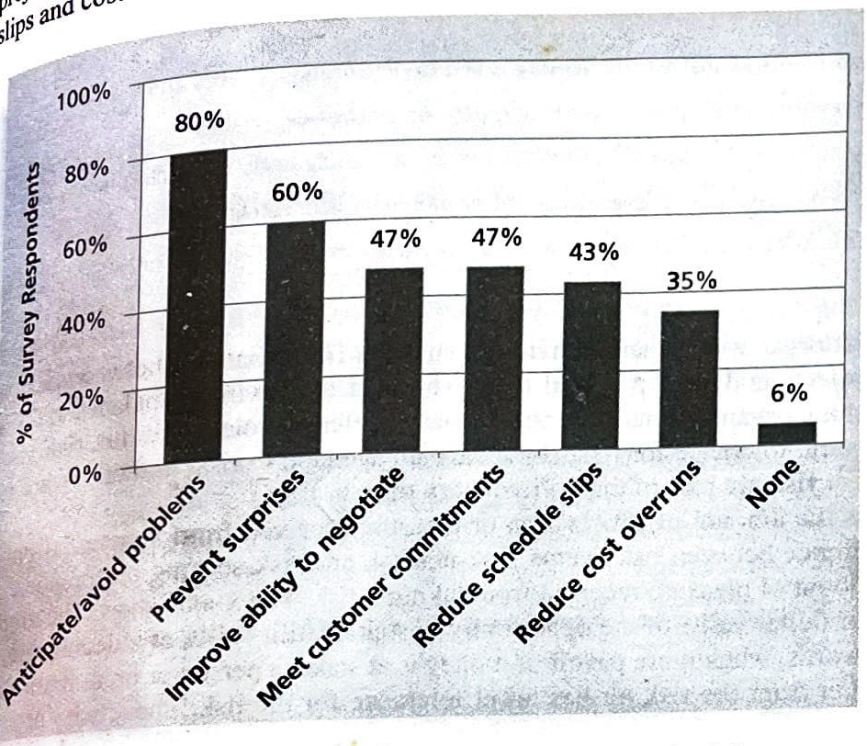

Figure 11-1. Benefits from Software Risk Management Practices

Before you can improve project risk management, you must understand what risk is. A basic dictionary definition says that risk is "the possibility of loss or injury." This definition highlights the negativity often associated with risk and suggests that uncertainty is involved. Project risk management involves understanding potential problems that might occur on the project and how they might impede project success. The *PMBOK® Guide Third Edition* refers to this type of risk as a negative risk. However, there are also positive risks, which can result in good things happening on a project. A general definition of a project risk, therefore, is an uncertainty that can have a negative or positive effect on meeting project objectives.

In many respects, negative risk management is like a form of insurance. It is an activity undertaken to lessen the impact of potentially adverse events on a project. Positive risk management is like investing in opportunities. It is important to note that risk management *is* an investment—there are costs associated with it. The investment an organization is willing to make in risk management activities depends on the nature of the project, the experience of the project team, and the constraints imposed on both. In any case, the cost for risk management should not exceed the potential benefits.

If there is so much risk in information technology projects, why do organizations pursue them? Many companies are in business today because they took risks that created great opportunities. Organizations survive over the long term when they pursue opportunities. Information technology is often a key part of a business's strategy; without it, many businesses might not survive. Given that all projects involve uncertainties that can have negative or positive outcomes, the question is how to decide which projects to pursue and how to identify and manage project risk throughout a project's life cycle.

Best Practice

Some organizations make the mistake of only addressing tactical and negative risks when performing project risk management. David Hillson (*www.risk-doctor.com*) suggests overcoming this problem by widening the scope of risk management to encompass both *strategic risks* and *upside opportunities*, which he refers to as integrated risk management. Benefits of this approach include:

- Bridging the strategy and tactics gap to ensure that project delivery is tied to organizational needs and vision
- Focusing projects on the benefits they exist to support, rather than producing a set of deliverables
- Managing opportunities proactively as an integral part of business processes at both strategic and tactical levels
- Providing useful information to decision-makers at all levels when the environment is uncertain
- Allowing an appropriate level of risk to be taken intelligently with full awareness of the degree of uncertainty and its potential effects on objectives.[4]

Several risk experts suggest that organizations and individuals strive to find a balance between risks and opportunities in all aspects of projects and their personal lives. The idea of striving to balance risks and opportunities suggests that different organizations and people have different tolerances for risk. Some organizations or people have a neutral tolerance for risk, some have an aversion to risk, and others are risk-seeking. These three preferences for risk are part of the utility theory of risk.

Risk utility or risk tolerance is the amount of satisfaction or pleasure received from a potential payoff. Figure 11-2 shows the basic difference between risk-averse, risk-neutral, and risk-seeking preferences. The y-axis represents utility, or the amount of pleasure received from taking a risk. The x-axis shows the amount of potential payoff, opportunity, or dollar value of the opportunity at stake. Utility rises at a decreasing rate for a risk-averse person. In other words, when more payoff or money is at stake, a person or organization that is risk-averse gains less satisfaction from the risk, or has lower tolerance for the risk. Those who are risk-seeking have a higher tolerance for risk, and their satisfaction increases when more payoff is at stake. A risk-seeking person prefers outcomes that are more uncertain and is often willing to pay a penalty to take risks. A risk-neutral person achieves a balance between risk and payoff.

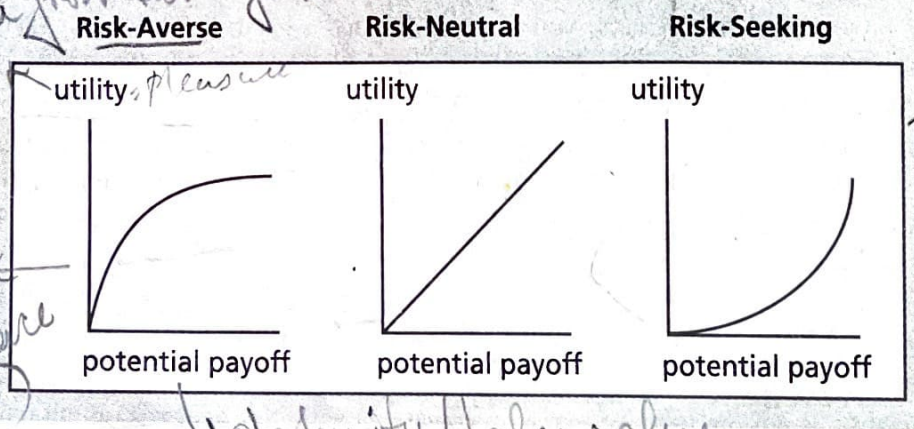

Figure 11-2. Risk Utility Function and Risk Preference

The goal of project risk management can be viewed as minimizing potential negative risks while maximizing potential positive risks. The term "known risks" is sometimes used to describe risks that the project team have identified and analyzed. Known risks can be managed proactively. However, unknown risks, or risks that have not been identified and analyzed, cannot be managed. As you can imagine, good project managers know it is good practice to take the time to identify and manage project risks. There are six major processes involved in risk management:

1. Risk management planning involves deciding how to approach and plan the risk management activities for the project. By reviewing the project scope statement, project management plan, enterprise environmental factors, and organizational process assets, project teams can discuss and analyze risk management activities for their particular projects. The main output of this process is a risk management plan.
2. Risk identification involves determining which risks are likely to affect a project and documenting the characteristics of each. The main output of this process is the start of a risk register, as described in more detail later in this chapter.
3. Qualitative risk analysis involves prioritizing risks based on their probability and impact of occurrence. After identifying risks, project teams can use various tools and techniques to rank risks and update information in the risk register. The main output is updates to the risk register.
4. Quantitative risk analysis involves numerically estimating the effects of risks on project objectives. The main output of this process is also updates to the risk register.
5. Risk response planning involves taking steps to enhance opportunities and reduce threats to meeting project objectives. Using outputs from the preceding risk management processes, project teams can develop risk response strategies that often result in updates to the risk register and project management plan as well as risk-related contractual agreements.
6. Risk monitoring and control involves monitoring identified and residual risks, identifying new risks, carrying out risk response plans, and evaluating the effectiveness of risk strategies throughout the life of the project. The main outputs of this process include recommended corrective and preventive actions, requested changes, and updates to the risk register, project management plan, and organizational process assets.

Figure 11-3 summarizes these processes and outputs, showing when they occur in a typical project.

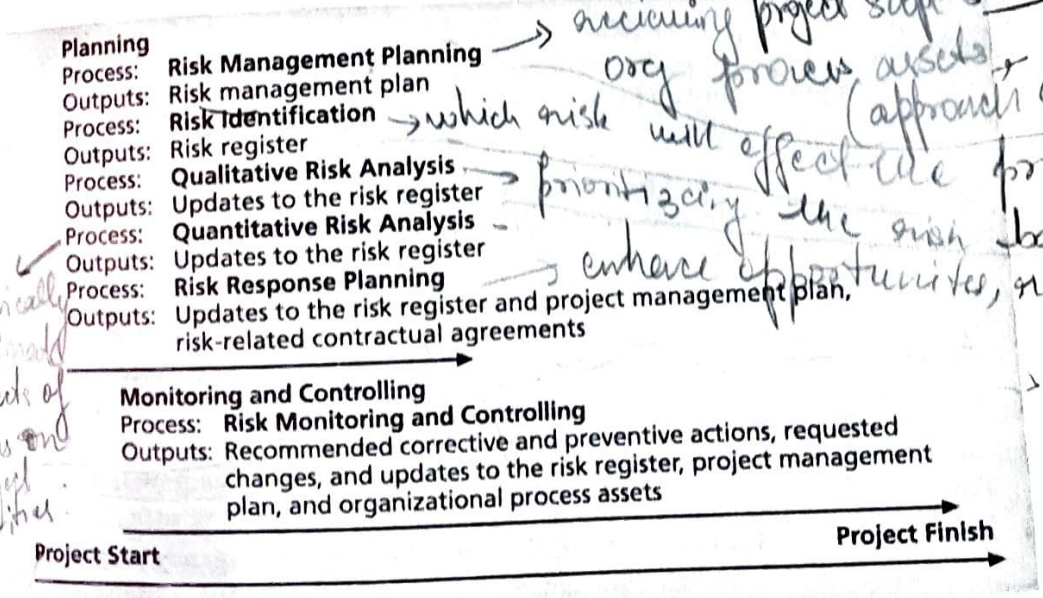

Figure 11-3. Project Risk Management Summary

The first step in project risk management is deciding how to address this knowledge area for a particular project by performing risk management planning.

RISK MANAGEMENT PLANNING

Risk management planning is the process of deciding how to approach and plan for risk management activities for a project, and the main output of this process is a risk management plan. A risk management plan documents the procedures for managing risk throughout the project. Project teams should hold several planning meetings early in the project's life cycle to help develop the risk management plan. The project team should review project documents as well as corporate risk management policies, risk categories, lessons-learned reports from past projects, and templates for creating a risk management plan. It is also important to review the risk tolerances of various stakeholders. For example, if the project sponsor is risk-averse, the project might require a different approach to risk management than if the project sponsor were a risk seeker.

A risk management plan summarizes how risk management will be performed on a particular project. Like other specific knowledge area plans, it becomes a subset of the project management plan. Table 11-2 lists the general topics that a risk management plan should address. It is important to clarify roles and responsibilities, prepare budget and schedule estimates for risk-related work, and identify risk categories for consideration. It is also important to describe how risk management will be done, including assessment of risk probabilities and impacts as well as creation of risk related documentation. The level of detail included in the risk management plan will vary with the needs of the project.

Table 11-2: Topics Addressed in a Risk Management Plan

- Methodology: How will risk management be performed on this project? What tools and data sources are available and applicable?
- Roles and Responsibilities: Who are the individuals responsible for implementing specific tasks and providing deliverables related to risk management?
- Budget and Schedule: What are the estimated costs and schedules for performing risk-related activities?
- Risk Categories: What are the main categories of risks that should be addressed on this project? Is there a risk breakdown structure for the project? (See the information on risk breakdown structures later in this section.)
- Risk Probability and Impact: How will the probabilities and impacts of risk items be assessed? What scoring and interpretation methods will be used for the qualitative and quantitative analysis of risks?
- Risk Documentation: What reporting formats and processes will be used for risk management activities?

In addition to a risk management plan, many projects also include contingency plans, fallback plans, and contingency reserves. Contingency plans are predefined actions that the project team will take if an identified risk event occurs. For example, if the project team knows that a new release of a software package may not be available in time for them to use it for their project, they might have a contingency plan to use the existing, older version of the software. Fallback plans are developed for risks that have a high impact on meeting project objectives, and are put into effect if attempts to reduce the risk are not effective. For example, a new college graduate might have a main plan and several contingency plans on where to live after

graduation, but if none of those plans works out, a fallback plan might be to live at home for a while. Sometimes the terms contingency plan and fallback plan are used interchangeably. Contingency reserves or contingency allowances are provisions held by the project sponsor or organization to reduce the risk of cost or schedule overruns to an acceptable level. For example, if a project appears to be off course because the staff is inexperienced with some new technology and the team had not identified that as a risk, the project sponsor may provide additional funds from contingency reserves to hire an outside consultant to train and advise the project staff in using the new technology.

Before you can really understand and use the other project risk management processes on information technology projects, it is necessary to recognize and understand the common sources of risk.

COMMON SOURCES OF RISK ON INFORMATION TECHNOLOGY PROJECTS

Several studies have shown that information technology projects share some common sources of risk. For example, the Standish Group did a follow-up study to the CHAOS research, which they called Unfinished Voyages. This study brought together 60 information technology professionals to elaborate on how to evaluate a project's overall likelihood of being successful. Table 11-3 shows the Standish Group's success potential scoring sheet and the relative importance of the project success criteria factors. If a potential project does not receive a minimum score, the organization might decide not to work on it or to take actions to reduce the risks before it invests too much time or money.[5]

Table 11-3: Information Technology Success Potential Scoring Sheet

Success Criterion	Relative Importance
User Involvement	19
Executive Management Support	16
Clear Statement of Requirements	15
Proper Planning	11
Realistic Expectations	10
Smaller Project Milestones	9
Competent Staff	8
Ownership	6
Clear Visions and Objectives	3
Hardworking, Focused Staff	3
Total	**100**

The Standish Group provides specific questions for each success criterion to help decide the number of points to assign to a project. For example, the five questions related to user involvement include the following:

- Do I have the right user(s)?
- Did I involve the user(s) early and often?
- Do I have a quality relationship with the user(s)?

- Do I make involvement easy?
- Did I find out what the user(s) need(s)?

The number of questions corresponding to each success criterion determines the number of points each positive response is assigned. For example, in the case of user involvement there are five questions. For each positive reply, you would get 3.8 (19/5) points; 19 represents the weight of the criterion, and 5 represents the number of questions. Therefore, you would assign a value to the user involvement criterion by adding 3.8 points to the score for each question you can answer positively.

Many organizations develop their own risk questionnaires. Broad categories of risks described on these questionnaires might include:

- *Market risk*: If the information technology project is to produce a new product or service, will it be useful to the organization or marketable to others? Will users accept and use the product or service? Will someone else create a better product or service faster, making the project a waste of time and money?
- *Financial risk*: Can the organization afford to undertake the project? How confident are stakeholders in the financial projections? Will the project meet NPV, ROI, and payback estimates? If not, can the organization afford to continue the project? Is this project the best way to use the organization's financial resources?
- *Technology risk*: Is the project technically feasible? Will it use mature, leading edge, or bleeding edge technologies? When will decisions be made on which technology to use? Will hardware, software, and networks function properly? Will the technology be available in time to meet project objectives? Could the technology be obsolete before a useful product can be produced? You can also break down the technology risk category into hardware, software, and network technology, if desired.
- *People risk*: Does the organization have or can they find people with appropriate skills to complete the project successfully? Do people have the proper managerial and technical skills? Do they have enough experience? Does senior management support the project? Is there a project champion? Is the organization familiar with the sponsor/customer for the project? How good is the relationship with the sponsor/customer?
- *Structure/process risk*: What is the degree of change the new project will introduce into user areas and business procedures? How many distinct user groups does the project need to satisfy? With how many other systems does the new project/system need to interact? Does the organization have processes in place to complete the project successfully?

Reviewing a proposed project in terms of the Standish Group's success criteria, a risk questionnaire, or any other similar tool is a good method for understanding common sources of risk on information technology projects. It is also useful to review the work breakdown structure (WBS) for a project to see if there might be specific risks by WBS categories. For example, if one item on the WBS involves preparing a press release and no one on the project team has ever done that, it could be a negative risk if it is not handled professionally.

A risk breakdown structure is a useful tool that can help project managers consider potential risks in different categories. Similar in structure to a work breakdown structure, a risk breakdown structure is a hierarchy of potential risk categories for a project. Figure 11-4 shows a sample risk breakdown structure that might apply to many information technology projects. The highest-level categories are business, technical, organizational, and project management. Competitors, suppliers, and cash flow are categories that fall under business risks. Under technical risks are the categories of hardware, software, and network. Notice how the risk breakdown structure provides a simple, one-page chart to help ensure a project team is considering important risk categories related to all information technology projects. For example, Cliff and his managers in the opening case could have benefited from considering several of the categories listed under project management—estimates, communication, and resources. They could have discussed these and other types of risks related to the projects

their company bid on and developed appropriate strategies for optimizing positive risks and minimizing negative ones.

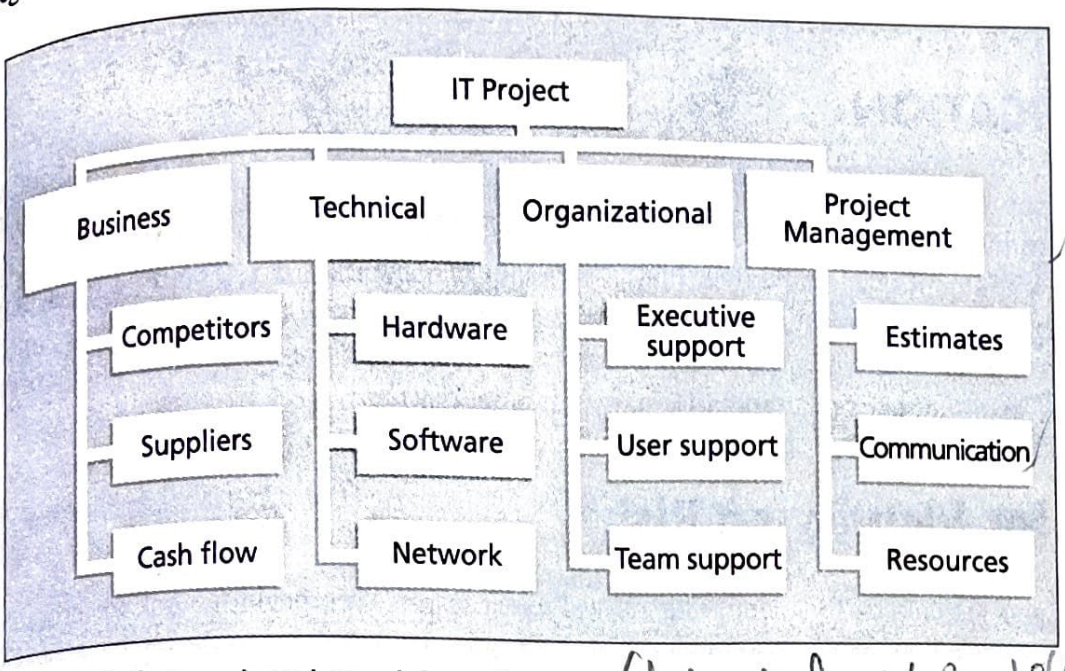

Figure 11-4. Sample Risk Breakdown Structure

In addition to identifying risk based on the nature of the project or products produced, it is also important to identify potential risks according to project management knowledge areas, such as scope, time, cost, and quality. Notice that one of the major categories in the risk breakdown structure in Figure 11-4 is project management. Table 11-4 lists potential negative risk conditions that can exist within each knowledge area.[6]

Table 11-4: Potential Negative Risk Conditions Associated with Each Knowledge Area

KNOWLEDGE AREA	RISK CONDITIONS
Integration	Inadequate planning; poor resource allocation; poor integration management; lack of post-project review
Scope	Poor definition of scope or work packages; incomplete definition
Time	Errors in estimating time or resource availability; errors in determining the critical path; poor allocation and management of float; early release of competitive products
Cost	Estimating errors; inadequate productivity, cost, change, or contingency
Quality	Poor attitude toward quality; substandard design/materials/workmanship; inadequate quality assurance program
Human Resources	Poor conflict management; poor project organization and definition of responsibilities; absence of leadership
Communications	Carelessness in planning or communicating; lack of consultation with key stakeholders
Risk	Ignoring risk; unclear analysis of risk; poor insurance management
Procurement	Unenforceable conditions or contract clauses; adversarial relations

Understanding common sources of risk is very helpful in risk identification, which is the next step in project risk management.

RISK IDENTIFICATION

Identifying risks is the process of understanding what potential events might hurt or enhance a particular project. It is important to identify potential risks early, but you must also continue to identify risks based on the changing project environment. Also remember that you cannot manage risks if you do not first identify them. By understanding common sources of risks and reviewing a project's risk management plan, project scope statement, project management plan, enterprise environmental factors, and organizational process assets, project managers and their teams can identify many potential risks.

Suggestions for Identifying Risks

There are several tools and techniques for identifying risks. Project teams often begin the risk identification process by reviewing project documentation, recent and historical information related to the organization, and assumptions that might affect the project. Project team members and outside experts often hold meetings to discuss this information and ask important questions about them as they relate to risk. After identifying potential risks at this initial meeting, the project team might then use different information-gathering techniques to further identify risks. Five common information-gathering techniques include brainstorming, the Delphi Technique, interviewing, root cause analysis, and SWOT analysis.

Brainstorming is a technique by which a group attempts to generate ideas or find a solution for a specific problem by amassing ideas spontaneously and without judgment. This approach can help the group create a comprehensive list of risks to address later in the qualitative and quantitative risk analysis processes. An experienced facilitator should run the brainstorming session and introduce new categories of potential risks to keep the ideas flowing. After the ideas are collected, the facilitator can group and categorize the ideas to make them more manageable. Care must be taken, however, not to overuse or misuse brainstorming. Although businesses use brainstorming widely to generate new ideas, the psychology literature shows that individuals, working alone, produce a greater number of ideas than the same individuals produce through brainstorming in small, face-to-face groups. Group effects, such as fear of social disapproval, the effects of authority hierarchy, and domination of the session by one or two very vocal people often inhibit idea generation for many participants.[7]

An approach to gathering information that helps prevent some of the negative group affects found in brainstorming is the Delphi Technique. The basic concept of the Delphi Technique is to derive a consensus among a panel of experts who make predictions about future developments. Developed by the Rand Corporation for the U.S. Air Force in the late 1960s, the Delphi Technique is a systematic, interactive forecasting procedure based on independent and *anonymous* input regarding future events. The Delphi Technique uses repeated rounds of questioning and written responses, including feedback to earlier-round responses, to take advantage of group input, while avoiding the biasing effects possible in oral panel deliberations. To use the Delphi Technique, you must select a panel of experts for the particular area in question. For example, Cliff Branch from the opening case could use the Delphi Technique to help him understand why his company is no longer winning many contracts. Cliff could assemble a panel of people with knowledge in his business area. Each expert would answer questions related to Cliff's scenario, and then Cliff or a facilitator would evaluate their responses, together with opinions and justifications, and provide that feedback to each expert in the next iteration. Cliff would continue this process until the group responses converge to a specific solution. If the responses diverge, the facilitator of the Delphi Technique needs to determine if there is a problem with the process.

Interviewing is a fact-finding technique for collecting information in face-to-face, phone, e-mail, or instant-messaging discussions. Interviewing people with similar project experience is an important tool for identifying potential risks. For example, if a new project involves using a particular type of hardware or software, someone with recent experience with that hardware or software could describe problems he or she had on a past project. If someone has worked with a particular customer, he or she might provide insight into potential risks involved in working for that group again. It is important to be well-prepared for leading interviews; it often helps to create a list of questions to use as a guide during the interview.

It is not uncommon for people to identify problems or opportunities without really understanding them. Before suggesting courses of action, it is important to identify the root cause of a problem or opportunity. Chapter 8, Project Quality Management, provides information on root cause analysis. Root cause analysis often results in identifying even more potential risks for a project.

Another technique described in Chapter 4, Project Integration Management, is a SWOT analysis (strengths, weaknesses, opportunities, and threats), which is often used in strategic planning. SWOT analysis can also be used during risk identification by having project teams focus on the broad perspectives of potential risks for particular projects. For example, before writing a particular proposal, Cliff Branch could have a group of his employees discuss in detail what their company's strengths are, what their weaknesses are related to that project, and what opportunities and threats exist. Do they know that several competing firms are much more likely to win a certain contract? Do they know that winning a particular contract will likely lead to future contracts and help expand their business? Applying SWOT to specific potential projects can help identify the broad risks and opportunities that apply in that scenario.

Three other techniques for risk identification include the use of checklists, analysis of assumptions, and creation of diagrams.

- Checklists based on risks that have been encountered in previous projects provide a meaningful template for understanding risks in a current project. You can use checklists similar to those developed by the Standish Group or other groups to help identify risks on information technology projects.
- It is important to analyze project assumptions to make sure they are valid. Incomplete, inaccurate, or inconsistent assumptions might lead to identifying more risks.
- Diagramming techniques include using cause-and-effect diagrams or fishbone diagrams, flow charts, and influence diagrams. Recall from Chapter 8, Project Quality Management, that fishbone diagrams help you trace problems back to their root cause. System or process flow charts are diagrams that show how different parts of a system interrelate. For example, many programmers create flow charts to show programming logic. A sample flow chart is also provided in Chapter 8. Another type of diagram, an influence diagram, represents decision problems by displaying essential elements, including decisions, uncertainties, causality, and objectives, and how they influence each other. See other references, such as *www.lumina.com/software/influencediagrams.html*, for detailed information on influence diagrams.

The Risk Register

The main output of the risk identification process is a list of identified risks and other information needed to begin creating a risk register. A risk register is a document that contains results of various risk management processes, often displayed in a table or spreadsheet format. It is a tool for documenting potential risk events and related information. Risk events refer to specific, uncertain events that may occur to the detriment or enhancement of the project. For example, negative risk events might include the performance failure of a product produced as part of a project, delays in completing work as scheduled, increases in estimated costs, supply shortages, litigation against the company, strikes, and so on. Examples of positive risk events include completing work sooner or cheaper than planned, collaborating with suppliers to produce better products, good publicity resulting from the project, and so on.

Table 11-5 provides a sample of the format for a risk register that Cliff and his managers from the opening case might use on a new project. Actual data that might be entered for one of the risks is included below the table. Notice the main headings often included in the register. Many of these items are described in more detail later in this chapter.

- *An identification number for each risk event*: The project team may want to sort or quickly search for specific risk events, so they need to identify each risk with some type of unique descriptor, like an identification number.
- *A rank for each risk event*: The rank is usually a number, with 1 being the highest ranked risk.
- *The name of the risk event*: For example, defective server, late completion of testing, reduced consulting costs, or good publicity.
- *A description of the risk event*: Because the name of a risk event is often abbreviated, it helps to provide a more detailed description. For example, reduced consulting costs might be expanded in the description to say that the organization might be able to negotiate lower-than-average costs for a particular consultant because the consultant really enjoys working for that company in that particular location.
- *The category under which the risk event falls*: For example, defective server might fall under the broader category of technology or hardware technology.
- *The root cause of the risk*: The root cause of the defective server might be a defective power supply.
- *Triggers for each risk*: Triggers are indicators or symptoms of actual risk events. For example, cost overruns on early activities may be symptoms of poor cost estimates. Defective products may be symptoms of a low-quality supplier. Documenting potential risk symptoms for projects also helps the project team identify more potential risk events.
- *Potential responses to each risk*: A potential response to the risk event of a defective server might be the inclusion of a clause in a contract with the supplier to replace a defective server within a certain time period at a negotiated cost.
- *The* risk owner *or person who will own or take responsibility for the risk*: For example, a certain person might be in charge of any server-related risk events and managing response strategies.
- *The probability of the risk occurring*: There might be a high, medium, or low probability of a certain risk event occurring. For example, the risk might be low that the server would actually be defective.
- *The impact to the project if the risk occurs*: There might be a high, medium, or low impact to project success if the risk event actually occurs. A defective server might have a high impact on successfully completing a project on time.
- *The status of the risk*: Did the risk event occur? Was the response strategy completed? Is the risk no longer relevant to the project? For example, a contract clause may have been completed to address the risk of a defective server.

Table 11-5: Sample Risk Register

No.	Rank	Risk	Description	Category	Root Cause	Triggers	Potential Responses	Risk Owner	Probability	Impact	Status
R44	1										
R21	2										
R7	3										

For example, the following data might be entered for the first risk in the register as follows. Notice that Cliff's team is taking a very proactive approach in managing this risk.

- *No.*: R44
- *Rank*: 1
- *Risk*: New customer
- *Description*: We have never done a project for this organization before and don't know too much about them. One of our company's strengths is building good customer relationships, which often leads to further projects with that customer. We might have trouble working with this customer since they are new to us.
- *Category*: People risk
- *Root cause*: We won a contract to work on a project without really getting to know the customer.
- *Triggers*: The project manager and other senior managers realize that we don't know much about this customer and could easily misunderstand their needs or expectations.
- *Risk Responses*: Make sure the project manager is sensitive to the fact that this is a new customer and takes the time to understand them. Have the PM set up a meeting to get to know the customer and clarify their expectations. Have Cliff attend the meeting, too.
- *Risk owner*: Our project manager
- *Probability*: Medium
- *Impact*: High
- *Status*: PM will set up the meeting within the week.

After identifying risks, the next step is to understand which risks are most important by performing qualitative risk analysis.

QUALITATIVE RISK ANALYSIS

Qualitative risk analysis involves assessing the likelihood and impact of identified risks, to determine their magnitude and priority. This section describes examples of using a probability/impact matrix to produce a prioritized list of risks. It also provides examples of using the Top Ten Risk Item Tracking technique to produce an overall ranking for project risks and to track trends in qualitative risk analysis. Finally, it discusses the importance of expert judgment in performing risk analysis.

Using Probability/Impact Matrixes to Calculate Risk Factors

People often describe a risk probability or consequence as being high, medium or moderate, or low. For example, a meteorologist might predict that there is a high probability, or likelihood, of severe rain showers on a certain day. If that day happens to be your wedding day and you are planning a large outdoor wedding, the consequences or impact of severe showers might also be high.

A project manager can chart the probability and impact of risks on a probability/impact matrix or chart. A probability/impact matrix or chart lists the relative probability of a risk occurring on one side of a matrix or axis on a chart and the relative impact of the risk occurring on the other. Many project teams would benefit from using this simple technique to help them identify risks that they need to pay attention to. To use this approach, project stakeholders list the risks they think might occur on their projects. They then label each risk as being high, medium, or low in terms of its probability of occurrence and its impact if it did occur.

4. Risk acceptance also applies to positive risks when the project team cannot or chooses not to take any actions toward a risk. For example, the computer classrooms project manager might just assume the project will result in good public relations for their company without doing anything extra.

The main outputs of risk response planning include risk-related contractual agreements, updates to the project management plan, and updates to the risk register. For example, if Cliff's company decided to partner with a local training firm on the computer classrooms project to share the opportunity of achieving good public relations, it could write a contract with that firm. The project management plan and its related plans might need to be updated if the risk response strategies require additional tasks, resources, or time to accomplish them. Risk response strategies often result in changes to the WBS and project schedule, so plans with that information must be updated. The risk response strategies also provide updated information for the risk register by describing the risk responses, risk owners, and status information.

Risk response strategies often include identification of residual and secondary risks as well as contingency plans and reserves, as described earlier. Residual risks are risks that remain after all of the response strategies have been implemented. For example, even though a more stable hardware product may have been used on a project, there may still be some risk of it failing to function properly. Secondary risks are a direct result of implementing a risk response. For example, using the more stable hardware may have caused a risk of peripheral devices failing to function properly.

RISK MONITORING AND CONTROL

Risk monitoring and control involves executing the risk management processes to respond to risk events. Executing the risk management processes means ensuring that risk awareness is an ongoing activity performed by the entire project team throughout the entire project. Project risk management does not stop with the initial risk analysis. Identified risks may not materialize, or their probabilities of occurrence or loss may diminish. Previously identified risks may be determined to have a greater probability of occurrence or a higher estimated loss value. Similarly, new risks will be identified as the project progresses. Newly identified risks need to go through the same process as those identified during the initial risk assessment. A redistribution of resources devoted to risk management may be necessary because of relative changes in risk exposure.

Carrying out individual risk management plans involves monitoring risks based on defined milestones and making decisions regarding risks and their response strategies. It may be necessary to alter a strategy if it becomes ineffective, implement a planned contingency activity, or eliminate a risk from the list of potential risks when it no longer exists. Project teams sometimes use workarounds—unplanned responses to risk events—when they do not have contingency plans in place.

Risk reassessment, risk audits, variance and trend analysis, technical performance measurements, reserve analysis, and status meetings or periodic risk reviews such as the Top Ten Risk Item Tracking method are all tools and techniques for performing risk monitoring and control. Outputs of this process are requested changes, recommended corrective and preventive actions, and updates to the risk register, project management plan, and organizational process assets, such as lessons-learned information that might help future projects.

USING SOFTWARE TO ASSIST IN PROJECT RISK MANAGEMENT

As demonstrated in several parts of this chapter, you can use a variety of software tools to enhance various risk management processes. Most organizations use software to create, update, and distribute information in their