Chapter 5

Risk Management

CONTENTS

This page intentionally left blank.

Chapter 5

Risk Management

5.1 Introduction

Risk is a product of the uncertainty of future events and is a part of all activity. It is a fact of life. We tend to stay away from those things that involve high risk to things we hold dear. When we cannot avoid risk, we look for ways to reduce the risk or the impact of the risk upon our lives. But even with careful planning and preparation, risks cannot be completely eliminated because they cannot all be identified beforehand. Even so, risk is essential to progress. The opportunity to succeed also carries the opportunity to fail. It is necessary to learn to balance the possible negative consequences of risk with the potential benefits of its associated opportunity. [1]

Risk may be defined as the possibility to suffer damage or loss. The possibility is characterized by three factors: [1]

1. The probability or likelihood that loss or damage will occur.
2. The expected time of occurrence.
3. The magnitude of the negative impact that can result from its occurrence.

The seriousness of a risk can be determined by multiplying the probability of the event actually occurring by the potential negative impact to the cost, schedule, or performance of the project:

Risk Severity = Probability of Occurrence • Potential Negative Impact

Thus, risks where probability is high and potential impact is very low, or vice versa, are not considered as serious as risks where both probability and potential impact are medium to high.

Project managers recognize and accept the fact that risk is inherent in any project. They also recognize that there are two ways of dealing with risk. One, risk management, is proactive and carefully analyzes future project events and past projects to identify potential risks. Once risks are identified, they are dealt with by taking measures to reduce their probability or reduce the impact associated with them. The alternative to risk management is crises management. It is a reactive and resource-intensive process, with available options constrained or restricted by events. [1]

Effective risk management requires establishing and following a rigorous process. It involves the entire project team, as well as requiring help from outside experts in critical risk areas (e.g., technology, manufacturing, logistics, etc.) Because risks will be found in all areas of the project and will often be interrelated, risk management should include hardware, software, integration issues, and the human element. [2]

5.2 Process Description

Various paradigms are used by different organizations to organize their risk manage management activities. A commonly used approach is shown in Figure 5-1. While there are variations in the different paradigms, certain characteristics are universally required for the program to be successful. These are listed below: [2]

- The risk management process is planned and structured.
- The risk process is integrated with the acquisition process.
- Developers, users, procurers, and all other stakeholders work together closely to implement the risk process.

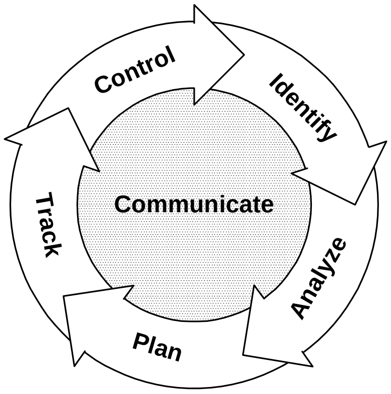


Figure 5-1 Software Engineering Institute Risk Management paradigm [3]

- Risk management is an ongoing process, with continual monitoring and reassessment.
- A set of success criteria is defined for all cost, schedule, and performance elements of the project.
- Metrics are defined and used to monitor effectiveness of risk management strategies.
- An effective test and evaluation program is planned and followed.
- All aspects of the risk management program are formally documented.
- Communication and feedback are an integral part of all risk management activities.

While your risk management approach should be tailored to the needs your project, It should incorporate these fundamental characteristics. The process is iterative and should have all the components shown in Figure 5-2. Note that while planning appears as the first step, there is a feedback loop from the monitoring activity that allows planning and the other activities to be redone or controlled by actual results, providing continual updates to the risk management strategy.

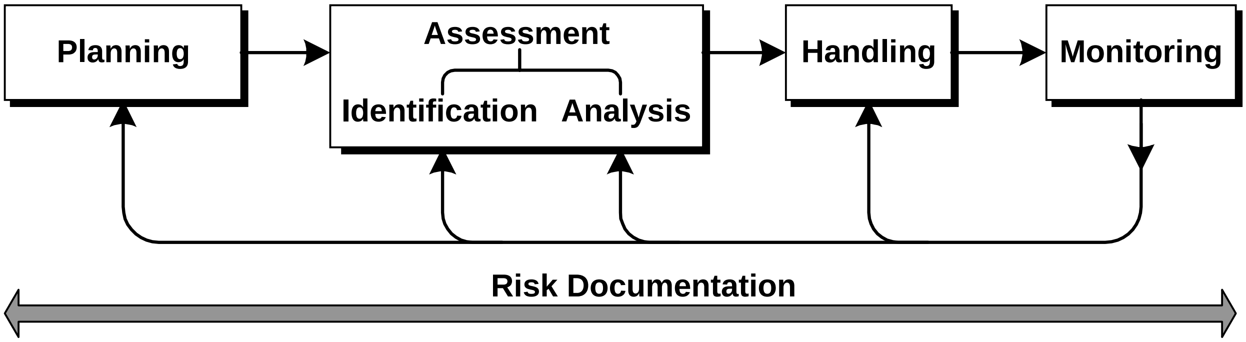


Figure 5-2 - Risk Management Process Example

In essence, the process is a standard approach to problem solving:

1. Plan or define the problem solving process.
2. Define the problem.
3. Work out solutions for those problems.
4. Track the progress and success of the solutions.

5.2.1 Planning

Risk planning includes developing and documenting a structured, proactive, and comprehensive strategy to deal with risk. Key to this activity is the establishment of methods and procedures to do the following:

- Establishing an organization to take part in the risk management process.
- Identify and analyze risks.
- Develop risk-handling plans.
- Monitoring or tracking risk areas.
- Assigning resources to deal with risks.

A generic example risk management plan can be found in Appendix B of the *Risk Management Guide for DoD Acquisition*. (See resources.)

5.2.2 Assessment

Risk assessment involves two primary activities, risk identification and risk analysis. Risk identification is actually begun early in the planning phase and continues throughout the life of the project. The following methods are often used to identify possible risks: [1]

- Brainstorming.
- Evaluations or inputs from project stakeholders.
- Periodic reviews of project data.
- Questionnaires based on taxonomy, the classification of product areas and disciplines.
- Interviews based on taxonomy.
- Analysis of the Work Breakdown Structure (WBS).
- Analysis of historical data.

When identifying a risk it is essential to do so in a clear and concise statement. It should include three components: [1]

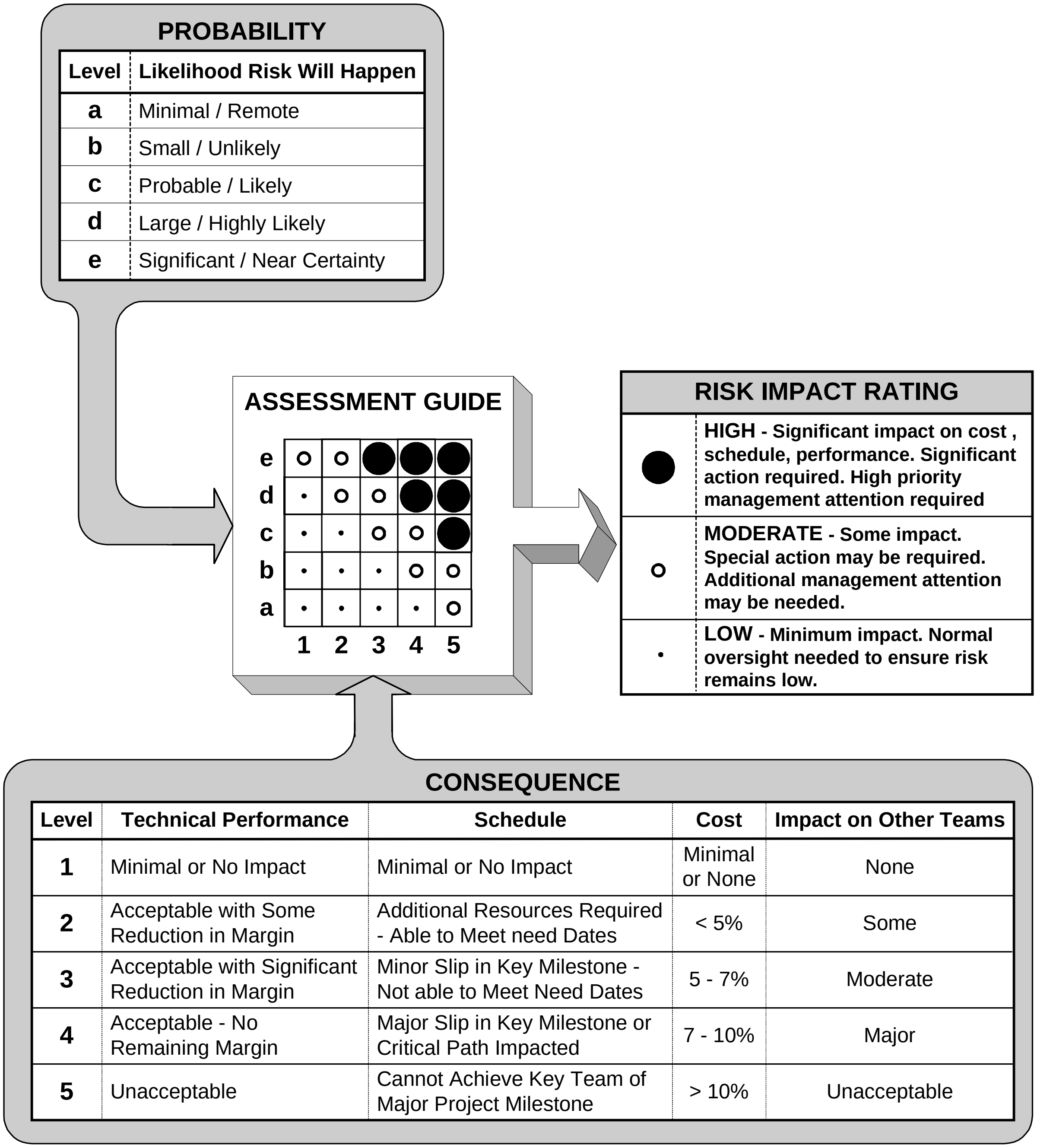
1. Condition - A sentence or phrase briefly describing the situation or circumstances that may have caused concern, anxiety, or uncertainty.
2. Consequence – A sentence describing the key negative outcomes that may result from the condition.
3. Context – Additional information about the risk to ensure others can understand its nature, especially after the passage of time.

The following is an example of a risk statement [1]:

Condition	End users submit requirements changes even though we're in the design phase and the requirements have been baselined.
Consequence	Changes could extend system design cycle and reduce available coding time.
Probability & Impact	80%. $2 million.
Mitigation Actions	Who, what, and when?

The other half of assessment is risk analysis. This is the process of examining each risk to refine the risk description, isolate the cause, quantify the probability of occurrence, and determine the nature and impact of possible effects. The result of this process is a list of risks rated and prioritized according to their probability of occurrence, severity of impact, and relationship to other risk areas. [2]

Once risks have been defined, with probability of occurrence and consequences assigned, the risk can be rated as to its severity. This facilitates prioritizing risks and deciding what level of resources to devote to the risk. Figure 5-3 depicts an assessment model using risk probability and consequence levels in a matrix to determine a level of risk severity. In addition to an overall method of risk rating, the model also gives good examples of probability levels, and types and levels of consequences. The ratings given in the assessment guide matrix are suggested minimum ratings. It may be necessary to adjust the moderate and high thresholds to better coincide with the type of project.



PROBABILITY

Level	Likelihood Risk Will Happen
a	Minimal / Remote
b	Small / Unlikely
c	Probable / Likely
d	Large / Highly Likely
e	Significant / Near Certainty

ASSESSMENT GUIDE

e	○	○	●	●	●
d	•	○	○	●	●
c	•	•	○	○	●
b	•	•	•	○	○
a	•	•	•	•	○
	1	2	3	4	5

RISK IMPACT RATING

●	**HIGH - Significant impact on cost , schedule, performance. Significant action required. High priority management attention required**
○	**MODERATE - Some impact. Special action may be required. Additional management attention may be needed.**
•	**LOW - Minimum impact. Normal oversight needed to ensure risk remains low.**

CONSEQUENCE

Level	Technical Performance	Schedule	Cost	Impact on Other Teams
1	Minimal or No Impact	Minimal or No Impact	Minimal or None	None
2	Acceptable with Some Reduction in Margin	Additional Resources Required - Able to Meet need Dates	< 5%	Some
3	Acceptable with Significant Reduction in Margin	Minor Slip in Key Milestone - Not able to Meet Need Dates	5 - 7%	Moderate
4	Acceptable - No Remaining Margin	Major Slip in Key Milestone or Critical Path Impacted	7 - 10%	Major
5	Unacceptable	Cannot Achieve Key Team of Major Project Milestone	> 10%	Unacceptable

Figure 5-3 Defense Acquisition University Assessment Model [4]

5.2.3 Handling

Risk handling is the process that identifies, evaluates, selects, and implements options for mitigating risks, as shown in Figure 5-3. Two approaches are used in handling risk. The first is to employ options that reduce the risk itself. This usually involves a change in current conditions to lessen the probability of occurrence. The second approach, often employed where risk probability is high, is to use options that reduce the negative impact to the project if the risk condition should occur. Improving jet engine maintenance and inspection procedures to reduce the risk of in-flight engine failure is an example of the first approach. Providing a parachute for the pilot, to reduce loss if the risk condition should occur, is an example of the second.

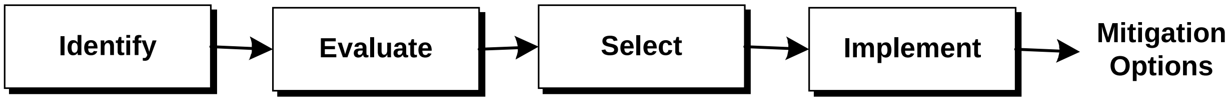


Figure 5-3 Risk Handling Process

5.2.4 Monitoring

Risk monitoring is the process of continually tracking risks and the effectiveness of risk handling options to ensure risk conditions do not get out of control. This is done by knowing the baseline risk management plans, understanding the risks and risk handling options, establishing meaningful metrics, and evaluating project performance against the established metrics, plans, and expected results throughout the acquisition process. Continual monitoring also enables the identification of new risks that may become apparent over time. It also discovers the interrelationships between various risks. [2]

The monitoring process provides feedback into all other activities to improve the ongoing, iterative risk management process for the current and future projects.

5.2.5 Documentation

Risk documentation is absolutely essential for the current, as well as future, projects. It consists of recording, maintaining, and reporting risk management plans, assessments, and handling information. It also includes recording the results of risk management activities, providing a knowledge base for better risk management in later stages of the project and in other projects. [2] Documentation should include as a minimum the following information:

- Risk management plans.
- Project metrics to be used for risk management.
- Identified risks and their descriptions.
- The probability, severity of impact, and prioritization of all known risks.
- Description of risk handling options selected for implementation.
- Project performance assessment results, including deviations from the baseline plans.
- A record of all changes to the above documentation, including newly identified risks, plan changes, etc.

5.3 Risk Management Checklist

This checklist is provided as to assist you in risk management. If you answer “no” to any of these questions you should examine the situation carefully for the possibility of greater risks to the project. This is only a cursory checklist for such an important subject. Please see the reference documents for more detailed checklists. [5] [6]

❑ 1. Do you have a comprehensive, planned, and documented approach to risk management?

❑ 2. Are all major areas/disciplines represented on your risk management team?

❑ 3. Is the project manager experienced with similar projects?

❑ 4. Do the stakeholders support disciplined development methods that incorporate adequate planning, requirements analysis, design, and testing?

❑ 5. Is the project manager dedicated to this project, and not dividing his or her time among other efforts?

❑ 6. Are you implementing a proven development methodology?

❑ 7. Are requirements well defined, understandable, and stable?

❑ 8. Do you have an effective requirements change process in place and do you use it?

❑ 9. Does your project plan call for tracking/tracing requirements through all phases of the project?

❑ 10. Are you implementing proven technology?

- ❑ 11. Are suppliers stable, and do you have multiple sources for hardware and equipment?
- ❑ 12. Are all procurement items needed for your development effort short-lead time items (no long-lead items?)
- ❑ 13. Are all external and internal interfaces for the system well defined?
- ❑ 14. Are all project positions appropriately staffed with qualified, motivated personnel?
- ❑ 15. Are the developers trained and experienced in their respective development disciplines (i.e. systems engineering, software engineering, language, platform, tools, etc.?)
- ❑ 16. Are developers experienced or familiar with the technology and the development environment?
- ❑ 17. Are key personnel stable and likely to remain in their positions throughout the project?
- ❑ 18. Is project funding stable and secure?
- ❑ 19. Are all costs associated with the project known?
- ❑ 20. Are development tools and equipment used for the project state-of-the-art, dependable, and available in sufficient quantity, and are the developers familiar with the development tools?
- ❑ 21. Are the schedule estimates free of unknowns?
- ❑ 22. Is the schedule realistic to support an acceptable level of risk?
- ❑ 23. Is the project free of special environmental constraints or requirements?
- ❑ 24. Is your testing approach feasible and appropriate for the components and system?
- ❑ 25. Have acceptance criteria been established for all requirements and agreed to by all stakeholders?
- ❑ 26. Will there be sufficient equipment to do adequate integration and testing?
- ❑ 27. Has sufficient time been scheduled for system integration and testing?
- ❑ 28. Can software be tested without complex testing or special test equipment?
- ❑ 29. Is the system being developed by a single group in one location?
- ❑ 30. Are subcontractors reliable and proven?
- ❑ 31. Is all project work being done by groups over which you have control?
- ❑ 32. Are development and support teams all collocated at one site?
- ❑ 33. Is the project team accustomed to working on an effort of this size (neither bigger nor smaller?)

5.4 Regulations

- DCMA Directive 1, Contract Management "One Book", 0.0 -- Operating Principles.
- DoD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, Part 2; 2.5, Risk, and Part 6; 6.7, Technology Protection.
- DoD Directive 5000.1 The Defense Acquisition System (October 23, 2000).
- DoD Manual 5000.4-M, Cost Analysis Guidance and Procedures.
- DoDD 5000.4, OSD Cost Analysis Improvement Group (CAIG).
- FAR -- Part 39; Acquisition of Information Technology; (FAC 97-27); 25 June 2001.
- OMB Circular A-109, Major System Acquisition, Para 7, Major System Acquisition Management Objectives.
- Supplement to OMB Circular A-11, Part 3, Planning, Budgeting, and Acquisition of Capital Assets, Appendix Six, Risk Management in the Procurement Phase.
- The Information Technology Acquisition Reform act of 1996 (also known as the Clinger-Cohen Act).

5.5 References

[1] Software Technology Support Center Course: *Life Cycle Software Project Management*, Project Initiation, 9 October 2001.

[2] *Risk Management Guide for DoD Acquisition*, Chapter 2, February 2001. www.dsmc.dsm.mil/pubs/gdbks/risk_management.htm

[3] Higuera, Ron & Haimes, Yacov, "Software Risk Management," Technical Report, 1996. www.sei.cmu.edu/publications/documents/96.reports/96.tr.012.html

[4] *Risk Management Guide for DoD Acquisition*, Appendix B, February 2001.

[5] Arizona State University (ASU), "Question List for Software Risk Identification." www.eas.asu.edu/~riskmgmt/qlist.html

[6] Department of Energy, Risk Assessment Questionnaire. http://cio.doe.gov/sqse/pm_risk.htm

5.6 Resources

Arizona State University software risk management resources: www.eas.asu.edu/~riskmgmt/

Guidelines for the Successful Acquisition and Management of Software-Intensive Systems (GSAM), Version 3.0, Chapter 6, OO-ALC/TISE, May 2000. Download at: www.stsc.hill.af.mil/gsam/guid.asp

Crosstalk Magazine: www.stsc.hill.af.mil/crosstalk/

- "A Practical Approach to Quantifying Risk Evaluation Results": www.stsc.hill.af.mil/crosstalk/2000/feb/hantos.asp
- "A Risk Management Bibliography": www.stsc.hill.af.mil/crosstalk/1994/mar/xt94d03k.asp
- "Continuing Risk Management at NASA": www.stsc.hill.af.mil/crosstalk/2000/feb/rosenberg.asp
- "Identifying and Managing Risks for Software Process Improvement": www.stsc.hill.af.mil/crosstalk/2000/feb/risk.asp
- "Managing Risk Management": www.stsc.hill.af.mil/crosstalk/1999/jul/neitzel.asp
- "Managing Risk with TSP": www.stsc.hill.af.mil/crosstalk/2000/jun/webb.asp
- "Risk Management in Practice": www.stsc.hill.af.mil/crosstalk/1997/apr/management.asp
- "Team Risk Management": www.stsc.hill.af.mil/crosstalk/1995/jan/teamrisk.asp

Department of Energy, Software Risk Management Practical Guide: http://cio.doe.gov/sqse/pm_risk.htm

Department of Justice, *Systems Development Life Cycle Guidance Document*, Risk Management, Chapter 3: www.usdoj.gov/jmd/irm/lifecycle/table.htm

Higuera, Dorofee, Walker, & Williams, "Team Risk Management: A New Model for Customer Supplier Relationships," 1994. Download at: www.sei.cmu.edu/publications/documents/94.reports/94.sr.005.html

Higuera, Ron, et. Al., *Continuous Risk Management Guidebook*, 1996, CMU.

Program Manager's Guide for Managing Software, 0.6, 29 June 2001, Chapter 5: www.geia.org/sstc/G47/SWMgmtGuide%20Rev%200.4.doc

Risk Management Guide for DoD Acquisition, 2001. Download at: www.dsmc.dsm.mil/pubs/gdbks/risk_management.htm

Risk Radar, Software for managing risk. Available at: www.iceincusa.com/rskrdr.htm

Software Engineering Institute, Risk management overview: www.sei.cmu.edu/programs/sepm/risk/

Software Engineering Institute , risk management frequently asked questions: www.sei.cmu.edu/programs/sepm/risk/risk.faq.html

US Treasury, Systems Development Life Cycle Handbook, Risk Management Processes, Chapter 5. Download: www.customs.ustreas.gov/contract/modern/sdlcpdfs/tocsdlc.htm

This page intentionally left blank.