Chapter 6

Know Your Enemy: Introduction to Risk Management[1]

In this chapter:

When my wife and I moved from Rochester, New York, to Portland, Oregon, we had a great project plan. We had a realistic schedule for daily travel distances, routes and hotels selected, and sightseeing activities planned along the way. None of our planning, however, considered the possibility of hitting the world's largest pothole in the middle of South Dakota, which cracked a wheel rim and caused a slow air leak from that tire. Nor did we anticipate the major wreck we had in Boise, Idaho. These unforeseen events were low-probability risks with high impacts. We eventually made it to Portland, but sometimes I think Lewis and Clark had an easier trip west.

Software engineers are eternal optimists. When planning software projects, we usually assume that everything will go exactly as planned. Or, we take the other extreme position: the creative nature of software development means we can never predict what's going to happen, so what's the point of making detailed plans? Both of these perspectives can lead to software surprises, when unexpected things happen that throw the project off track. In my experience, software surprises are never good news.

Risk management has become recognized as a best practice in the software industry for reducing the surprise factor (Brown 1996; DeMarco and Lister 2003). Although we can never predict the future with certainty, we can apply structured risk management practices to peek over the horizon at the traps that might be looming. Then we can take actions to minimize the

1 This chapter was originally published in *Software Development,* 1998, 6(10): 38–42. It is reprinted here, with modifications, with permission of CMP Media Inc.

likelihood or impact of these potential problems. Risk management means dealing with a concern before it becomes a crisis. This improves the chance of successful project completion and reduces the consequences of those risks that cannot be avoided.

During project initiation take the time to do a first cut at identifying significant risks. At this stage it's most important to consider business risks, the risks of either undertaking or not undertaking the project. The project charter template described in Chapter 7 includes a slot for business risks. It's possible that the risks will outweigh the potential benefits of the project. More likely, getting an early glimpse of potential pitfalls will help you make more sensible projections of what it will take to execute this project successfully. Build time for risk identification and risk management planning into the early stages of your project. You'll find that the time you spend assessing and controlling risks will be repaid many times over.

What Is Risk?

A "risk" is a problem that could cause some loss or threaten the success of your project, but which hasn't happened yet. And you'd like to keep it that way. These potential problems might have an adverse impact on the cost, schedule, or technical success of the project, the quality of your products, or team morale. Risk management is the process of identifying, addressing, and controlling these potential problems before they do any harm.

Whether we tackle them head-on or keep our heads in the sand, risks have a potentially huge impact on many aspects of our project. The tacit assumption that nothing unexpected will derail the project is simply not realistic. Estimates should incorporate our best judgment about the potentially scary things that could happen on each project, and managers need to respect the assessments we make. Risk management is about discarding the rose-colored glasses and confronting the very real potential of undesirable events conspiring to throw the project off track.

Why Manage Risks Formally?

A formal risk management process provides multiple benefits to both the project team and the development organization as a whole. First, it gives us a structured mechanism to provide visibility into threats to project success. By considering the potential impact of each risk item, we can focus on controlling the most severe risks first. We can marry risk assessment with project estimation to quantify possible schedule slippage if certain risks materialize into problems. This approach helps the project manager generate sensible contingency buffers. Sharing what does and does not work to control risks across multiple projects helps the team avoid repeating the mistakes of the past. Without a formal approach, we cannot ensure that our risk management actions will be initiated in a timely fashion, completed as planned, and effective.

Controlling risks has a cost. We must balance this cost against the potential loss we could incur if we don't address the risk and it does indeed bite us. Suppose we're concerned about the ability of a subcontractor to deliver an essential component on time. We could engage multiple subcontractors to increase the chance that at least one will come through on schedule. That's an expensive remedy for a problem that might not even exist. Is it worth it? It depends on the downside we incur if indeed the subcontractor dependency causes the project to miss its planned ship date. Only you can decide for each individual situation.

Typical Software Risks

The list of evil things that can befall a software project is depressingly long. The enlightened project manager will acquire lists of these risk categories to help the team uncover as many concerns as possible early in the planning process. Possible risks to consider can come from group brainstorming activities or from a risk factor chart accumulated from previous projects. In one of my groups, individual team members came up with descriptions of the risks they perceived, which I edited together and we then reviewed as a team.

The Software Engineering Institute has assembled a taxonomy of hierarchically-organized risks in 13 major categories, with some 200 thought-provoking questions to help you spot the risks facing your project (Carr et al. 1993). Steve McConnell's *Rapid Development* (1996) also contains excellent resource material on risk management and an extensive list of common schedule risks.

Following are several typical risk categories and some specific risks that might threaten your project. Have any of these things have happened to you? If so, add them to your master risk checklist to remind future project managers to consider if it could happen to them, too. There are no magic solutions to any of these risk factors. We need to rely on past experience and a strong knowledge of software engineering and management practices to control those risks that concern us the most.

> Expecting the project manager to identify all the relevant risks. Different project participants will think of different possible risks. Risk identification should be a team effort.

Dependencies

Some risks arise because of dependencies our project has on outside agencies or factors. We cannot usually control these external dependencies. Mitigation strategies could involve contingency plans to acquire a necessary component from a second source, or working with the source of the dependency to maintain good visibility into status and detect any looming problems. Following are some typical dependency-related risk factors:

- Customer-furnished items or information
- Internal and external subcontractor or supplier relationships
- Intercomponent or intergroup dependencies
- Availability of trained and experienced people
- Reuse from one project to the next

Requirements Issues

Many projects face uncertainty and turmoil around the product's requirements. Some uncertainty is tolerable in the early stages, but the threat increases if such issues remain unresolved as the project progresses. If we don't control requirements-related risks we might build the wrong product or build the right product badly. Either outcome results in unpleasant surprises and unhappy customers. Watch out for these risk factors:

- Lack of a clear product vision
- Lack of agreement on product requirements
- Inadequate customer involvement in the requirements process
- Unprioritized requirements
- New market with uncertain needs
- Rapidly changing requirements
- Ineffective requirements change management process
- Inadequate impact analysis of requirements changes

Management Issues

Although management shortcomings affect many projects, don't be surprised if your risk management plan doesn't list too many of these. The project manager often leads the risk identification effort, and most people don't wish to air their own weaknesses (assuming they even recognize them) in public. Nonetheless, issues like those listed here can make it harder for projects to succeed. If you don't confront such touchy issues, don't be surprised if they bite you at some point. Defined project tracking processes and clear project roles and responsibilities can address some of these conditions.

- Inadequate planning and task identification
- Inadequate visibility into project status
- Unclear project ownership and decision making
- Unrealistic commitments made, sometimes for the wrong reasons
- Managers or customers with unrealistic expectations
- Staff personality conflicts

Lack of Knowledge

Software technologies change rapidly and it can be difficult to find suitably skilled staff. As a result, our project teams might lack the skills we need. The key is to recognize the risk areas early enough so we can take appropriate preventive actions, such as obtaining training, hiring consultants, and bringing the right people together on the project team. Consider whether the following factors apply to your team:

- Lack of training
- Inadequate understanding of methods, tools, and techniques
- Insufficient application domain experience
- New technologies or development methods
- Ineffective, poorly documented, or ignored processes
- Technical approaches that might not work

Outsourcing

Outsourcing development work to another organization, possibly in another country, poses a whole new set of risks. Some of these are attributable to the acquiring organization, others to the supplier, and still others are mutual risks. If you are outsourcing part of your project work, watch out for the following risks:

- Acquirer's requirements are vague, ambiguous, incorrect, or incomplete.
- Acquirer does not provide complete and rapid answers to supplier's questions or requests for information.
- Supplier lacks appropriate software development and management processes.
- Supplier does not deliver components of acceptable quality on contracted schedule.
- Supplier is acquired by another company, has financial difficulties, or goes out of business.
- Supplier makes unachievable promises in order to get the contract.
- Supplier does not provide accurate and timely visibility into actual project status.
- Disputes arise about scope boundaries based on the contract.
- Import/export laws or restrictions pose a problem.
- Limitations in communications, materials shipping, or travel slow the project down.

Risk Management Components

Risk management is the application of appropriate tools and procedures to contain risk within acceptable limits. As with other project activities, begin risk management by developing a plan. The work aids that accompany this book include a risk management plan template; an outline of this template appears in Figure 6-1. The template document includes guidance that describes how to complete each section. This template is suitable for larger projects. Small projects can include a concise risk management plan as a section within the overall project management plan.

1. Purpose
2. Roles and Responsibilities
3. Risk Documentation
4. Activities
5. Schedule for Risk Management Activities
6. Risk Management Budget
7. Risk Management Tools

Appendix. Sample Risk Documentation Form

Figure 6-1 Risk management plan template.

Risk management consists of the subactivities illustrated in Figure 6-2 and described in the next section (Boehm 1989).

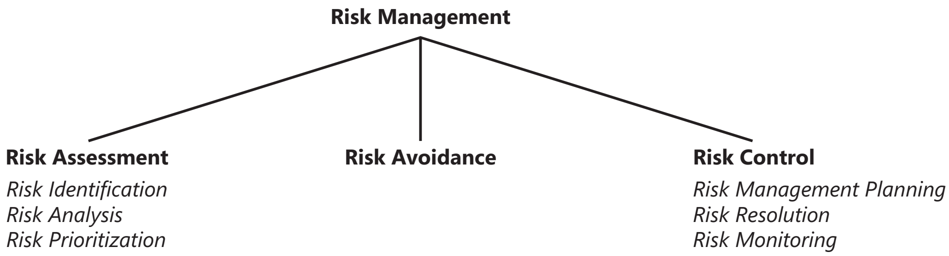

Figure 6-2 Components of risk management.

Risk Assessment

Risk assessment is the process of examining a project to identify areas of potential risk. *Risk identification* can be facilitated with the help of a checklist of common risk areas for software projects, such as the brief lists presented in this chapter. You might also study an organization-wide compilation of previously identified risks and mitigation strategies, both successful and unsuccessful. *Risk analysis* examines how project outcomes might change as a result of the identified risks.

Risk prioritization helps the project focus on its most severe risks by assessing the risk exposure. Exposure is the product of the probability of incurring a loss due to the risk and the potential magnitude of that loss. I usually estimate the probability from 0.1 (highly unlikely) to 1.0 (certain to happen), and the loss (also called impact) on a relative scale of 1 (no problem) to 10 (deep tapioca). Multiplying these factors together provides an estimate of the risk exposure due to each item, which can run from 0.1 (don't give it another thought) through 10 (stand back, here it comes!). It's simpler to estimate both probability and loss as High, Medium, or Low. Table 6-1 shows how you can estimate the risk exposure level as High, Medium, or Low by combining the probability and loss estimates. It's also a good idea to consider the time horizon during which a risk might pose a threat. Confront imminent risks more aggressively than those for which you still have some breathing space.

Table 6-1 Estimating Risk Exposure from Probability and Loss

	Loss		
Probability	**Low**	**Medium**	**High**
Low	*Low*	*Low*	*Medium*
Medium	*Low*	*Medium*	*High*
High	*Medium*	*High*	*High*

Risk Avoidance

Risk avoidance is one way to deal with a risk: don't do the risky thing! You might avoid risks by not undertaking certain projects, or by relying on proven rather than cutting-edge technologies when possible. In certain situations you might be able to transfer a risk to some other party, such as a subcontractor.

Risk Control

Risk control is the process of managing risks to achieve the desired outcomes. *Risk management planning* produces a plan for dealing with each significant risk, including mitigation approaches, owners, and timelines. *Risk resolution* entails executing the plans for dealing with each risk. Finally, *risk monitoring* involves tracking your progress toward resolving each risk item.

Let's look at an example of risk management planning. Suppose the "project" is to take a hike through a swamp in a nature preserve. You've been warned that the swamp might contain quicksand. So the risk is that we might step in quicksand and be injured or even die. One strategy to mitigate this risk is to reduce the probability of the risk actually becoming a problem. A second option is to consider actions that could reduce the impact of the risk if it does in fact become a problem. So, to reduce the probability of stepping in the quicksand, we might be on the alert, looking for signs of quicksand as we walk, and we might draw a map of the swamp so we can avoid these quicksand areas on future walks. To reduce the impact if someone does step in quicksand, perhaps the members of the tour group should rope themselves together. That way if someone does encounter some quicksand the others could quickly pull him to safety. In that way we reduce the impact of stepping in the quicksand. Although, of course, we still stepped in the quicksand.

Even better, is there some way to prevent the risk from becoming a problem under any circumstances? Maybe we build a boardwalk as we go so we avoid the quicksand. That will slow us down and it will cost some money. But, we don't have to worry about quicksand any more. The very best strategy is to eliminate the root cause of the risk entirely. Perhaps we should drain the swamp, but then it wouldn't be a very interesting nature walk. By taking too aggressive a risk approach, you can eliminate the factors that make a project attractive in the first place.

Documenting Risks

Simply identifying the risks facing a project is not enough. We need to write them down in a way that lets us communicate the nature and status of risks throughout the affected stakeholder community over the duration of the project. Figure 6-3 shows a form I've found to be convenient for documenting risks. It's a good idea to keep the risk list itself separate from the risk management plan, as you'll be updating the risk list frequently throughout the project.

ID: *<sequence number or a more meaningful label>*		
Description: *<List each major risk facing the project. Describe each risk in the form "condition-consequence.">*		
Probability: *<What's the likelihood of this risk becoming a problem?>*	**Loss:** *<What's the damage if the risk does become a problem?>*	**Exposure:** *<Multiply Probability times Loss.>*
First Indicator: *<Describe the earliest indicator or trigger condition that might indicate that the risk is turning into a problem.>*		
Mitigation Approaches: *<State one or more approaches to control, avoid, minimize, or otherwise mitigate the risk.>*		
Owner: *<Assign each risk mitigation action to an individual for resolution.>*	**Date Due:** *<State a date by which the mitigation approach is to be completed.>*	

Figure 6-3 A risk documentation form.

Use a *condition-consequence* format when documenting risk statements. That is, state the risk situation (the condition) that you are concerned about, followed by at least one potential adverse outcome (the consequence) if that risk should turn into a problem. Often, people suggesting risks state only the condition—"The customers don't agree on the product requirements"—or the consequence—"We can only satisfy one of our major customers." Pull those together into the condition-consequence structure: "The customers don't agree on the pr oduct requirements, so we'll only be able to satisfy one of our major customers." This statement doesn't describe a certain future, just a possible outcome that could harm the project if the condition isn't addressed.

Keep the items that have high risk exposures at the top of your priority list. You can't address every risk item, so use this prioritization mechanism to learn where to focus your risk control energy. Set goals for determining when each risk item has been satisfactorily controlled. Your mitigation strategies for some items may focus on reducing the probability, whereas the approach for other risks could emphasize reducing the potential loss or impact.

The cell in the form labeled Mitigation Approaches allows you to identify the actions you intend to take to keep the risk item under control. With any luck, some of your mitigation approaches will attack multiple risk factors. For example, one group with which I worked identified several risks related to failures of components of their Web delivery infrastructure (servers, firewall, e-mail interface, and so forth). A mitigation strategy that addressed several of those risks was to implement an automated monitoring system that could check the status of the servers and communication functions periodically and alert the team to any failures.

Figure 6-4 illustrates an alternative template for your risk list, which is also included in the process assets on the Web site that accompanies this book. This format includes essentially the same information that's in Figure 6-3 but it is laid out in a way that is amenable to storing in a spreadsheet or a table in a word-processing document. Storing the risks in a table or spreadsheet facilitates sorting the risk list by descending risk exposure.

Risk Tracking

As with other project management activities, you need to get into a rhythm of periodic monitoring. You may wish to appoint a risk manager or "risk czar" for the project. The risk manager is responsible for staying on top of the things that could go wrong, just as the project manager is staying on top of the activities leading to project completion. One project team dubbed their risk manager "Eeyore" after the Winnie-the-Pooh character who always bemoaned how bad things could become. It's a good idea to have someone other than the project manager serve as the risk manager. The project manager is focused on what he has to do to make a project succeed. The risk manager, in contrast, is identifying factors that might prevent the project from succeeding. In other words, the risk manager is looking for the black cloud around the silver lining that the project manager sees. Asking the same person to take these two opposing views of the project can lead to cognitive dissonance; in an extreme case, his brain can explode!

Keep the top 10 risks highly visible (McConnell 1996) and track the effectiveness of your mitigation approaches regularly. As the initial list of top priority items gradually gets beaten into submission, new risks might float up into the top 10. You can drop a risk off your radar when you conclude that your mitigation approaches have reduced the risk exposure from that item to an acceptable level.

> Assuming that a risk is controlled simply because the selected mitigation action has been completed. Controlling a risk might require you to change the risk control strategy if you conclude it is ineffective.

A student in a seminar once asked me, "What should you do if you have the same top five risks week after week?" A static risk list suggests that your risk mitigation actions aren't working. Effective mitigation actions should lower the risk exposure as the probability, the loss, or both decrease over time. If your risk list isn't changing, check to see whether the planned mitigation actions have been carried out and whether they had the desired effect.

> Failing to look for new risks that might arise during the course of the project. Conditions can change, assumptions can prove to be wrong, and other factors might lead to risks that weren't apparent or perhaps did not even exist at the beginning of the project.

ID	Description	P	L	E	First Indicator	Mitigation Approach	Owner	Date Due
	<List each major risk facing the project. Describe each risk in the form "condition – consequence". Example: "Subcontractor's staff does not have sufficient technical expertise, so their work is delayed for training and slowed by learning curve.">	**P*	*†L*	*‡E*	*<For each risk, describe the earliest indicator or trigger condition that might indicate that the risk is turning into a problem.>*	*<For each risk, state one or more approaches to avoid, transfer, control, minimize, or otherwise mitigate the risk. Accepting the risk is another option. Risk mitigation approaches should yield demonstrable results, so you can measure whether the risk exposure is changing.>*	*<Assign each risk action to an individual.>*	*<State a date by which each mitigation action is to be completed.>*

Key: **P*= Probability of occurrence of the risk, expressed as a number between 0.1 (highly unlikely) and 1.0 (guaranteed to happen). Alternatively, you could estimate this as Low, Medium, High.

†*L*= Relative loss if the risk does turn into a problem, expressed as a number between 1 (minimal impact) and 10 (catastrophe). Alternatively, you could estimate this as Low, Medium, High. Even better, estimate the actual loss in terms of calendar weeks for schedule impact, dollars for a cost impact, etc.

‡*E*= Risk Exposure. If numeric values were assigned to Probability and Loss, then Risk Exposure = P * L. If relative values were used (Low, Medium, High), estimate the overall risk exposure using Table 6-1.

Figure 6-4 An alternative risk list template.

Risk Management Can Be Your Friend

The skillful project manager will use risk management to raise awareness of conditions that could cause the project to go down the tubes. Consider a project that begins with a fuzzy product vision and no customer involvement. The astute project manager will spot this situation as posing potential risks and will document them in the risk list. Early in the project's life, the impact of this situation might not be too severe. However, if time passes and the lack of product vision and customer involvement are not improved, the risk exposure will steadily rise.

By reviewing the risk list periodically, the project manager can adjust the estimated probability and/or impact of these risks. The project manager can escalate risks that aren't being controlled to the attention of senior managers or other stakeholders. They can then either stimulate corrective actions or else make a conscious business decision to proceed in spite of the risks. In this way we're keeping our eyes open and making informed decisions, even if we can't control every threat the project faces.

Learning from the Past

We can't predict exactly which of the many threats to our projects might come to pass. However, most of us can do a better job of learning from previous experiences to avoid the same pain and suffering on future projects. As you begin to implement risk management approaches, record your actions and results for future reference. Try these suggestions:

- Record the results of even informal risk assessments, to capture the thinking of the project participants.
- Document the mitigation strategies attempted for each risk you chose to confront, noting which approaches worked well and which didn't pay off.
- Conduct retrospectives to identify the unanticipated problems that arose (see Chapter 15). Should you have been able to see them coming through better risk management, or would you likely have been blindsided in any case? Could these same problems occur on other projects? If so, add them to your growing checklist of potential risk factors for the next project to consider.

Anything you can do to improve your ability to avoid or minimize problems on future projects will improve your company's business success. Risk management can also reduce the chaos, frustration, and constant firefighting that impair the quality of work life in so many software organizations. The risks are out there. Find them before they find you.

Practice Activities

1. On Worksheet 6-1 list some risk categories that might threaten the success of your project. Identify several specific risk factors in each category.
2. Use Worksheet 6-2 to document several of the risks you identified in the previous practice activity. Be sure to describe each risk in the form of a condition followed by one or more possible consequences. Plan how you might control each risk.

Worksheet 6-1: Your Risk List

Risk Category	Specific Risks

Worksheet 6-2: Documenting Risks

ID	Description	P	L	E	First Indicator	Mitigation Approach	Owner	Date Due
1								
2								
3								
4								
5								
6								