Carnegie Mellon University
Software Engineering Institute

Continuous Risk Management Guidebook

Audrey J. Dorofee

Julie A. Walker

Christopher J. Alberts

Ronald P. Higuera

Richard L. Murphy

Ray C. Williams

19970108 045

DTIC QUALITY INSPECTED 3

This document was prepared for the

SEI Joint Program Office
HQ ESC/ENS
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this document should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Thomas R. Miller, Lt Col, USAF
SEI Joint Program Office

Preface

Background

The Software Engineering Institute (SEI), a federally funded research and development center and part of Carnegie Mellon University in Pittsburgh, Pennsylvania, has been formally studying and developing risk management concepts since January, 1990 as an efficient means to improve the success of programs developing software-intensive systems.

A project was formed in 1992 to focus on
- the joint management of risks between customers and suppliers (we refer to this as Team Risk Management)
- the continuous practice of risk management (we refer to this as Continuous Risk Management)

Our knowledge and experience with Continuous Risk Management is collected in this guidebook. We plan to follow up with a guidebook on Team Risk Management. Our work has included long-term collaborative development work with clients to revise and improve the risk management practice, including processes, methods, and tools.

As the acquisition community streamlines and adopts new, more effective paradigms, we see cooperative approaches such as team risk management gaining acceptance and use.

Why a Book on Continuous Risk Management?

Although we could have waited for the completion of work on Team Risk Management and produced one guidebook, we felt that there was a community that needed to know about risk management within a project, how to perform it, and how to implement it. Indeed, the first draft of this guidebook was the Team Risk Management Guidebook; it was too much for one book, and too confusing for our audience. So we split it into two books and concentrated on completing the Continuous Risk Management part first. The purpose was to put into the hands of the community a book that would enable them to implement risk management within projects. Joint risk management between customers, suppliers, and subcontractors could be addressed later.

Another reason for publishing this guidebook now is that risk management is a key practice within the framework of the Software Acquisition Capability Maturity Model (SA-CMM^{SM})[1] and is expected to become a key process area within the Software Capability Maturity Model (SW-CMM^{SM})[2] in the future.

Book Purpose and Scope

The purpose of this guidebook is to explain what Continuous Risk Management is; to help you understand the principles, functions, methods, and tools; to show what it could look like when implemented within a project; and to show you how a project could implement its own adaptation. The intent is not to provide a "cookie-cutter" answer for everyone. There is no such answer. This is a generic practice with a variety of methods and tools from which to choose. It is meant to be adapted to suit an organization and a project.

Is Anything Else Needed?

Just as no "solution" fits all problems, no guidebook could hope to be complete for all readers and their needs. Additional or supplementary training may be required or desired by some organizations. Organizations can accelerate their adoption of these practices through a service to adapt the risk management practice documented in this guidebook. Does everyone need these services? No; but we intend to provide them for those who do.

---

1. The SA-CMM is being published at the time of this writing.
2. CMM and Capability Maturity Model are service marks of Carnegie Mellon University.

Intended Audience

Everyone in a project needs to actively participate for risk management to be effective. Therefore, this guidebook, whole or in part, is aimed at everyone involved in a project. It is also targeted towards sponsors of change and improvement as well as change agents and champions who help the process of improvement and transition. Not everyone needs to read the entire guidebook. Part 1 provides a detailed table identifying which parts should be read by whom.

Where Did This Come From?

The contents of this book are a compilation of what we have read, learned, tested, and experienced over the last six years. Many clients have contributed, in varying degrees, to the methods, guidelines, and tips in this book. Observations of successes and failures clarified the principles that we use. Successful and less-than-successful experiments with clients helped us to refine and develop new methods and tools that are, we hope, of a practical nature.

What We Hope You Get From this Book

We hope that readers will be able to take the ideas presented here and implement a successful risk management practice in their projects and organizations, achieving improvements in their ability to deliver quality systems on-time and within budget. But even if all you take from this book is a handful of ideas to help you improve your practices, we will consider the book a success.

Where We Go From Here

As we continue to work with clients and expand our use of the World Wide Web, we intend to produce at least one, perhaps two, more versions or addendums to this guidebook, focusing on new methods and tools. The rapid expansion of the capability embodied in the World Wide Web holds promise for promoting and collecting best practices and new methods. So although the exact media by which additional information about Continuous Risk Management will be provided to the community is unknown, we do intend to provide it.

Final Words

We sincerely hope you will find this book to be of use to you. We welcome any and all feedback from our readers (see Chapter 20, Section 2).

Acknowledgments

**Document
Production
Assistance**

Finally, we wish to acknowledge the hard work and dedication of all those involved in the building, editing, graphic design, and production of this document:

- Mary Lou Moore
- Eileen C. Forrester
- Bob Lang
- Mark Lotter
- Skip Shelly
- Barbara White
- Pennie Walters

Table of Contents

Part 1

Introduction

Introduction

This part introduces the readers to Continuous Risk Management and how to use this guidebook. Chapter 1 focuses on why Continuous Risk Management is important, why people don't do risk management, and the costs and benefits of performing risk management. The chapter ends with a discussion of the principles of Continuous Risk Management. Chapter 2 focuses on how this guidebook is organized and how the readers may want to navigate the guidebook based on their role or function within their organization.

Chapter

Chapter 1

Introduction to Continuous Risk Management
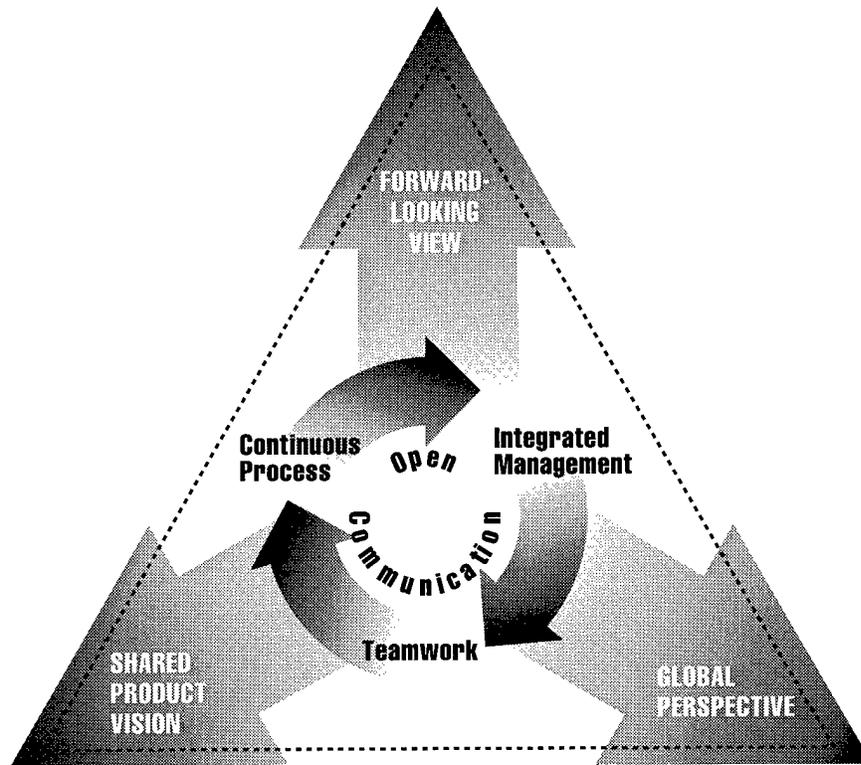
Continuous Risk Management Principles

Section 1

Why Do Continuous Risk Management?

Why Manage Risks?

Everybody agrees that risk management, if done properly, is a good thing to do. Who wouldn't want to identify potential problems early enough to make a difference in the ultimate quality of the product? Continuous Risk Management "helps people avoid disasters, avoid rework, avoid overkill, and stimulate win-win situations on software projects [Boehm 89, p. 1]." Risk management reduces a project's risk exposure and reducing exposure makes good business sense [Charette 89].

Reasons We Don't Do Risk Management

If it's so wonderful, why don't we do it or why do we fail to do it successfully? Here are some of the reasons project personnel give for not doing risk management. All of these reasons are barriers to effective risk management. Some of them are cultural barriers. All of them need to be overcome.

- ❑ I don't have the time. There's too much regular project work to do.

- ❑ It's not rewarded. Nobody wants to hear about what we can't do.

- ❑ It's a bureaucratic nightmare. The processes are too complicated and time consuming.

- ❑ I don't want to look stupid, especially in front of upper management.

- ❑ We already know our risks. We did an assessment at the beginning of the project. Once is enough!

- ❑ This is just another management initiative. I'll wait to see if they're serious before I put any effort into it. Why waste time and energy?

- ❑ They shoot the messenger. If I had a solution I wouldn't need to bring it up in the first place.

- ❑ Identifying risks means you need to solve them. We already have enough to do.

- ❑ _____(Fill in your own)

What is Continuous Risk Management?

Continuous Risk Management is a software engineering practice with processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making to
- assess continuously what could go wrong (risks)
- determine which risks are important to deal with
- implement strategies to deal with those risks

Note: Project and program are considered synonymous terms in this document.

Benefits of Continuous Risk Management

Continuous Risk Management, when performed successfully, provides a number of benefits:

- *prevents problems before they occur*: identifies potential problems and deals with them when it is easier and cheaper to do so—before they are problems and a crisis exists
- *improves product quality*: focuses on the project's objective and consciously looks for things that may affect quality throughout product development
- *enables better use of resources*: allows the early identification of potential problems (the proactive approach) and provides input into management decisions regarding resource allocation
- *promotes teamwork*: involves personnel at all levels of the project and focuses their attention on a shared product vision and provides a mechanism for achieving it.

Costs of Continuous Risk Management

There are three types of costs associated with Continuous Risk Management:

- *infrastructure costs*: those costs associated with implementing and supporting risk management within an organization (e.g., setting up a training program, purchasing common tools)
- *risk management costs*: those costs associated with conducting risk management activities within a project (e.g., time to document new risks or write risk status reports)
- *mitigation costs*: those costs directly associated with mitigating a specific risk to the project (e.g., the cost to carry out the mitigation plans)

These types of cost typically include "expenditure of funds, time, personnel, and management involvement [Charette 89, p. 69]."

Cost vs. Benefit

Determining cost-benefit value is difficult when some costs and benefits cannot be quantified. For example, how do you quantify what you saved by mitigating a risk? How do you estimate what it would have cost you if it had become a problem [Charette 89]? There are no clear-cut answers.

The cost of performing Continuous Risk Management must be balanced against the expected benefits and the cost of not doing risk management [Charette 89].

Example: A major acquisition program manager from the Department of the Defense learned about a risk that could have a been a "showstopper" for the program. Through Continuous Risk Management, a risk was identified regarding achievement of the specified gross aircraft weight. Added equipment to satisfy specific new mission requirements might increase the weight beyond allowable limits. Early identification and better definition of the risk enabled the program manager to justify funding for an early start of the design, thereby ensuring proper aircraft weight in time to meet the program schedule. This example illustrates a risk identified through Continuous Risk Management that could have stopped the program if it had gone unnoticed until it became a problem. For this program manager, the mitigation of this risk saved what would have been a year's delay in the program schedule, clearly worth the expense of performing risk management.

How Should I Do Continuous Risk Management?

Continuous Risk Management is simply an area of emphasis of every day business. It should be ongoing and comfortable. Like any good habit, it should seamlessly fit into your daily work. There is no one special set of methods, tools, or communication mechanisms that will work for every project. The key is to adhere to the principles, perform the functions, and adapt the practice to suit your needs. The principles are described in the next section and the functions are described in Part 2. Part 3 provides an example of how these principles and functions might look when implemented in a project. Part 4 of this document will describe a process of installing and adapting Continuous Risk Management to your project.

Section 2

What Are the Principles of Continuous Risk Management?

Introduction   Continuous Risk Management is built upon a set of principles that provide an effective approach to managing risk regardless of the specific methods and tools used. These principles, as depicted below [Higuera 94], break down into three types: core, sustaining, and defining.

Continuous Risk Management Principles

Defining Principles

Sustaining Principles
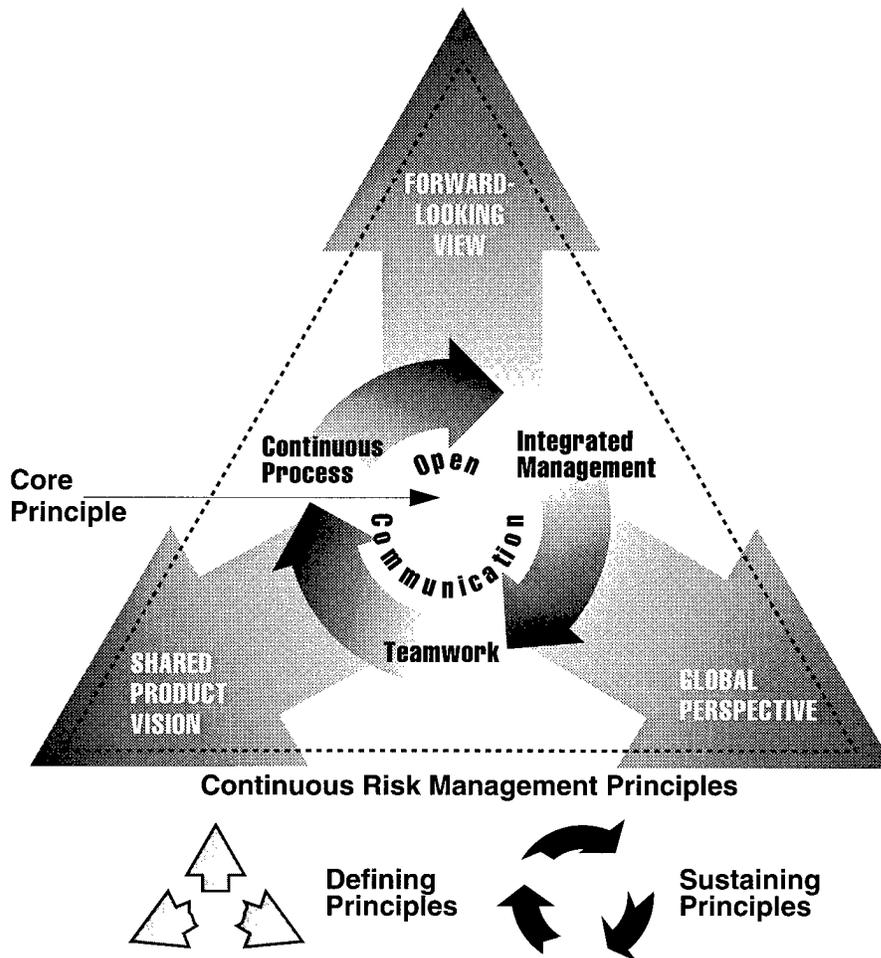
Core Principle   Continuous Risk Management simply cannot succeed without the constant attention to fostering **open communication,** the *core* principle. No one can find the risks to the project as well as the people who work on it day in and day out. Always ask, "Is the way the project responds when members bring forward issues and concerns going to encourage them to bring more?" Open communication requires

- encouraging free-flowing information at and between all project levels
- enabling formal, informal, and impromptu communication
- using consensus-based processes that value the individual voice (bringing unique knowledge and insight to identifying and managing risk)

Defining Principles

The *defining* principles focus on how the project sees risks, and how ambitious it is about looking for and dealing with uncertainty. The principles foster the development of a shared view that clarifies the when, why, and what of Continuous Risk Management.

Forward-looking view: Develop the ability to look ahead, beyond today's crisis to the consequences of that crisis and of the decisions the project makes to deal with it. This principle is also concerned with sharpening the view of how far into the future to look. Forward-looking view requires

- thinking toward tomorrow, identifying uncertainties, anticipating potential outcomes
- managing project resources and activities while anticipating uncertainties

Shared product vision: This is the development of a common understanding of the objectives of the project and the goods and services it will produce for the world. Shared product vision requires

- arriving at a mutual product vision based upon common purpose, shared ownership, and collective commitment
- focusing on results

Global perspective: This requires project members to escape the local interests of groups within the project and within the organization to reach a common view of "what's most important to the project." Project members should develop a common viewpoint at a global level, and be able to move toward deciding how to mitigate specific risks. Global perspective requires

- viewing software development within the context of the larger systems-level definition, design, and development
- recognizing both the potential value of opportunity and the potential impact of adverse effects

Sustaining Principles

The *sustaining* principles focus on how the project goes about its daily business of Continuous Risk Management. These are foundational. If established early in the project and constantly nurtured, these will assure that Continuous Risk Management becomes the way business is conducted.

Integrated management: This principle is concerned with assuring that Continuous Risk Management processes, paperwork, and discipline are consistent with established project culture and practice. Continuous Risk Management is simply an area of emphasis of good project management; therefore, wherever possible, Continuous Risk Management tasks should be integrated into well-established project routine. Integrated management requires

- making Continuous Risk Management an integral and vital part of project management
- adapting Continuous Risk Management methods and tools to a project's infrastructure and culture

Teamwork: No single person can anticipate all the risks that face the project. Continuous Risk Management requires that the project members find, analyze, and work risks together. Group synergy, reliance, and cooperation in dealing with risk need to be rewarded.

Teamwork requires
- working cooperatively to achieve a common goal
- pooling talent, skills, and knowledge

Continuous process: Risk management must not be allowed to become "shelfware." The processes must be part of daily, weekly, monthly, and quarterly project management. Stamp out the idea that risk management only happens during "risk management season." Continuous process requires

- sustaining constant vigilance
- identifying and managing risks routinely throughout all phases of the project's life cycle

Principles and Tailoring Continuous Risk Management Processes

Continuous Risk Management is not "one size fits all." To be effective, tailoring is needed. Tailoring occurs when organizations adapt the Continuous Risk Management processes and select methods and tools which best fit with their project management practice and their organizational culture. Following the principles of Continuous Risk Management is the key to successful tailoring.

Section 3

References

Cited in this chapter:

[Boehm 89]   Boehm, Barry. *IEEE Tutorial on Software Risk Management*. New York: IEEE Computer Society Press, 1989.

[Charette 89]   Charette, Robert N. *Software Engineering Risk Analysis and Management*. New York: McGraw-Hill, 1989.

[Higuera 94]   Higuera, Ronald P.; Dorofee, Audrey J.; Walker, Julie A.; & Williams, Ray C. *Team Risk Management: A New Model for Customer-Supplier Relationships* (CMU/SEI-94-SR-05). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

For more information on software development risk, see the following:

[Van Scoy 92]   Van Scoy, Roger L. *Software Development Risk: Opportunity, Not Problem* (CMU/SEI-92-TR-30, ADA 258743). Pittsburgh, Pa.: Software Engineering Institute, 1992.

Chapter 2

How to Use This Guidebook

Guidebook Organization
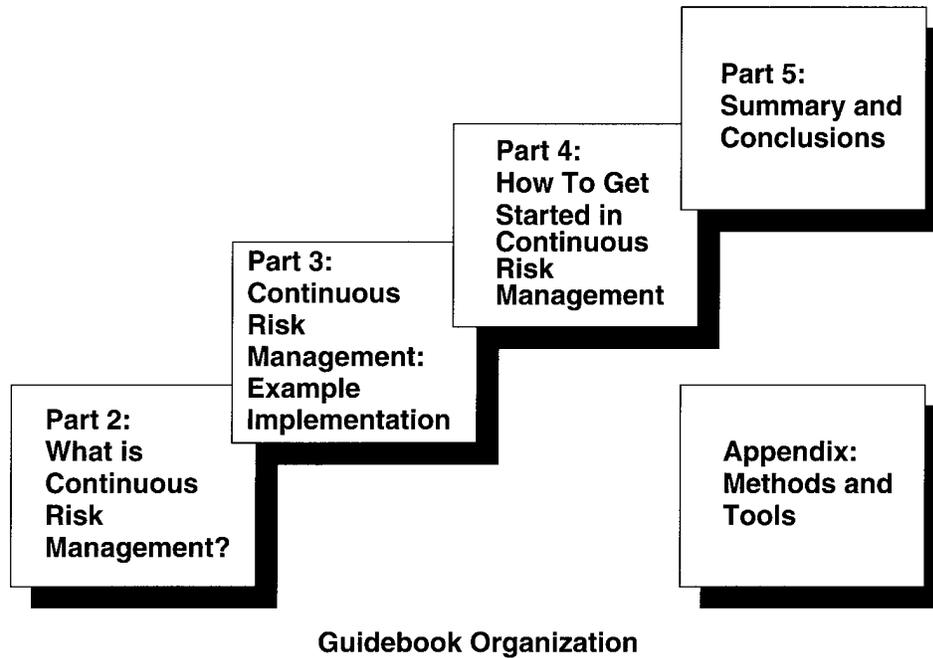
Section	
What's in This Guidebook?	12
How Should I Use the Guidebook?	15
References	16

Section 1

What's in This Guidebook?

Why this Guidebook?

In working with many organizations who are piloting risk management efforts, the SEI Risk Management Program has had the opportunity to see what these organizations did, what they struggled with, and, ultimately, what lessons were learned that could be applied to other efforts. This guidebook contains what the program has learned to date in helping organizations implement Continuous Risk Management.

Software vs. System Risk Management

This guidebook primarily deals with performing Continuous Risk Management with a software development focus but can also be used to address systems, hardware, and other domains. Only a few of the methods are specifically focused on software.

Guidebook Organization

This guidebook separates the "what" of risk management from the "how to do it." The following table outlines the guidebook organization.

Part	Content	Purpose
Part 2	What is Continuous Risk Management?	Provide an overview of terminology, processes, and functions
Part 3	Continuous Risk Management: Example Implementation	Illustrate Continuous Risk Management as implemented in a typical project
Part 4	How to Get Started in Continuous Risk Management	Provide instructions for a project or organization to implement Continuous Risk Management
Part 5	Summary and Conclusions	Summarize Continuous Risk Management and describe future directions for SEI work
Appendix	Methods and Tools	Describe methods and tools used in Continuous Risk Management

Guidebook Format

This document was structured and formatted based on the guidelines and formats provided by an Information Mapping® seminar given by Information Mapping, Inc. The most visible aspect of this format is the use of **labels** for each block of information to enable the reader to quickly scan the document for relevant information. The document is divided into five major **parts**, each part having **chapters**, each chapter having **sections**. Parts and chapters each start with a detailed list of the contents.

Part 2: What is Continuous Risk Management?

Part 2 provides the foundation for what the SEI Risk Management Program means by Continuous Risk Management. Risk terminology is defined and the SEI risk management paradigm (see diagram below) is described. A chapter is devoted to each paradigm function, which includes a function diagram (see diagram below) outlining the required inputs to the function, any constraints, supporting information, the activities involved, and the output. Associated methods and tools are listed and described in detail in the appendix.
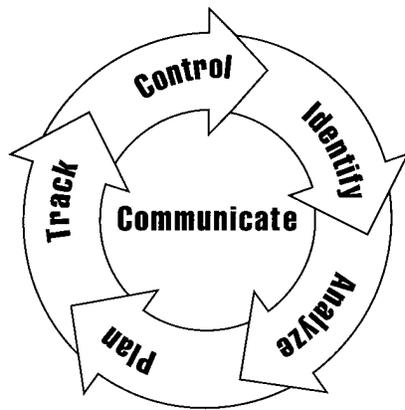
SEI Risk Management Paradigm
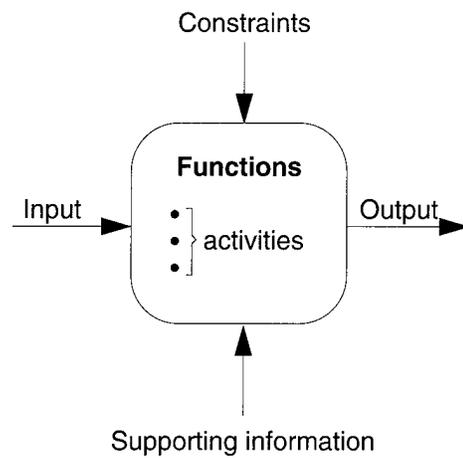
Function Diagram

**Part 3:
Continuous
Risk
Management:
Example
Implementation**

Part 3 provides one view of Continuous Risk Management implemented within a project. An example implementation (see diagram below) is used to provide a framework for showing how an organization might tailor the Continuous Risk Management practice to fit their environment. Internal and external risk communication on a project is discussed and a risk example is taken through a life-cycle from identification through closure.
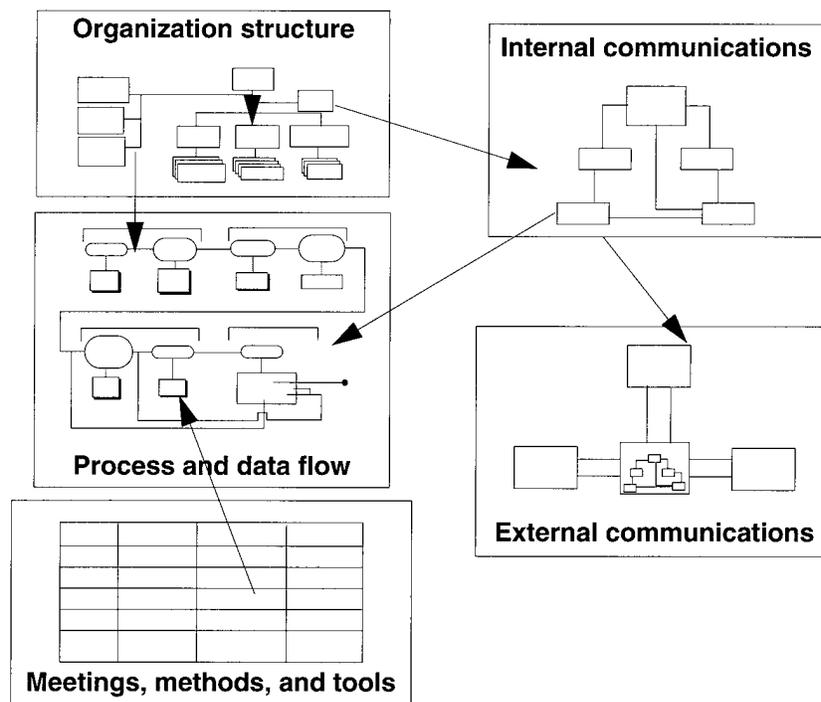
Example Implementation

Part 4: How to Get Started in Continuous Risk Management

Part 4 focuses on how an organization can implement Continuous Risk Management within a project. An application roadmap (see diagram below) is provided describing what aspects to work on first and how to continue to build an effective risk management practice including helpful guidelines and tips.
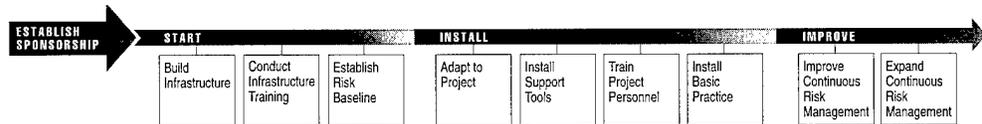
Continuous Risk Management Application Roadmap

Part 5: Summary and Conclusions

Part 5 summarizes the activities for each function of the paradigm (described in Part 2), the key elements of a successful implementation of Continuous Risk Management (described in Part 3), and the key elements for implementing Continuous Risk Management (described in Part 4). Considerations for future directions in work at the SEI on risk management are also presented.

Appendix: Methods and Tools

The appendix contains all the methods and tools referenced throughout this guidebook. Methods provide systematic approaches to performing the Continuous Risk Management processes and include procedures and guidelines and tips. Tools include templates and forms along with an example. Tools described within methods are either tools that are specific to the method or are examples of more general tools described elsewhere in the appendix.

Method
- description
- when to use
- procedure
- tools (if applicable)
- guidelines and tips

Tool
- description
- how to use
- example
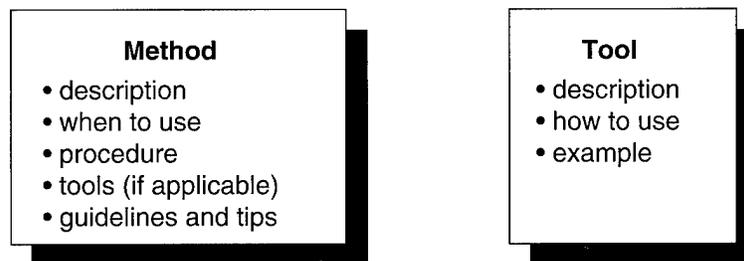
Method and Tool Content

Section 2

How Should I Use the Guidebook?

**Where Should
I Begin?**

Depending on an individual's role or function in the organization, different parts of this guidebook will be of more interest than others. The table below provides a suggested way to navigate this guidebook, depending on that role or function.

Role/Function	Desire	Guidebook Parts
Oversee Continuous Risk Management practice (e.g., project manager, sponsor)	Gain general understanding of Continuous Risk Management and why it should be done	Part 1: Introduction Part 3: Continuous Risk Management: Example Implementation Part 5: Summary and Conclusions
Coordinate/ develop Continuous Risk Management practice (e.g., technical managers or leads)	Learn what it is, how to build tailored processes, and alternative methods and tools	Part 1: Introduction Part 2: What is Continuous Risk Management? Part 3: Continuous Risk Management: Example Implementation Part 4: How to Get Started in Continuous Risk Management Part 5: Summary and Conclusions Appendix: Methods and Tools
Participate in Continuous Risk Management (e.g., software engineers, hardware engineers, testers, etc.)	Understand the Continuous Risk Management processes and how to perform the methods and tools	Part 1: Introduction Part 2: What is Continuous Risk Management? Part 3: Continuous Risk Management: Example Implementation Appendix: Methods and Tools (for specific methods and tools)
Improve organization processes (e.g., change agents, process improvement groups [e.g., Software Engineering Process Group[a] (SEPG)])	Learn what it is and how it can be used to help projects get started	Part 1: Introduction Part 2: What is Continuous Risk Management? Part 3: Continuous Risk Management: Example Implementation Part 4: How to Get Started in Continuous Risk Management Part 5: Summary and Conclusions Appendix: Methods and Tools

a. "The software engineering process group is the focal point for process improvement. Composed of line practitioners who have varied skills, the group is at the center of the collaborative effort of everyone in the organization who is involved in software process improvement" [Fowler 90, p. 13].

Section 3

References

Cited in this chapter:

[Fowler 90]   Fowler, Priscilla J.; Rifkin, Stan; & Card, David N. *Software Engineering Process Group Guide* (CMU/SEI-90-TR-24, ADA235784). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1990.

Part 2

What Is Continuous Risk Management?
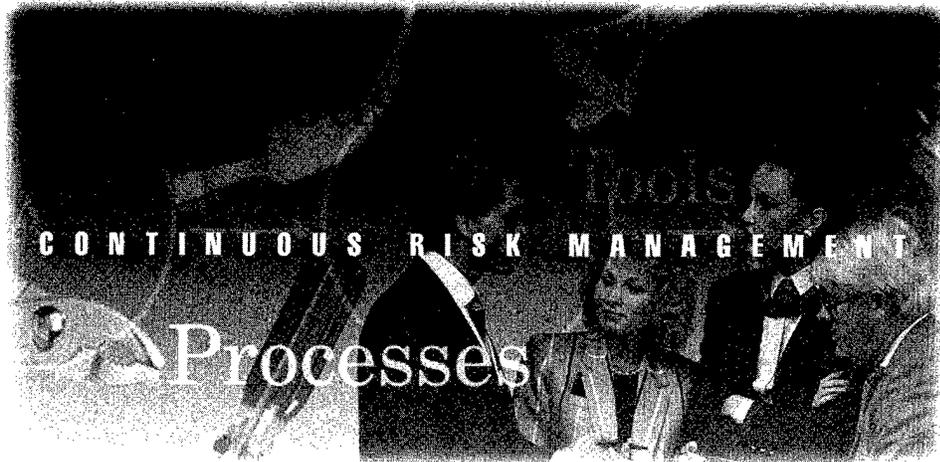
Introduction   This part describes the concepts and functions of Continuous Risk Management. The overview chapter introduces risk terminology and the SEI risk management paradigm. The following chapters provide detailed descriptions of each function in the paradigm including the activities involved and pointers to associated methods and tools described in the appendix.

Chapter 3

Overview
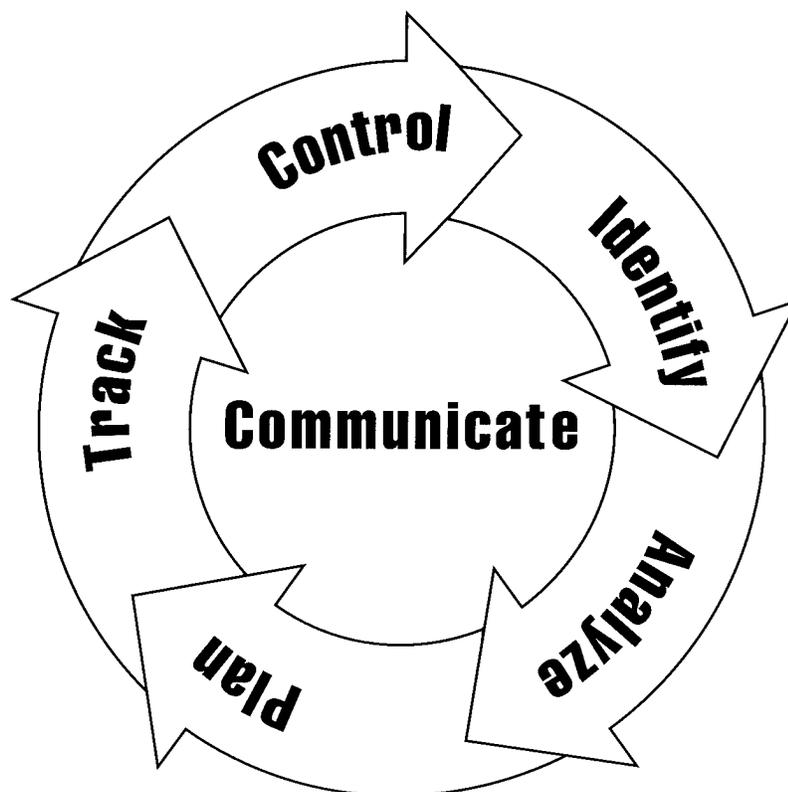
Section 1

Risk Terms and Definitions

Risk

There are a number of definitions and uses for the term risk, but no universally accepted definition.

What all definitions have in common is agreement that risk has two characteristics [Kirkpatrick 92, p.7]:
- *uncertainty:* An event may or may not happen.
- *loss:* An event has unwanted consequences or losses.

Example Risk Definitions

Three example definitions of risk are shown below:

Risk is the potential for realization of unwanted negative consequences of an event [Rowe 88, p. 24].

Risk is the measure of the probability and severity of adverse effects [Lowrance 76, p. 94].

Risk is the possibility of suffering loss, injury, disadvantage, or destruction [Webster's 81, p. 1961].

SEI Definition of Risk

The SEI uses the Webster's Dictionary definition of risk.

Risk is the possibility of suffering loss.

In a development project, the loss describes the impact to the project which could be in the form of diminished quality of the end product, increased costs, delayed completion, or failure.

Risk vs. Opportunity

Risk and opportunity go hand in hand. Many development projects strive to advance current capabilities and achieve something that hasn't been done before. The opportunity for advancement cannot be achieved without taking risk. "Risk in itself is not bad; risk is essential to progress, and failure is often a key part of learning. But we must learn to balance the possible negative consequences of risk against the potential benefits of its associated opportunity" [Van Scoy 92, p. 3].

SEI Risk Statement

For a risk to be understandable, it must be expressed clearly. Such a statement must include
- a description of the current conditions that may lead to the loss
- a description of the loss or consequence

Risk Example

A company has introduced object-oriented (OO) technology into its organization by selecting a well-defined project "X" with hard schedule constraints to pilot the use of the technology. Although many "X" project personnel were familiar with the OO concept, it had not been part of their development process, and they have had very little experience and training in the technology's application. It is taking project personnel longer than expected to climb the learning curve. Some personnel are concerned, for example, that the modules implemented to date might be too inefficient to satisfy project "X" performance requirements.

The risk is: Given the lack of OO technology experience and training, there is a possibility that the product will not meet performance or functionality requirements within the defined schedule.

Non-Risk Example

Another company is developing a flight control system. During system integration-testing, the flight control system becomes unstable because processing of the control function is not quick enough during a specific maneuver sequence.

The instability of the system is not a risk since the event is a certainty—it is a problem.

Section 2

Continuous Risk Management Definition

Background

The term *risk management* is applied in a number of diverse disciplines. People in the fields of statistics, economics, psychology, social sciences, biology, engineering, toxicology, systems analysis, operations research, and decision theory, to name a few, have been addressing the field of risk management [Kirkpatrick 92, p. 8].

Kloman summarized the meaning of risk management in the context of a number of different disciplines in an article for *Risk Analysis*:

> What is risk management? To many social analysts, politicians, and academics it is the management of environmental and nuclear risks, those technology-generated macro-risks that appear to threaten our existence. To bankers and financial officers it is the sophisticated use of such techniques as currency hedging and interest rate swaps. To insurance buyers and sellers it is coordination of insurable risks and the reduction of insurance costs. To hospital administrators it may mean 'quality assurance.' To safety professionals it is reducing accidents and injuries [Kloman 90, p. 20].

Kloman Paraphrase of Rowe

Risk management is a discipline for living with the possibility that future events may cause adverse effects [Kloman 90, p. 203].

SEI Definition

Continuous Risk Management is a software engineering practice with processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making to

- assess continuously what could go wrong (risks)
- determine which risks are important to deal with
- implement strategies to deal with those risks

Note: The SEI definition emphasizes the continuous aspect of risk management—hence the name Continuous Risk Management (CRM).

Continuous Risk Management Example

When using Continuous Risk Management, risks are assessed continuously and used for decision-making in all phases of a project. Risks are carried forward and dealt with until they are resolved or they turn into problems and are handled as such.

Non-Continuous Risk Management Example

In some projects, risks are assessed only once during initial project planning. Major risks are identified and mitigated, but risks are never explicitly looked at again.

This is not an example of Continuous Risk Management because risks are not continuously assessed and new risks are not continuously identified.

Section 3

SEI Risk Management Paradigm

Risk Management Paradigm

The SEI risk management paradigm is depicted below [Van Scoy 92, p. 9]. The paradigm illustrates a set of functions that are identified as continuous activities throughout the life cycle of a project.

Functions of Continuous Risk Management

The functions of Continuous Risk Management are introduced below [SEI 92] [Higuera 93] and described in detail in Chapters 4 through 9. Each risk nominally goes through these functions sequentially but the activity occurs continuously, concurrently (e.g., risks are tracked in parallel while new risks are identified and analyzed), and iteratively (e.g., the mitigation plan for one risk may yield another risk) throughout the project life cycle.

Function	Description
Identify	Search for and locate risks before they become problems.
Analyze	Transform risk data into decision-making information. Evaluate impact, probability, and timeframe, classify risks, and prioritize risks.
Plan	Translate risk information into decisions and mitigating actions (both present and future) and implement those actions.
Track	Monitor risk indicators and mitigation actions.
Control	Correct for deviations from the risk mitigation plans.
Communicate	Provide information and feedback internal and external to the project on the risk activities, current risks, and emerging risks. *Note*: Communication happens throughout all the functions of risk management.

Principles and the Paradigm

The SEI risk management paradigm sets forth a practice for managing risks within a project. The foundation for the paradigm is the set of seven principles described in Part 1. The following paragraphs summarize what principles apply to each paradigm function. These need to be kept in mind as methods and tools are selected and implementation details are determined for a specific project. While it is difficult to measure the effectiveness of the principles, it is easy to detect their absence in any implemented risk management practice.

23

Identify

The principles applicable during the **Identify** function are

- Effective risk management requires that risks be identified as part of a continuous process, not a one-time only activity at the start of the project.
- Risk identification must employ both open communication and a forward-looking view to encourage all personnel to bring forward new risks and to look beyond their immediate problems.
- Although individual contributions play a role in risk management, teamwork improves the chances of identifying new risks by allowing personnel to combine their knowledge and understanding of the project.

Analyze

The principles applicable during the **Analyze** function are

- Conditions and priorities often change on a project and can affect the important risks to a project—risk analysis must be a continuous process.
- Analysis requires open communication so that prioritzation and evaluation is accomplished using all known information.
- A forward-looking view enables personnel to consider long-range impacts of risks.
- A global perspective and a shared product vision allow project personnel to consider their risks in the larger scheme of the end product, the customer's needs, and organizational goals.

Plan

The principles applicable during the **Plan** function are

- Planning risks is a continuous process of determining what to do with new risks as they are identified, to enable efficient use of resources.
- Integrated management is needed to ensure mitigation actions do not conflict with project or team plans and goals.
- A shared product vision and global perspective are needed to create mitigation actions that ultimately benefit the project, customer, and organization.
- The focus of risk planning is to be forward-looking, to prevent risks from becoming problems.
- Teamwork and open communication enhance the planning process by increasing the amount of knowledge and expertise that can be applied to the development of mitigation actions.

Track

The principles applicable during the **Track** function are

- Open communication about a risk's status stimulates the project and risk management processes.
- Tracking is a continuous process—current information about a risk's status is conveyed periodically to the rest of the project.
- When project personnel review tracking data with a forward-looking view and a global perspective, they can interpret the data to reveal adverse trends and potential risks.
- Integrated management combines risk tracking with routine project monitoring processes, creating a synergy that better predicts and identifies new issues.

Control

The principles applicable during the **Control** function are

- Open communication is important for effective feedback and decision making, a critical aspect of Control.
- Risk control is also enhanced through integrated management—combining it with routine project management activities enables comprehensive project decision making.
- Shared product vision and a global perspective support control decisions that are effective for the long-term success of the project and organization.

Communicate

The principles applicable during the **Communicate** function are

- Risk communication is often difficult because it deals with probability and negative consequences—it relies upon open communication to be effective and must encourage a free flow of information within and between all project levels.
- Communication must value the individual voice as well as promote teamwork to support the effectiveness of the other functions.

Section 4

References

Cited in this chapter:

[Higuera 93]   Higuera, Ronald P. & Gluch, David P. "Risk Management and Quality in Software Development." *Proceedings of the Eleventh Annual Pacific Northwest Software Quality Conference*. Portland, Oregon, October 18-20, 1993. Portland, Oregon: Pacific Northwest Software Quality Conference, 1993.

[Kirkpatrick 92]   Kirkpatrick, Robert J.; Walker, Julie A.; & Firth, Robert. "Software Development Risk Management: An SEI Appraisal." *Software Engineering Institute Technical Review '92* (CMU/SEI-92-REV). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1992.

[Kloman 90]   Kloman, H.F. "Risk Management Agonists." *Risk Analysis 10*, 2 (1990): 201-205.

[Lowrance 76]   Lowrance, William W. *Of Acceptable Risk*. Los Altos, Ca.: William Kaufmann, 1976.

[Rowe 88]   Rowe, William D. *An Anatomy of Risk*. Malabar, Fla.: Robert E. Krieger, 1988.

[SEI 92]   Software Engineering Institute. "The SEI Approach to Managing Software Technical Risks." *Bridge* (October 1992): 19-21.

[Van Scoy 92]   Van Scoy, Roger L. *Software Development Risk: Opportunity, Not Problem*. (CMU/SEI-92-TR-30, ADA 258743). Pittsburgh, Pa.: Carnegie Mellon University, Software Engineering Institute, 1992.

[Webster's 81]   *Webster's Third New International Dictionary*. Springfield, Ma.: Merriam-Webster, 1981.

Chapter 4

Identify
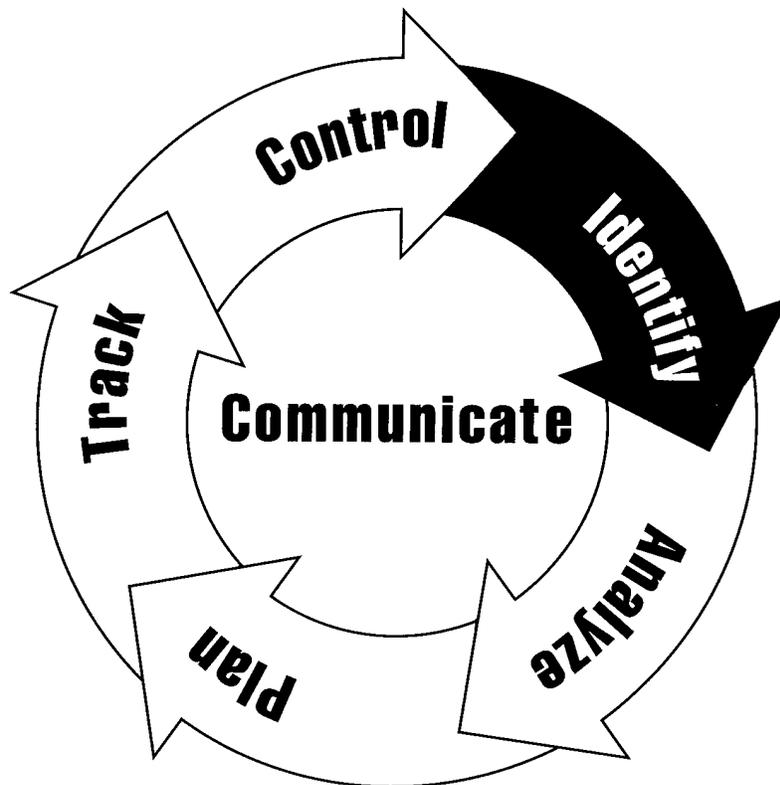
Section 1

What Is Identification?

Description
Identification is a process of transforming uncertainties and issues about the project into distinct (tangible) risks that can be described and measured. Identifying risks involves two activities:
- capturing a statement of risk
- capturing the context of a risk [Gluch 94a]

Note: Context provides additional information about the circumstances of the risk.

Objective
The objective of risk identification is to locate risks before they become problems and to incorporate this information into the project management process.

Diagram
The following diagram shows the inputs and outputs of the **Identify** function.
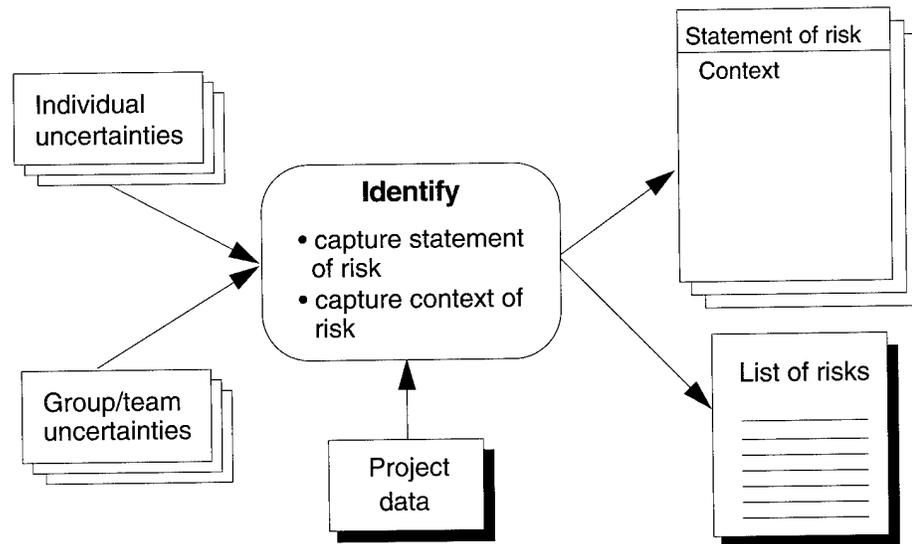
Data Items
The following table describes the data items of the Identify function.
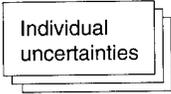
Data Item	Description
Individual uncertainties	Individuals have uncertainties and issues about the project and project progress which may or may not be risks.
Group/team uncertainties	In group activities, individuals may together identify uncertainties and issues about the project and project progress which may or may not be risks.
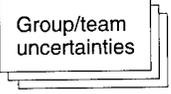
Data Item	Description
Project data	The project data is supporting information that consists of items such as the schedule, budget, plans, work breakdown structure, etc. that may provide information helpful in identifying risks (e.g., previously unknown dependencies between module development schedules).
Statement of risk / Context	For each risk identified, a statement of risk is captured along with the associated context for the risk.
List of risks	This list contains all the statements of risk identified for the project.
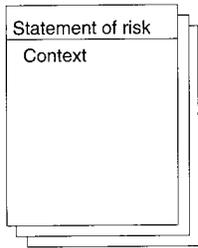
Risk Identifiers

A unique risk identifier is generally used to help keep track of risks that have been identified and are going to be managed. This can be a number, project name and number combination, or some other unique combination of letters and numbers.

Methods and Tools

This table provides a summary of the methods and tools used for each activity. More details are provided in subsequent sections of this chapter and chapters in the appendix.

Activity	Method or Tool
All activities	Risk information sheet
Capture a statement of risk	Brainstorming
	Periodic risk reporting
	Project profile questions
	Risk form
	Short TBQ
	Taxonomy-based questionnaire (TBQ)
	TBQ interviews
	Voluntary risk reporting

Activity	Method or Tool
Capture the context of a risk	All of the above methods and tools are applicable since context is captured any time a risk is identified.

Section 2

Capturing a Statement of Risk

Description
Capturing a statement of risk involves considering and recording the conditions that are causing concern for a potential loss to the project, followed (optionally) by a brief description of the potential consequences of these conditions.

Objective
The objective of capturing a statement of risk is to arrive at a concise description of risk, which can be understood and acted upon.

Diagram
The following diagram shows the inputs and outputs for capturing a statement of risk.
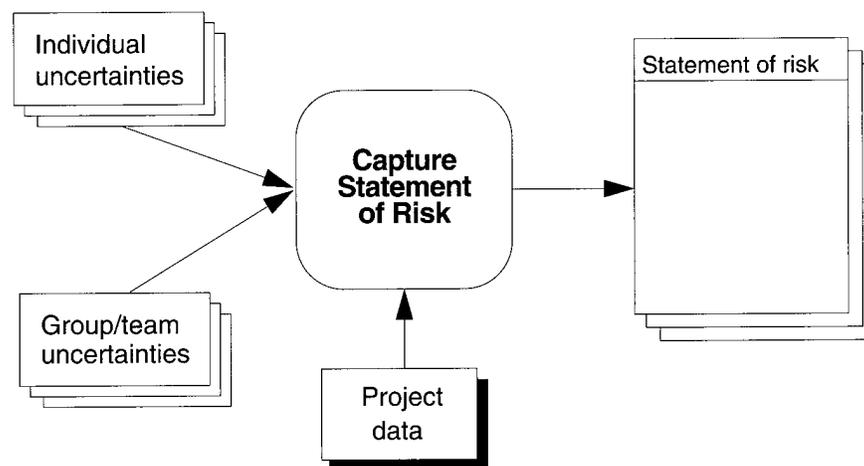
Components of a Statement of Risk
The components and description of a statement of risk are

- *condition*: a single phrase or sentence that briefly describes the key circumstances, situations, etc., causing concern, doubt, anxiety, or uncertainty

- *consequence*: a single phrase or sentence that describes the key, possible negative outcome(s) of the current conditions

Note: The minimum statement of risk is the condition. It is desirable to capture the originator's assessment of the possible consequences of the risk to assure that it is given suitable weight during analysis; however, the explicit statement of consequence is not required, is often omitted, and can be subsequently added at the planning step.

Condition-Consequence Format
The condition-consequence format provides a more complete picture of the risk, which is critical during mitigation planning. The condition component focuses on what is currently causing concern. This component provides information that is useful when determining how to mitigate a risk. The consequence component focuses on the intermediate and long term impact of the risk. Understanding the depth and breadth of the impact is useful information in determining how much time, resource, and effort should be allocated to the mitigation effort.

**Example
Statement of
Risk**

Statement of Risk: Given that the graphical user interface (GUI) must be coded using X Windows and we do not have expertise in X Windows, then there is concern that (possibly) the GUI code will not be completed on time and will be inefficient.

The following diagram illustrates the condition and consequence of a statement of risk.

Statement of Risk

Condition	Consequence
The graphical user interface (GUI) must be coded using X Windows and we do not have expertise in X Windows	The GUI code may not be completed on time and may be inefficient
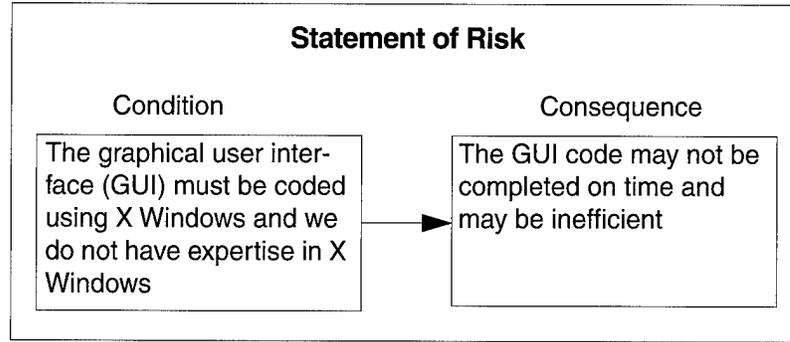
**Simplified
Notation**

When writing the statement of risk the words "given that" can be omitted, and the phrase, "then there is concern that (possibly)", can be replaced by a semicolon [Gluch 94a].

Example: The graphical user interface (GUI) must be coded using X Windows and we do not have expertise in X Windows; the GUI code may not be completed on time and may be inefficient.

**Non-
Statement of
Risk Example**

Capturing the condition is the important aspect of risk identification. The following statement is not a satisfactory statement of a risk.

Example: There is risk in the schedule.

**Identify:
Methods and
Tools**

The following table summarizes the methods and tools for capturing statements of risks. Detailed descriptions are provided in the appendix.

Method or Tool	Description
Brainstorming [Chapter A-7]	Project personnel verbally identify risks as they think of them, thus providing the opportunities for participants to build on each others' ideas
Periodic Risk Reporting [Chapter A-19]	Periodic (mandatory and scheduled) reporting of risks by project personnel
Project Profile Questions [Chapter A-25]	A description of how to tailor the taxonomy-based questionnaire (TBQ) based on project characteristics
Risk Form [Chapter A-26]	A form used to document new risks as they are identified.

Method or Tool	Description
Risk Information Sheet [Chapter A-27]	A means of documenting information about a risk, much as a software trouble or problem report documents a problem in software. Information is added to the sheet as it is acquired or developed.
Short TBQ [Chapter A-29]	A shortened version of the TBQ used in meetings, one-on-one interviews and as a memory jogger adjunct to voluntary or periodic risk reporting
Taxonomy-Based Questionnaire [Chapter A-32]	A listing of interview questions organized according to the software development risk taxonomy [Carr 93]
TBQ Interviews [Chapter A-33]	Structured peer group interviews and structured interviews of individuals using the TBQ [Carr 93]
Voluntary Risk Reporting [Chapter A-39]	Routine distribution and processing of risk forms, voluntarily submitted by project personnel as risks are identified

Section 3

Capturing the Context of a Risk

Description The statement of risk provides a brief, concise description of the condition and consequence of the risk. Capturing the context of a risk involves recording the additional information regarding the circumstances, events, and interrelationships within the project that may affect the risk. This description has captured more detailed than can be captured in the basic statement of risk.

Objective The objective of capturing the context of a risk is to provide enough additional information about the risk to ensure that the original intent of the risk can be understood by other personnel, particularly after time has passed.

Diagram The following diagram shows the inputs and outputs for capturing the context of a risk.
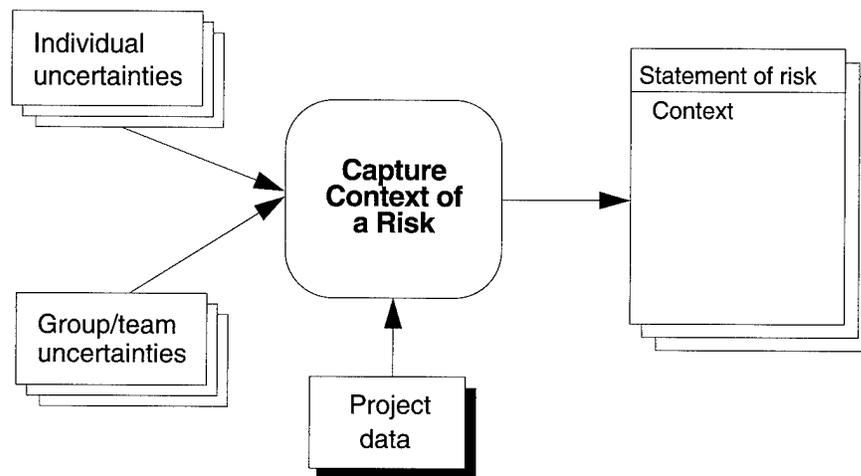
Note: In most cases, context is being captured in parallel as a statement of risk is identified.

Effective Context Effective context captures the what, when, where, how, and why of the risk by describing the circumstances described in the risk statement, contributing factors, related issues, and potential consequences of the risk. It enables understanding of the risk by other personnel. It is especially effective when it can be used later when time and current circumstances have changed the perceptions of the risk.

Structure of the Context The structure of the context is informal text, which may consist of brief comments through one or more sentences of explanation.

The textual comments may include information on personnel, technical, or management issues, communications, or other pertinent aspects of the project.

Example Statement of Risk with Context

An example statement of risk with its context is shown below.

Statement of Risk: The graphical user interface (GUI) must be coded using X Windows and we do not have expertise in X Windows; the GUI code may not be completed on time and may be inefficient.

Context: The graphical user interface is an important part of the system and we do not have anyone trained in the X Window System. We all have been studying the language but it is complex and only one person in the group has any graphics experience and that is with Windows on the PC.

Updating the Context

While the original version of the context is generated as part of the identification, it is often modified and expanded as a normal part of the risk management process. This is done to reflect the most current risk information. Things that are added to the context are

- changes in conditions
- new conditions or concerns
- decisions made

Section 4

Guidelines and Tips

Guidelines and Tips for Identify

Develop a common understanding of the risk by sharing several points of view.

Provide an opportunity for individual contributions.

Ensure that the common view does not eliminate individual views.

State risks in objective terms which are understood by project personnel.

State risks in a way such that they can be addressed.

References

Cited in this chapter:

[Carr 93]   Carr, Marvin; Konda, Suresh; Monarch, Ira; Ulrich, Carol; & Walker, Clay. *Taxonomy-Based Risk Identification* (CMU/SEI-93-TR-6, ADA266992). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

[Gluch 94a]   Gluch, David P. *A Construct for Describing Software Development Risk* (CMU/SEI-94-TR-14, ADA284922). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

Chapter 5

Analyze
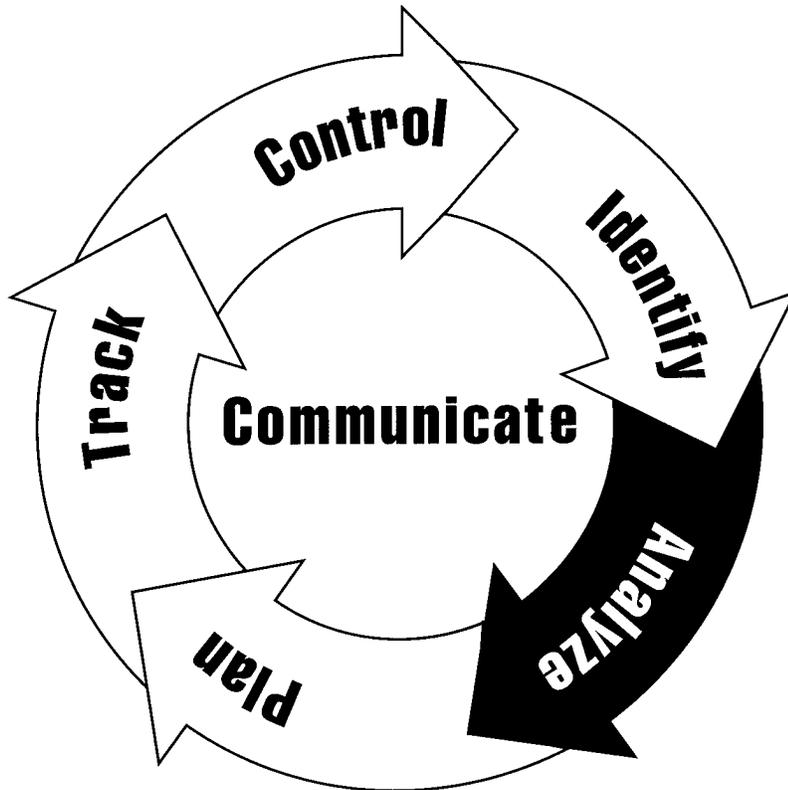
Section

Section 1

What Is Analysis?

Description   Analysis is a process of examining the risks in detail to determine the extent of the risks, how they relate to each other, and which ones are the most important. Analyzing risks has three basic activities:

- evaluating attributes of risks
- classifying risks
- prioritizing (ranking) risks

Note: While **Analyze** is a distinct Continuous Risk Management function, analytical activities also occur within other functions of the paradigm.

Objective   The objective of the Analyze function is to convert risk data into decision-making information.

Note: All risks are analyzed at some level.

Diagram   The following diagram shows the inputs and outputs of the Analyze function.

Statement of risk
Context

Statement of risk
Context
Impact
Probability
Timeframe
Classification
Rank

Analyze
- evaluate
- classify
- prioritize

List of risks

Classification
Class 1 Class 2
Risk Risk
Risk Risk
Risk Class 3
Risk Risk

Master list
of risks
Top
N
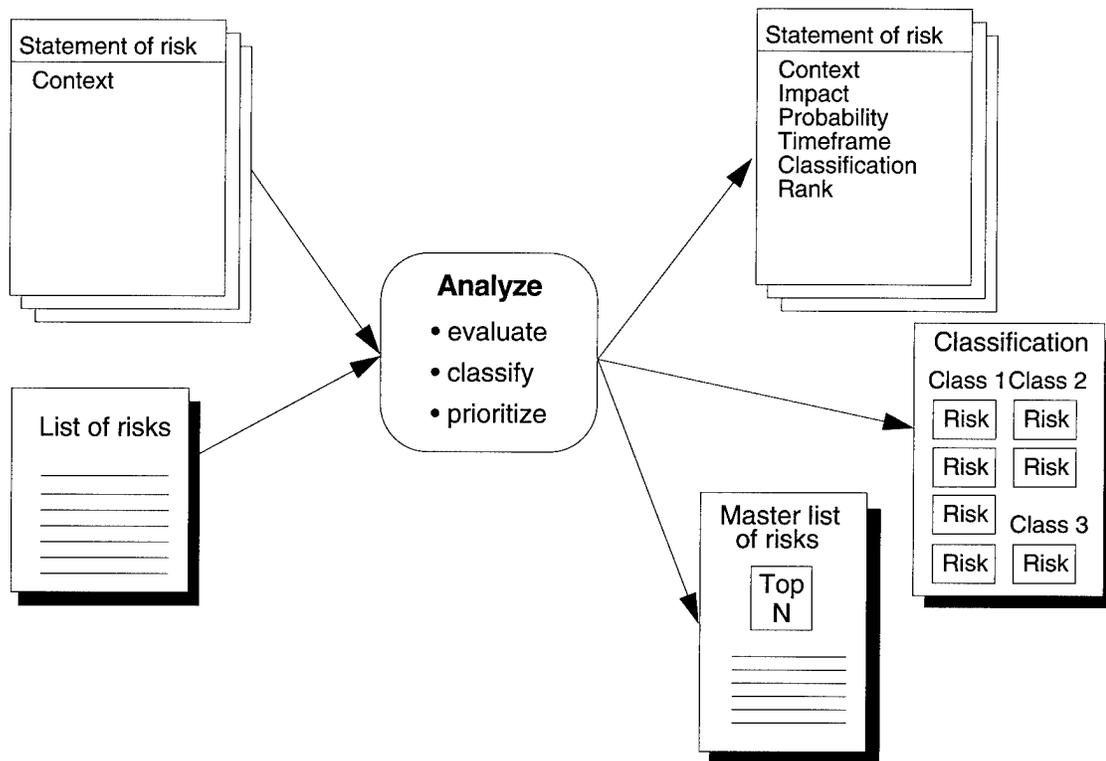
Data Items

The following table describes the data items of the Analyze function.

Data Item	Description
List of risks	The list of risks contains all the statements of risk that need to be analyzed.
Statement of risk Context	Prior to analysis, the risk information for each risk contains the statement of risk and its supporting context.
Statement of risk Context Impact Probability Timeframe Classification Rank	After analysis, values for impact, probability, time-frame, class, and rank are added to the risk information (statement of risk, supporting context) for each risk.
Classification Class 1 Class 2 Risk Risk Risk Risk Risk Class 3 Risk Risk	Classification organizes risks into groups having some common basis. The organization may come from a pre-defined structure or from a self-organized structure. This list is an organization of the risks according to its classification.
Master list of risks Top N	The master list of risks contains all risks that have been identified and the priority ranking of the top N risks.
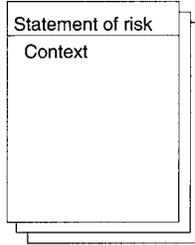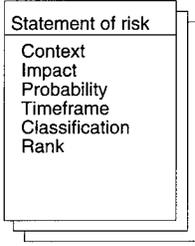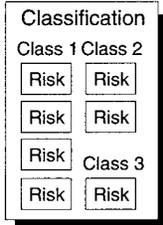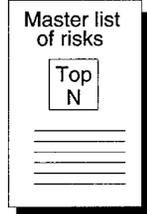
Methods and Tools

This table provides a summary of the methods and tools used for each activity. More details are provided in subsequent sections of this chapter and chapters in the appendix.

Activity	Method or Tool
All activities	Risk information sheet
Evaluating attributes of risks	Binary attribute evaluation
	Risk form
	Tri-level attribute evaluation
Classifying risks	Affinity grouping
	Bar graph
	Risk form
	Taxonomy classification
Prioritizing (ranking) risks	Comparison risk ranking
	Multivoting
	Pareto top N
	Potential top N
	Top 5

Section 2

Evaluating Attributes of Risks

Description

Evaluating the attributes of a risk involves establishing the current *values* for

- *impact*: the loss or effect on the project if the risk occurs
- *probability*[1]: the likelihood the risk will occur
- *timeframe*: the period when action is required in order to mitigate the risk

Objective

The objective of evaluating the attributes is to gain a better understanding of the risk by determining the expected impact, probability, and timeframe of the risk.

Diagram

The following diagram shows the inputs and outputs for evaluating the attributes of risks.
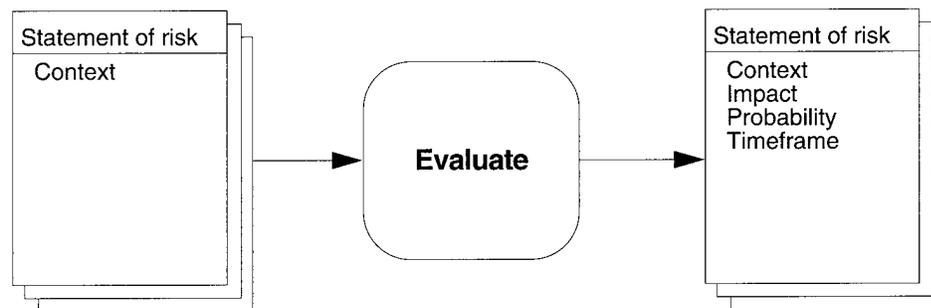
Levels of Analysis

Risks should be evaluated at a level of analysis that is sufficient to determine the relative importance, for planning cost-effective mitigation strategies, and to support tracking. Therefore, individual risks can be analyzed and managed at various levels of detail at different points in time.

Example: A high impact, high probability risk may require a more detailed level of analysis to plan a mitigation strategy. In contrast, simply knowing a risk is not likely to occur (low probability) and will have an insignificant impact (low impact) if it does occur may be all that you need to know to decide how to deal with the risk.

Levels of Analysis and Attributes

The following table lists some ranges of the attribute values for a risk at various levels of analysis. It is only representative of many possibilities of levels. There is a wide range of levels possible between the binary level and the quantitative level. There could be four levels, ten levels, etc. It is also possible to have a combination of levels for attributes of a given risk.

1. To some people the word probability means a number between zero and one. In this guidebook, the term is used generically and can refer to a qualitative description, an ordinal number, or a cardinal number. In general, evaluating probability requires a subjective judgment and will be represented by a qualitative description or ordinal number.

Level	Impact	Probability	Timeframe
Binary level	yes no	yes no	near far
3-level	high moderate low	high moderate low	near mid far
5-level	very high high moderate low very low	very high high moderate low very low	imminent near mid far very far
n-level	n levels of impact	n levels of proba- bility	n levels of time- frame

Air Force Example

The Air Force Systems Command / Air Force Logistics Command (AFSC/AFLC) Pamphlet 800-45 [Air Force 88] describes a four-level analysis approach.

Level	Impact	Probability	Timeframe
AFSC/AFLC Pamphlet 800-45	catastrophic critical marginal negligible	frequent probable improbable impossible	N/A

Combination Example

A risk may have the impact evaluated qualitatively using the 5-level, probability evaluated qualitatively using the 3-level, and the timeframe evaluated qualitatively using the binary level.

Level	Impact	Probability	Timeframe
Combination	very high high moderate low very low	high moderate low	near far

Risk Exposure

Risk exposure is an attribute of risk that is derived from two of the attributes: impact (loss) and probability (likelihood). You may use the combined attribute of risk exposure in place of the individual values of impact and probability.

Risk exposure (RE) is defined by the following relationship [Boehm 89, p. 6]:

RE = Prob(UO) * Loss(UO)

Where Prob(UO) is the probability of an unsatisfactory outcome (UO) or risk, and Loss(UO) is the loss to the parties affected if the outcome is unsatisfactory (i.e., the risk occurs).

Levels of Risk Exposure

The table below summarizes the various values of the risk exposure associated with the range of levels of analysis described earlier.

Level	Risk Exposure
Binary level	There are four (4) possible values of risk exposure [impact - probability]. • value 1 = yes-yes (High) • value 2 = yes-no (Moderate) • value 3 = no-yes (Moderate) • value 4 = no-no (Low)
3-level	There are nine (9) possible values of risk exposure [impact - probability]. • h-h, h-m, m-h (High) • h-l, m-m, l-h (Moderate) • m-l, l-m, l-l (Low)
5-level	There are twenty-five (25) possible values of risk exposure [impact - probability]. • vh-vh, vh-h, h-vh (Very High) • vh-m, h-h, h-m, m-vh, m-h (High) • vh-l, vh-vl, h-l, h-vl, m-m, l-vh, l-h, vl-vh, vl-h (Moderate) • m-l, m-vl, l-m, l-l, vl-m (Low) • l-vl, vl-l, vl-vl (Very Low)
n-level	There is a continuum of values for the risk exposure. The range of these values will depend on the maximum value used for the impact.

Air Force Summary

The table below shows the AFSC/AFLC Pamphlet 800-45 [Air Force 88, p.153] example of risk exposure.

Probability

Impact	Frequent	Probable	Improbable	Impossible
Catastrophic	High	High	Moderate	None
Critical	High	Moderate	Moderate	None
Marginal	Moderate	Moderate	Low	None
Negligible	Moderate	Low	Low	None

Risk Exposure and Ordinal Numbers

If the impact and probability have been evaluated qualitatively using ordinal numbers, beware of performing multiplication on the ordinal scale values. The individual scale values provide information on the impact and probability of the risk. Multiplying these ordinal values to obtain risk exposure provides information that if not careful, can be misinterpreted.

Example: The following table shows ordinal values applied to the Air Force impact and probability values as example as well as the combined values for risk exposure. Consider a risk, X, which is evaluated as critical (3) and frequent (4). This risk has a high risk exposure which is calculated as the product of impact and probability, which is 12. Consider a second risk, Y, which is evaluated as critical (3) and improbable (2). The risk exposure for Y is 6, a moderate risk exposure. With ordinal numbers all we can say is that risk X has a higher risk exposure than risk Y. It is tempting to say that risk X has twice the risk exposure than risk Y. With ordinal numbers we cannot say how much higher the risk exposure for risk X is than risk Y. The danger comes when we apply more meaning to numbers than they support.

Probability

Impact	Frequent (4)	Probable (3)	Improbable (2)	Impossible (1)
Catastrophic (4)	High (16)	High (12)	Moderate (8)	None (4)
Critical (3)	High (12)	Moderate (9)	Moderate (6)	None (3)
Marginal (2)	Moderate (8)	Moderate (6)	Low (4)	None (2)
Negligible (1)	Moderate (4)	Low (3)	Low (2)	None (1)

Choosing a Level of Analysis

Choosing a level of analysis depends on a number of factors, such as
- what fits in your organization
- what is prescribed by a customer or policy
- what is sufficient for planning a mitigation strategy for an individual risk

Note: Consider the purpose of the evaluation effort. The time and resources required for the evaluation must be balanced against the value of the added level of information. For example, initially you may choose a binary level of analysis to sort through a large number of risks. You may then decide that for a few of the more important risks you'd like to revisit the evaluation with a more refined measure of the attributes.

Analyze: Evaluation Methods and Tools

The following table summarizes the methods and tools for evaluating the attributes of risk. Detailed descriptions of the methods and tools are provided in the appendix.

Method or Tool	Description
Binary Attribute Evaluation [Chapter A-6]	Each risk is evaluated with respect to • impact (significant, insignificant) • probability (likely, unlikely) • timeframe (near-term, far-term)
Risk Form [Chapter A-26]	This form can be used to capture the results of the binary attribute evaluation or tri-level attribute evaluation methods for a risk.
Risk Information Sheet [Chapter A-27]	This sheet can be used to document the results of the binary attribute evaluation or tri-level attribute evaluation methods for a risk.
Tri-level Attribute Evaluation [Chapter A-38]	Each risk is evaluated with respect to: • impact (catastrophic, critical, marginal) • probability (very likely, probable, improbable) • timeframe (imminent, near-term, far-term)

Section 3

Classifying Risks

Description Classifying risks involves grouping risks based on shared characteristics. The groups or classes show relationships among the risks. Classification helps to identify duplicate risks and supports simplifying the list of risks.

Objective The objective of classifying risks is to look at a set of risks and how those risks relate to each other within a given structure. The classes or groups of risks provide a different perspective when planning risks.

Diagram The following diagram shows the inputs and outputs for classifying risks.
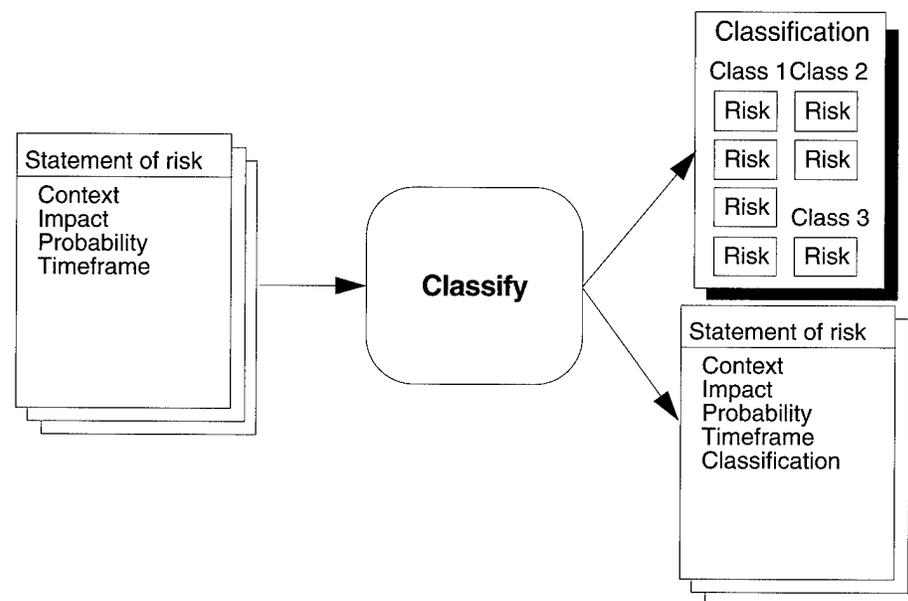
Classification Perspectives Within the Continuous Risk Management approach, risks are classified using two conceptual perspectives as listed in the following table.

Classification Perspective	Description
Predefined structure	Places risks into a predefined structure by applying the selected criterion to the statement of risk and context
	Example: software development risk taxonomy [Carr 93], work breakdown structure
Self-organized structure	Organizes risks into distinct categories based on common characteristics; the structure and criteria emerge as a result of the classification process
	Example: affinity grouping

Classification by Source or Impact

When classifying risks using the predefined structure, the criterion chosen will affect the outcome of groups of risks. There are two criteria for grouping risks:

- *by source:* Risks are grouped based on the same source or root cause. This will show the major sources of risk to the project.
- *by impact:* Risks are grouped based on where or how the impact will be felt by the project. This shows the project the major product areas that will be impacted by the risks.

Note: Classification by impact can occur at several levels. Risks may be classified by their impact on technical work, budget, or schedule. This high level classification can show a manager which risks may be seen by the customer and which are primarily internal. A useful classification for planning might look at a more detailed view of where the impact will be felt such as a product subsystem.

Classification Uses

There are several ways to classify or group risks. The ultimate purpose of classification is to understand the risks the project faces and group related risks to help build more cost-effective mitigation plans. Multiple views may provide insight into how best to deal with the risks in planning. It is important to maintain the classification structure during planning. The classification is not helpful if it is not used consistently in planning. If the structure is changed, reclassify all the risks.

Multiple Classification Example

The first time project members identify risks, they may come up with a large number of them. Initially, they may classify according to the source of risk (e.g., what are the risks resulting from requirements instability?) to understand the global risk picture. However, mitigating the risks may best be done by a different classification based on who should deal with it or what other risks affect the same area (e.g., what are all risks affecting the compiler performance?). Both views provide valuable information to the project.

There are no specific rules for selecting a classification scheme. Projects should consider what will help during the planning process.

Note: With database technology, storing multiple classification information is manageable.

Classification Bar Graph

The result of a classification may be shown as a **Bar Graph** [Chapter A-3]. A classification bar graph is a graphic display of the groups in a classification and the number of risks in each group.

Example: The following bar graph indicates the number of risks that were classified, based on source of risk, into each taxonomy element of the software development risk taxonomy class/element/attribute structure [Carr 93].

Taxonomy Element
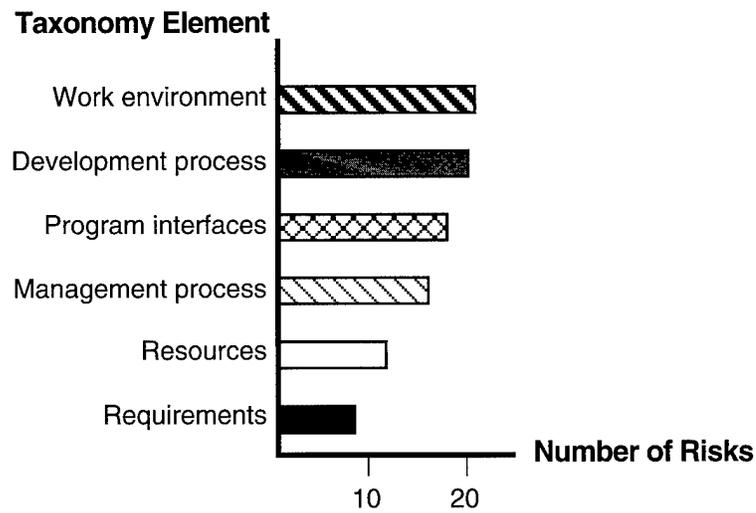
Combining Duplicates Risks

The process of classifying risks may reveal that two or more risks are equivalent—the statements of risk and context indicate that the subject of these risks is the same. Equivalent risks are therefore duplicate statements of the same risk and should be combined into one risk.

Analyze: Classification Methods and Tools

The following table summarizes the methods and tools for classifying risks. Detailed descriptions of the methods and tools are provided in the appendix.

Method or Tool	Description
Affinity Grouping [Chapter A-2]	Groups risks that are naturally related and then identifies the one concept that ties each grouping together [Brassard 89]
Bar Graph [Chapter A-3]	Presents a graphical summary of the number of risks in each classification category
Risk Form [Chapter A-26]	Used to capture the results of the affinity grouping or taxonomy classification methods for a risk
Risk Information Sheet [Chapter A-27]	Used to document the classification results of the Affinity Grouping or Taxonomy Classification methods for a risk
Taxonomy Classification [Chapter A-34]	Groups risks according to software development areas using the software development risk taxonomy's class/element/attribute structure

Section 4

Prioritizing (Ranking) Risks

Prioritization

Prioritizing risks involves partitioning risks or groups of risks based on the Pareto "vital few" sense [Juran 89] and ranking the risks or sets of risks based upon a criterion or set of criteria as appropriate.

Note: Sets of risks may be prioritized along with singular risk statements because a project's risks are dealt with at various levels of complexity. One singular risk statement may warrant being dealt with by itself due to the nature of the risk, while another may best be dealt with by grouping them with other risks that are related. In other words, sometimes a risk is only seen when all the component pieces (i.e., smaller, related risks) are put together. It is not uncommon to deal with both single risks and sets of risks at the same time.

Objective

The objective of prioritizing risks is to separate out which risks should be dealt with first (the vital few risks) when allocating resources.

Diagram

The following diagram shows the inputs and outputs for prioritizing risks.
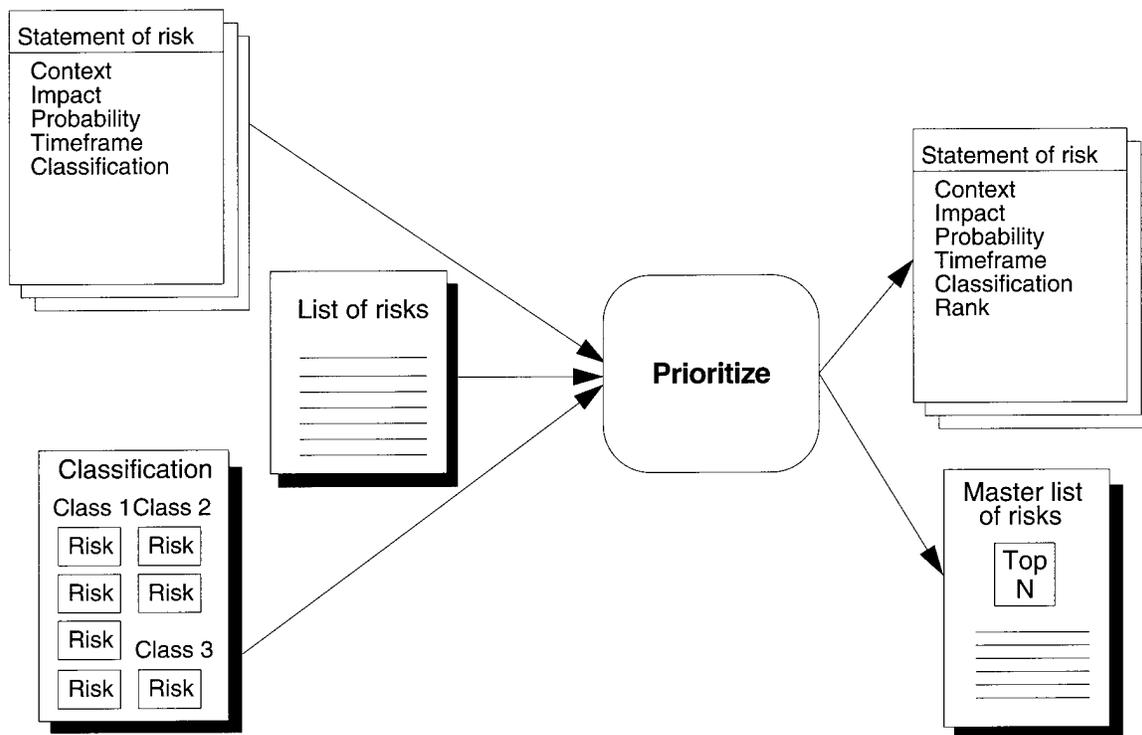
Vital Few/ Most Important

The perspective of importance to the project is used to identify the most important risks or sets of risk of the entire set in the Pareto sense (separating the "vital few" from the "useful many") [Juran 89]. The number of risks is not an exact percentage of the total risks identified but merely a rule of thumb. The actual number will vary based on the nature of the risks.

Example: A project has recently identified a set of fifty individual and groups of risks. Based on the probability, impact, and timeframe information, the project identified a subset of eight as the vital few that need to be dealt with first.

Ranking Top N

Ranking the top N risks or groups of risks involves taking the list of top N risks and ordering these based upon a criterion or set of criteria into a rank-ordered list. The following diagram shows a top N list made up of single risks and sets of risks (risk #3, for example, is a set of five risks).
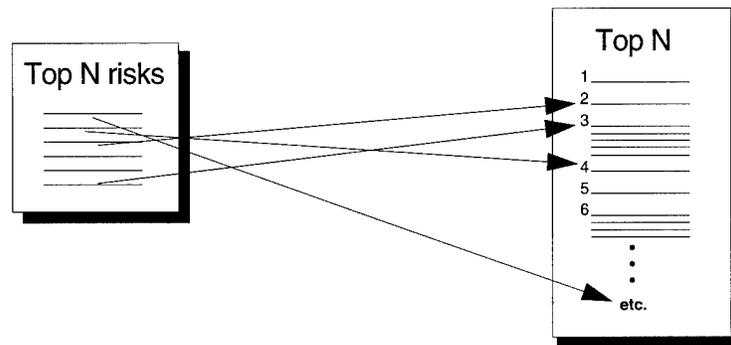
Prioritization Criteria

The criterion or set of criteria used to rank the risks is chosen based on what's most important to the project.

Examples:
• meeting the timing requirement for function x
• schedule for major milestones
• cost within budget

Most Important (Top N Selection)

The vital few top N selection process is shown in the following diagram.
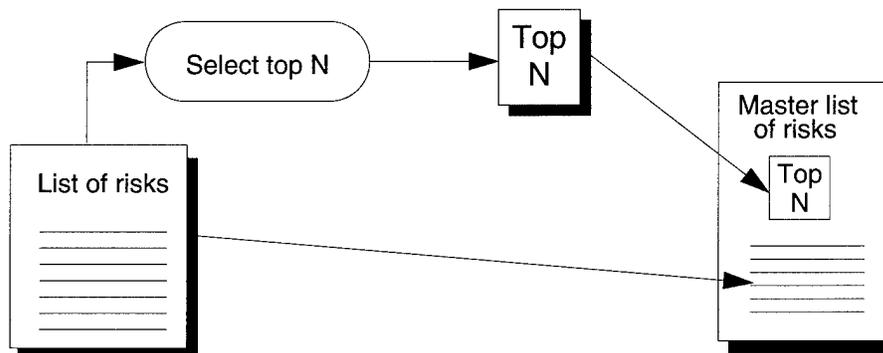
Note: While the project-wide Pareto "vital few" can be managed at the highest levels, all of the other risks can be managed within the departments or teams of the organization most suited to effectively manage those risks (i.e., these risks are *delegated* (see **Plan** [Chapter 6]) to the appropriate level of management).

Analyze: Prioritization Methods and Tools

The following table summarizes the methods and tools for prioritizing risks. Detailed descriptions of the methods and tools are provided in the appendix.

Method or Tool	Description
Comparison Risk Ranking [Chapter A-10]	Risks are ranked by comparing them to an established criterion or set of criteria two at a time.
Multivoting [Chapter A-17]	Individual votes are distributed across the risks, with the option to weight the votes. Risks are ordered by tallying the individual votes.
Pareto Top N [Chapter A-18]	The most important risks to the project are selected based on the tri-level attribute evaluation results.
Potential Top N [Chapter A-23]	The most important risks to the project are selected based on individual opinions.
Risk Information Sheet [Chapter A-27]	This sheet can be used to document the priority of a risk.
Top 5 [Chapter A-37]	Individuals choose the top 5 risks to the project.

Section 5

Guidelines and Tips

Guidelines and Tips for Analyze

Allocate scarce resources to the important issues rather than letting due dates drive resource allocation.

Address the urgent risks (e.g., near timeframe) or risks having the potential for extremely significant impact first.

Combine items that have similar origins or that are duplicates.

Reword risk statements to make them clear to all project members.

Eliminate risks that are already being addressed.

References

Cited in this chapter:

[Air Force 88]   Air Force Systems Command/Air Force Logistics Command Pamphlet 800-45. *Software Risk Abatement*, September 30, 1988.

[Boehm 89]   Boehm, Barry. *IEEE Tutorial on Software Risk Management*. New York: IEEE Computer Society Press, 1989.

[Brassard 89]   Brassard, Michael. *The Memory Jogger Plus +™: featuring the seven management and planning tools*. Methuen, Ma.: GOAL/QPC, 1989.

[Carr 93]   Carr, Marvin; Konda, Suresh; Monarch, Ira; Ulrich, Carol; & Walker, Clay. *Taxonomy - Based Risk Identification* (CMU/SEI-93-TR-6, ADA266992). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

[Juran 89]   Juran, J. M. *Juran on Leadership for Quality*. New York: The Free Press, 1989.

Chapter 6

Plan
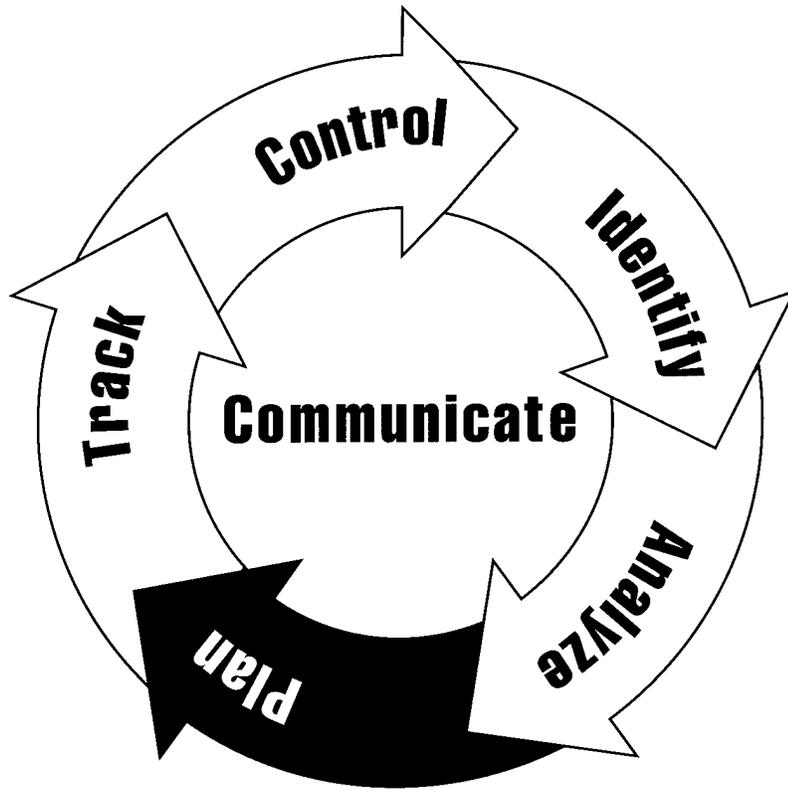
Section

Section 1

What Is Planning?

Description   Planning is the function of deciding what, if anything, should be done with a risk. Planning produces risk action plans for individual or sets of related risks. Risks are planned by those who have the knowledge, expertise, background, and resources to effectively deal with the risks. Planning answers the questions
- Is it my risk? (responsibility)
- What can I do? (approach)
- How much and what should I do? (scope and actions)

Note: Planning individual or sets of risks is basically the same. Section 5 of this chapter discusses considerations for planning a set of related risks.

Objectives   The objectives of the **Plan** function are to
- make sure consequences and sources of the risk are known
- develop effective plans
- plan efficiently (only as much as needed or will be of benefit)
- produce, over time, the correct set of actions that minimize risk and impacts (cost and schedule) while maximizing opportunity and value
- plan important risks first

Diagram   The following diagram shows the inputs and outputs of the Plan function.

Statement of risk*
Context
Impact
Probability
Timeframe
Classification
Rank

Resources

Project goals
and constraints

Statement of risk
Context
Impact
Probability
Timeframe
Classification
Rank
Plan Approach

Plan
- assign responsibility
- determine approach
- define scope and actions

Master list
of risks
Top
N

Classification
Class 1 Class 2
Risk   Risk
Risk   Risk
Risk   Class 3
Risk   Risk

Action plans

* Consequences may be added to the risk statement if not already documented

Data Items

The following table describes the data items of the Plan function.

Data Item	Description
Project goals and constraints	Targets and limits set by the project, team, or manager—for example • Do not slip the schedule. • Use no more than 5% of the team's budget for risk mitigation.
Resources	Available resources for mitigation. In order to develop effective action plans, planners need to know the limits of the available resources for mitigating and watching risks.
Master list of risks Top N	A list of all risks that have been identified and the priority ranking of the top N risks. The top N designation helps planners decide how much effort to put into planning a particular risk or set of risks and the scope of resources that should be used for mitigation.
Statement of risk Context Impact Probability Timeframe Classification Rank	Information associated with each risk. Before planning this includes the statement of risk; supporting context; and values for impact, probability, timeframe, class, and rank. This could be all the risks or a small subset assigned to the planners.
Classification Class 1 Class 2 Risk Risk Risk Risk Risk Class 3 Risk Risk	An organization of the risks according to their classification. Classification shows the relationships among risks and helps identify risks which could be mitigated as a set (see Section 5). For example, classification could show which risks impact the system's user interface, which need to be mitigated as a set, etc.
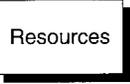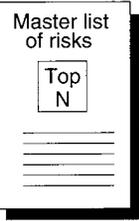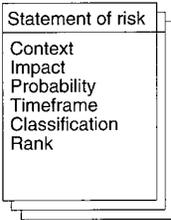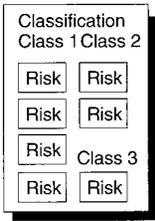
Data Item	Description
Action plans	A description of what action is to be taken to deal with the risk(s). Risk action plans can be one of four types: • research plan • acceptance rationale • tracking requirements • mitigation plan: either ab action item list or a task plan
Statement of risk Context Impact Probability Timeframe Classification Rank Plan Approach	Information associated with each risk, updated to include the approach to be taken for that risk (e.g., research, watch, accept, or mitigate).
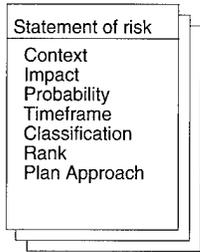
Planning Decision Flowchart

The flowchart on the following page gives a detailed view of the progressive decisions that are made during risk planning. Risks are reviewed to make sure they are understood and clearly documented (e.g., consequences are added if this was not done during identification). Responsibility for the risk is then assigned, resulting in a risk that is kept, delegated, or transferred. If the risk is kept, an approach for dealing with it is determined by the responsible person or team. Additional research may be needed, the risk could be accepted as is, it could be watched, or it could be mitigated. If the risk is to be mitigated, a mitigation plan needs to be developed. The scope of the mitigation plan is determined (action items or a complete task plan), and the plan is developed and implemented.

Planning Decision Flowchart

Statement of risk

Context
Impact
Probability
Timeframe
Classification
Rank

Review risks

**Responsibility:
Is it my risk?**

Is it my task
to deal with
this risk?   → no   Is it internal
to my orga-
nization?   no

↓ yes   ↓ yes

Keep   **Delegate**   **Transfer**

**Approach: Can I
do anything?**

Do I know
enough
about this
risk?   no →   **Research**

Research
plan

↓ yes

Can I live
with this
risk?   no →   Can I act
on this
risk?*   no

Tracking
requirements

Acceptance
rationale

↓ yes   ↓ yes

Accept   **Mitigate**   **Watch**

**Scope and Actions:
What should I do?**

Mitigation plan

Mitigation plan

Risk action item list   yes   Is an action
item list
enough?   no →   **Task plan**
Responsibility
Goals
Tasks   WBS

Item 1- do xxxx
Item 3- do yyyy
Item 12- do zzz

Schedule

* Or "Do I need to act on this risk?"

Which Risks Are Mitigated?

Not all risks have to be mitigated, although all risks should be reviewed by personnel familiar with the issues. "Attempts to plan for the elimination of all risks are almost always futile efforts" [Charette 89]. The result of planning is a risk action plan. The types of risk action plans are

- *research plans*: strategy, actions, responsibilities, schedules, etc., for conducting the research, evaluating, and reporting the results
- *acceptance rationale*: reasons for accepting the risk, including the current conditions and assumptions that support the decision
- *tracking requirements*: the indicators, thresholds, and tracking requirements for watching the risk
- *mitigation plan*: the mitigation strategy, actions, due dates, responsibilities, etc., for mitigating the risk

Methods and Tools

This table provides a summary of the methods and tools used for each activity. More details are provided in subsequent sections of this chapter and in chapters in the appendix.

Activity	Method or Tool
All planning activities	Planning decision flowchart
	Risk information sheet
Responsibility	No specific method or tool—this is a management or team decision.
Approach	Goal-question-measure (for *watched* risks)
Scope and actions	Action item list
	Planning worksheet
	Problem-solving planning
	Risk form
	Note: Problem-solving planning is a type of "meta" method that references many other methods.

Section 2

Assign Responsibility: Is it My Risk?

Description
Once risks are identified and analyzed, they are reviewed by a project manager or a designated person(s) to determine what to do with them. Risks that are not assigned have a higher probability of being ignored until it is too late to take action. There are three choices in determining responsibility for risks:
- Keep the risk (it's yours).
- Transfer the risk upward within the organization or to another organization.
- Delegate the risk within your own organization.

Note: It is important to remember at the beginning of planning to review the risk and make sure it is understood. In particular, if the consequences were not originally part of the risk statement, they should be explored (as much as possible) at this point.

Objectives
The objectives of assigning responsibility for risks are to
- ensure that no risks are ignored, i.e., "fall through the cracks"
- make effective use of expertise and knowledge within the project
- ensure that risks are being managed by those with the appropriate abilities, knowledge, and authority to commit resources for mitigation

Diagram
The diagram below shows the decision process for determining responsibility.
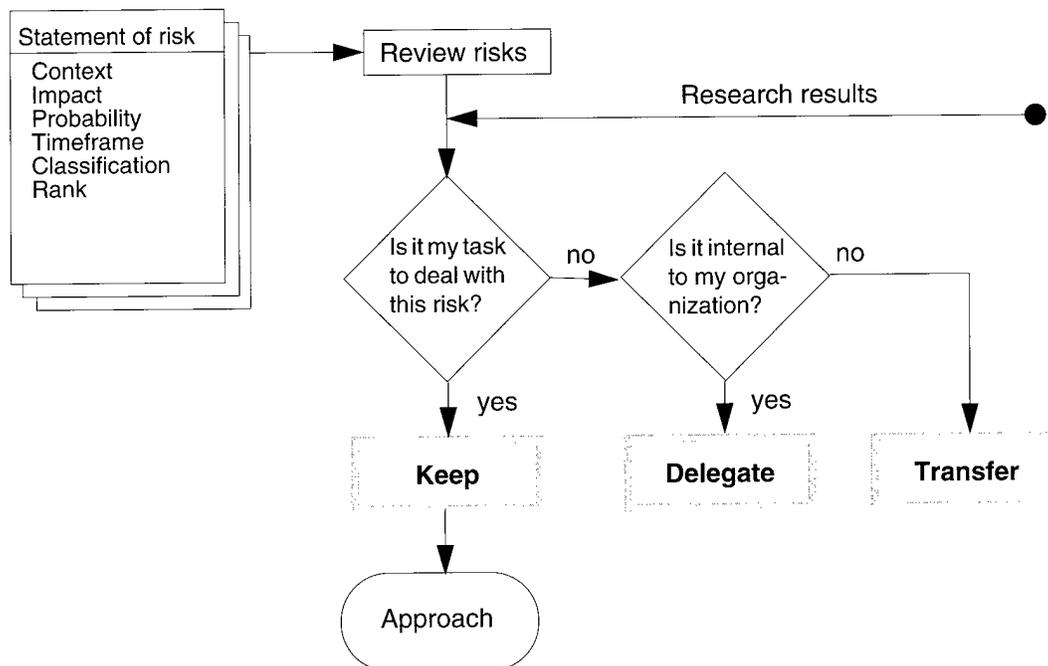
Responsibility Options
The following table further describes and provides examples of the three options for assigning responsibility. *Accountability* defines who is ultimately held "accountable" for the success or failure of mitigating the risk. Ultimately, the project manager is "accountable." *Responsibility* refers to who is charged with the duty of developing and implementing (or overseeing) the risk action plan. *Authority* is defined as the right and ability to assign resources for mitigation.

Option	Description	Example
Keep	Retain accountability, responsibility, and authority. You have the resources, knowledge, and position required to manage the risk. Part of the task might be accomplished by another, but you keep the responsibility and authority to commit resources and approve actions.	A manager has responsibility for a risk of inadequate Ada training and decides to contract for externally provided Ada instruction on a quarterly basis.
Delegate	Retain accountability, assign responsibility and authority. Delegate to maximize effective use of resources and relocate management of the risk closer to the source of expertise or knowledge.	A manager is responsible for a computer performance risk. One of his team's engineers has the required knowledge and expertise and is given the risk to resolve. Final approval of a mitigation strategy is retained by the manager as a part of accountability.
Transfer	Assign accountability, responsibility, and authority. Someone who is outside your organizational group is best able to manage this risk. Transferral implies the ultimate accountability, responsibility, and authority to expend required resources, etc., exists somewhere else. Transfers require acceptance of the risk by the other party. Transferer may ask to be kept informed of the risk status if the risk is going to impact the transferer. *Note*: If the transferee does not accept responsibility for the risk, the transferer may need to develop a contingency plan.	A software manager has identified a risk to her development schedule that originates with the hardware team. She transfers the risk to the hardware manager for resolution and asks for monthly status reports to avoid unpleasant surprises in her development schedule.

Questions to Consider

This is a list of the type of questions to consider when assigning responsibility for a risk or set of risks.
- Who could solve this risk?
- Who would have the power and authority to allocate resources?
- Who is accountable or can be held accountable for this risk?
- Who has the time to manage this risk?
- Who has the opportunity to take action?

**Transfer
Considerations**

While a transferred risk may be important to the one doing the transferring, the receiver of the risk may not have the same viewpoint or give the risk the same priority. The originator of the risk may need to develop a contingency plan in case the transferee chooses not to mitigate the risk.

**Plan:
Responsibility
Methods and
Tools**

There are no specific methods or tools for assigning responsibility; however, this table summarizes the methods and tools that assist this process.

Method or Tool	Description
Planning Decision Flowchart [Chapter A-21]	Tool to remind planners of possible responsibility options and the criteria for selecting those options
Risk Information Sheet [Chapter A-27]	Template for documenting who is responsible for the risk

Section 3

Determine Approach: What Can I Do?

Description

If the risk is your responsibility, then decide how to approach mitigating it.

- Do you know enough about the risk to decide? If not, *research* it.
- If the risk becomes a problem, can you live with the impact? or can the problem be more efficiently dealt with later as opposed to now? If so, *accept* the risk and expend no further resources managing it.
- If the risk can't be accepted, is there action you can take or must take (now or later)? If so, *mitigate* the risk—develop and implement a mitigation plan.
- If there is no reasonable mitigation action that can or needs to be taken, but you cannot accept the risk, watch the risk.

Objectives

The objectives of determining a mitigation approach are to

- ensure that you know enough to make an informed decision
- pick an appropriate approach for effective management of the risk(s)
- establish measurable mitigation goals to provide a target for evaluating success and direction during the development of action plans

Diagram

The following diagram shows the decision process for determining a mitigation approach.

* Or "Do I need to act on this risk?"
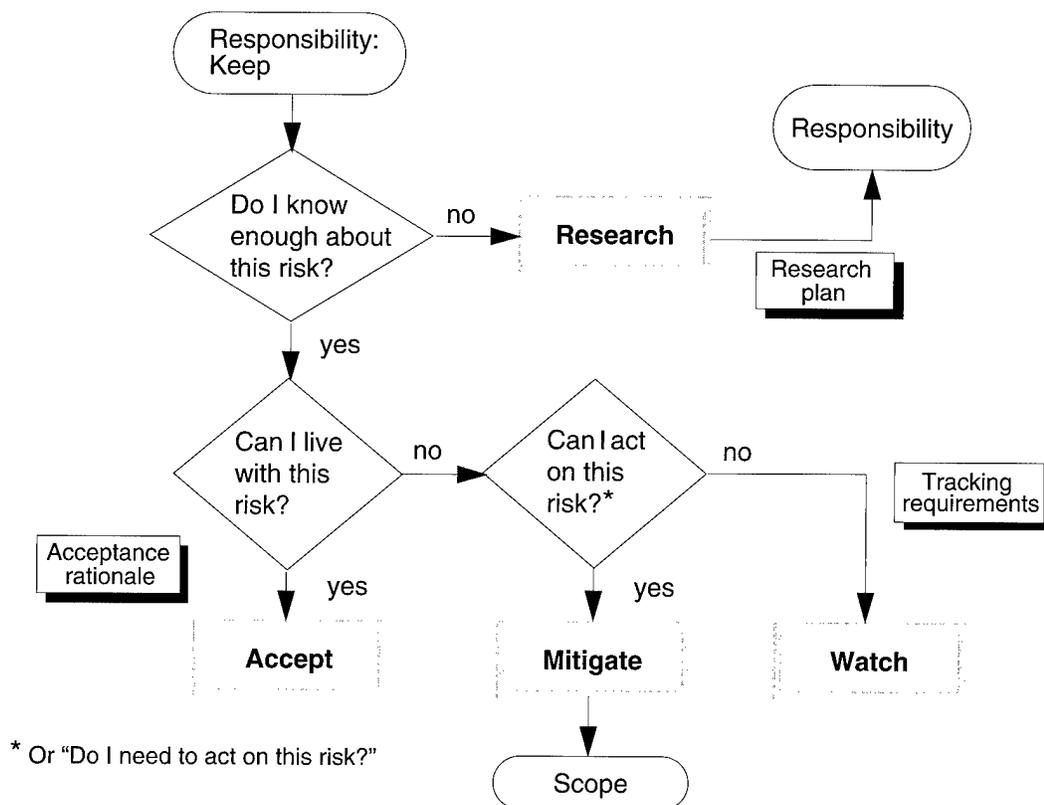
Additional Project Considerations

All risks cannot be planned simultaneously. Risks are planned in order of their importance, which depends on the goals and constraints of the project, managers, and individuals. However, priorities will change. When deciding what approach to take, consider these questions:

- What is currently important to the project, management, customer, or user?
- Are there critical milestones the project is currently facing?
- What limits and constraints does the project, organization, group, or manager have?
- What milestones and limits are fixed? flexible?
- What resources are available for mitigation?
- How does this risk fit into the overall project issues and concerns?

Range of Mitigation Approaches

This table provides a description of the range of mitigation approaches that can be used for a particular risk or set of risks.

Mitigation Approach	Description
Research	*Investigate* the risk until you know enough to be able to decide what to do (accept, watch, or mitigate). Research can range from making a few telephone calls to prototyping a system component.
Accept	*Do nothing*. The risk will be handled as a problem if it occurs (accepted risks are usually closed—see Chapter A-9). No further resources are expended in managing this risk. These are usually risks which are not significant enough to justify any expenditures—the project is willing to accept the consequences [Rowe 88].
Mitigate	*Eliminate or reduce* the risk by - reducing the impact (by some degree or to zero) - reducing the probability (to a lower probability or zero) - shifting the timeframe (i.e., when action must be taken) *Note*: recognize that mitigation plans may also introduce new risks to the project.
Watch	*Monitor* the risks and their attributes for early warning of critical changes in impact, probability, timeframe or other aspects. Decide what your goals for monitoring the risk are and what indicators will meet those goals [Basili 84]. Watched risks are usually those for which - existing conditions are not favorable for taking action; monitor for improved conditions - the potential for significant impact exists, but the probability is low - an early warning is needed to prepare for the consequences (take contingency actions).

Risk Action Plans

The type of risk action plan produced by this activity depends upon the selected approach. The following table identifies these.

Mitigation Approach	Risk Action Plan Type
Research	A *research plan* should document the actions and schedule for investigating the risk(s), evaluating the results, and reporting the conclusions. If the research schedule is lengthy, then indicators may also need to be identified to monitor the risk while it is being researched. Research ends with the action to reassign responsibility (if needed) and determine the next approach to take with the risk (accept, watch, or mitigate).
Accept	There is no action plan, however, accepted risks are generally closed [Chapter A-9], and the justification or *rationale for* accepting *the risk* should be documented in case the conditions change later.
Mitigate	A *mitigation plan* will document all of the actions required to mitigate the risk as well as supporting information such as tracking indicators and triggers [see Section 4 and Chapter 7]
Watch	*Tracking requirements* include indicators for monitoring the risk, triggers or thresholds for taking action, and reporting requirements (e.g., how often, by whom, extent of the report, and when) are identified [see also Chapter 7].

Planning Constraints

There are many constraints that can affect risk planning. These will vary with each project and situation. It is important to identify these and periodically check to make sure the circumstances have not changed. Never take constraints for granted.

Examples:
- project schedule limits or hard milestones
- available personnel
- hardware restrictions
- total cost of risk impact
- facility capacity and availability
- risk management budget (e.g., certain percentage set aside for mitigation)

When Mitigation Plans Already Exist

When looking at a risk and deciding what approach to take, consider its classification. Classification of risks helps find related risks that may already have mitigation plans in place. If a new risk is already being addressed by other mitigation plans, then those plans can be used. Risk documentation should be updated to identify the relationship and dependencies.

Existing Mitigation Plan Example

The following diagram shows that the newer risk M can use the existing mitigation plan for a set of risks related to "incomplete requirements" through the addition of two new actions.

Risk set—incomplete requirements

M added to risk set

M (new risk)

Action item list

Action 1
Action 2
Action 3
Action 4

Original mitigation plan

Action item list

Action 1
Action 2
Action 3
Action 3.1
Action 4
Action 5

Revised mitigation plan
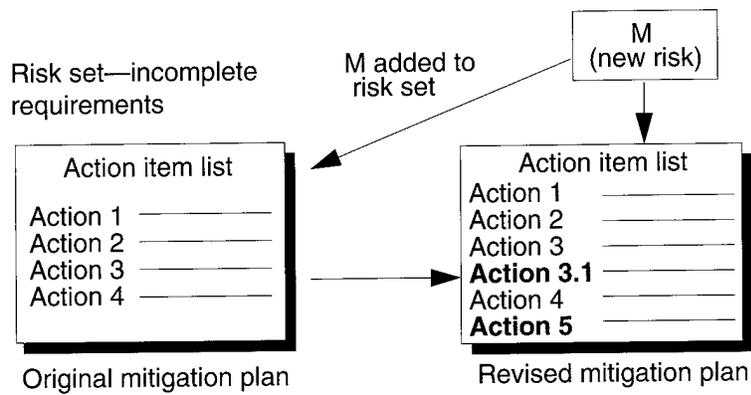
**Plan:
Approach
Methods and
Tools**

The following table summarizes the methods and tools for determining an approach for dealing with risks. Detailed descriptions of the methods and tools are provided in the appendix.

Method or Tool	Description
Goal-Question-Measure [Chapter A-13]	Technique for consideration and identification of indicators that can be used to track watched risks
Planning Decision Flowchart [Chapter A-21]	Tool to remind planners of possible approaches and the criteria for selecting those approaches
Risk Information Sheet [Chapter A-27]	Template for documenting who is responsible for the risk

Section 4

Define Scope and Actions: How Much and What Should I Do?

Description   Once mitigation has been chosen, the following questions must be answered:
- How complex will the mitigation be?
- How should it be documented?
- What is the strategy?
- What are the tasks?

There are generally two choices, based on the nature of the risk, complexity of the plan, and available resources:
- *action item list* for less complex mitigation (one or more actions)
- *task plan* with schedules and budgets for complex sets of actions

Note: Teams or groups are very effective at performing complex tasks that require multiple viewpoints [Scholtes 88], such as planning a complex risk.

Objective   The objective is to take a balanced approach in developing effective actions to mitigate risk(s). In other words
- avoid overplanning
- don't oversimplify

Note: The most effective solution is not always the first, most obvious, or immediate one, particularly with complex risks.

Diagram   This diagram shows the decision process for developing and documenting mitigation strategies.
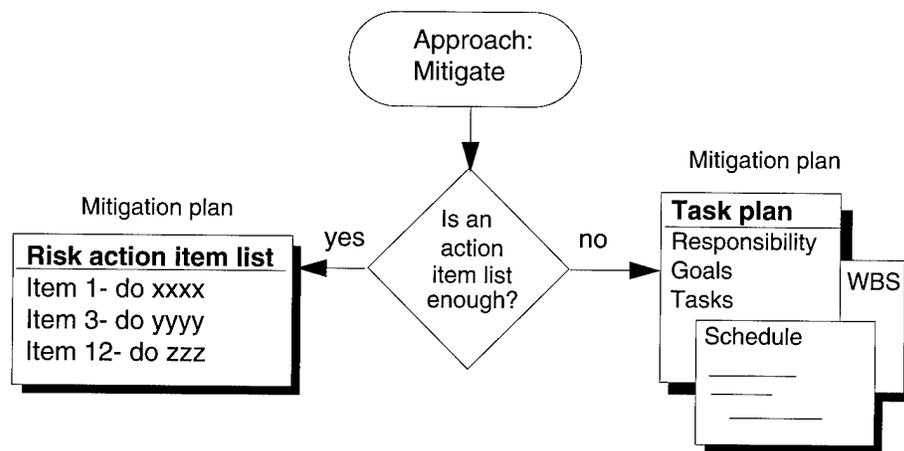
Mitigation Goals   It is important that a goal for mitigation be identified and documented. Goals will change, as circumstances and conditions improve or deteriorate, or as the constraints of the project force acceptance of less than perfect solutions. Mitigation plans should be periodically reviewed to ensure the mitigation goals are still sound and being met.

Action Item List vs. Task Plan

The following table summarizes the recommended contents for either an action item list or a task plan. More details can be found in the appendix under **Action Item List** [Chapter A-1], and **Problem-Solving Planning** [Chapter A-24]. Action item lists are simpler, but are not always appropriate for the complexity of the mitigation.

Note: Action item lists and task plans are two extremes. Anything in-between can also be used. It is not recommended that anything less than an action item list be used.

Action Item List	Task Plan
Risk statement(s)	Risk statement(s)
Mitigation goal/success measures	Mitigation goal/success measures or criteria
Responsible person	Responsible person(s)
	Related risks
	Due date for task plan completion
Action items	Chosen strategy(ies)
	Specific actions
	Budget
Due dates and closing date	Schedule (e.g., Gantt or PERT Charts)
	Risk tracking indicators, thresholds, reporting frequency
(Optional) contingency action and trigger	Contingency strategy and actions and trigger

What Type of Mitigation Plan Is Sufficient?

The type of mitigation plan needed for a risk(s) depends on many factors, including the following:
- relative importance of the risk(s)
- the complexity of the issues
- the breadth of expertise required to develop mitigation strategies
- probability and impact of the risk (particularly catastrophic)
- available planning resources (particularly personnel)

Return on Investment (ROI)

In relation to risk mitigation, return-on-investment (ROI) indicates how much benefit or reduction in risk exposure is achieved compared to the costs of planning and implementing the mitigation actions. One way to measure this is to use the original risk impact. A rule of thumb is 1:10—don't spend more than $100 to mitigate a risk that will cost $1000 if it becomes a problem.

Note: Remember that mitigation actions can cause additional risks. Consider those risks when determining the total cost of a mitigation plan.

Approval and Responsibility

The responsible person for the risk gets whatever approvals are necessary for the mitigation plan. Management approval may be needed to ensure that

- resources are not overcommitted
- conflicting mitigation plans are not implemented
- project objectives and constraints are not unintentionally violated

Specific actions may be distributed across several people. The responsible person for the risk is also responsible for assigning specific actions and seeing that all actions are effectively carried out.

Project Plans and Mitigation Plans

Complex or costly mitigation plans may impact the project plans. The project manager and personnel responsible for risks must keep in mind the impacts mitigation plans have on the current set of project plans. Project plans may need to be changed to reflect the activities being carried out to mitigate risks.

Plan: Scope and Actions Methods and Tools

The following table relates the type of mitigation plan with the methods or tools used to develop them. Detailed descriptions of the methods and tools are provided in the appendix.

Type of Mitigation Plan	Method or Tool	Description
For either action item lists or task plans	Planning Decision Flowchart [Chapter A-21]	Tool to remind planners of possible approaches and the criteria for selecting those approaches.
	Planning Worksheet [Chapter A-22]	Tool for analyzing and documenting the different aspects of developing mitigation action items or for documenting results as you develop the mitigation plan
	Risk Form [Chapter A-26]	Risk forms provide an optional field for a recommended mitigation action; this provides input to this activity
	Risk Information Sheet [Chapter A-27]	Template for documenting risk information and the chosen mitigation strategy and actions
Action item list	Action Item List [Chapter A-1]	List of one or more simple, obvious actions to mitigate a risk. Requires minimal documentation. Status is tracked and reported as part of the action item list.

Type of Mitigation Plan	Method or Tool	Description
Task plan	Problem-Solving Planning [Chapter A-24]	For a complex risk or set of related risks where dependencies are high and mitigation may be costly. Group expertise is required. Investigation and quantification of causes, probabilities, and impacts may be required. Detailed plans and schedules are needed. Status is detailed and reported frequently. Management approval is likely required to implement the task plan. Problem-solving planning includes the following methods and tools: • Affinity Grouping [Chapter A-2] • Brainstorming [Chapter A-7] • Cause and Effect Analysis [Chapter A-8] • Cost-Benefit Analysis [Chapter A-11] • Gantt Charts [Chapter A-12] • Goal-Question-Measure [Chapter A-13] • Interrelationship Digraph [Chapter A-14] • List Reduction [Chapter A-15] • Multivoting [Chapter A-17] • PERT charts [Chapter A-20] • Work Breakdown Structure [Chapter A-40]

Section 5

Considerations for Mitigating a Set of Related Risks

Description

Frequently, the most effective means of mitigating risks is to deal with them in sets, particularly if a large number of risks have been identified. Large numbers of risks can be made more manageable by classifying them into related sets. The planning process is modified with the following considerations when dealing with a set of related risks:

- Is there a set of risks that would benefit from coordinated mitigation (a mitigation area)?
- Do we know enough about these risks to proceed (their relationships, causes and consequences)?
- What are the goals of mitigating this set of risks (in addition to individual risk mitigation goals)?
- What strategies will address these risks, particularly the most important?
- What indicators are needed for monitoring a set of risks?

Objectives

The objectives of mitigating a related set of risks are to
- increase the cost-effectiveness of mitigation plans by eliminating duplicate efforts
- avoid conflicting mitigation goals and actions
- integrate planning efforts and avoid unnecessary time developing plans.

Mitigation Areas

In **Analyze** [Chapter 5], classification provides a view into the risks based upon related sets. If the basis for this relationship is the "big picture" of the risks in the project as opposed to identifying sets for mitigation, mitigation areas may need to be identified by looking for a common basis or reason for mitigation (e.g., the subsystem being impacted or who is responsible for the risk). Mitigation areas may include risks that are on the top N list of risks as well as those that are not.

Example: It might make more sense to group all of the compiler risks into a set to determine the common causes, take advantage of common mitigation actions, and ensure an integrated schedule of mitigation actions that will benefit the system component development efforts that depend on the compiler.

Analyzing a Set of Risks

In analyzing a set of risks, there are several key things to look for:
- causes and effects to identify common root causes or common effects that need to be avoided
- interrelationships among risks and causes—cycles of relationships (e.g., A causes B causes C causes D causes A) that can be broken or redefined

Mitigation Goals for a Set of Risks

Mitigation goals for a set of risks can be considerably more complex than the goals for a single risk. A hierarchy of goals may be appropriate, with a high level goal for the set and lower level goals for specific risks (especially any top N risks). It is important that all goals be identified and documented.

Strategies for Sets of Risks

The focus of the planning should be on mitigating the high priority (i.e., top N) risks. While mitigating all of the risks in the set is a desirable goal, it may not be realistic. Therefore, it is important to remember the relative priority or criticality of the risks to insure that the selected strategy deals with the most important or critical risks.

**Indicators for
a Set of Risks**

Monitoring a set of risks usually requires a hierarchy of indicators. Indicators can be high-level or abstracted, providing a summary status of the set. Additional indicators for specific risks in the set, particularly if there are any top N risks in the set, may also be used. If there are contingency plans, triggers or thresholds for those are also needed.

Section 6

Guidelines and Tips

Guidelines and Tips for Planning

Identify specific, implementable actions which will preempt problems.

Create the desired future state; things will not get better on their own.

Integrate risk mitigation plans with project plans when those plans affect project schedules, budgets, and deliverables.

Communicate mitigation plans to all affected personnel within the project, organization, customers, subcontractors, etc.

Do not lose sight of the end product when developing mitigation plans—don't unknowingly compromise the end product while trying to fix the smaller details.

References

Cited in this chapter:

[Basili 84]   Basili, Victor R. & Weiss, David M. "A Methodology for Collecting Valid Software Engineering Data." *IEEE Transactions on Software Engineering SE-10*, 6 (November 1984): 728-738.

[Charette 89]   Charette, Robert N. *Software Engineering Risk Analysis and Management.* New York: McGraw-Hill, 1989.

[Rowe 88]   Rowe, William D. *An Anatomy of Risk.* Malabar, Fla.: Robert E. Krieger, 1988.

[Scholtes 88]   Scholtes, Peter R. *The Team Handbook: How to Use Teams to Improve Quality.* Madison, Wi.: Joiner Associates, Inc., 1988.

Risk planning is similar to any other type of project planning or problem-solving activity. The approaches, methods, and tools are all very similar. This chapter includes a blending of many of the ideas and concepts proposed and discussed by the authors listed above, as well as those listed below:

[Boehm 89]   Boehm, Barry. *IEEE Tutorial on Software Risk Management.* New York: IEEE Computer Society Press, 1989.

[Kepner 81]   Kepner, Charles H. & Tregoe, Benjamin B. *The New Rational Manager.* Princeton, N.J.: Princeton Research Press, 1981.

[Lumsdaine 90]   Lumsdaine, Edward & Lumsdaine, Monika. *Creative Problem Solving.* New York: McGraw-Hill, 1990.

[Xerox 92]   Xerox Corporation and Carnegie Mellon University. *The University Challenge: Problem-Solving Process User Manual.* Stamford, Ct.: Xerox Corporation, 1992.

Chapter 7

Track
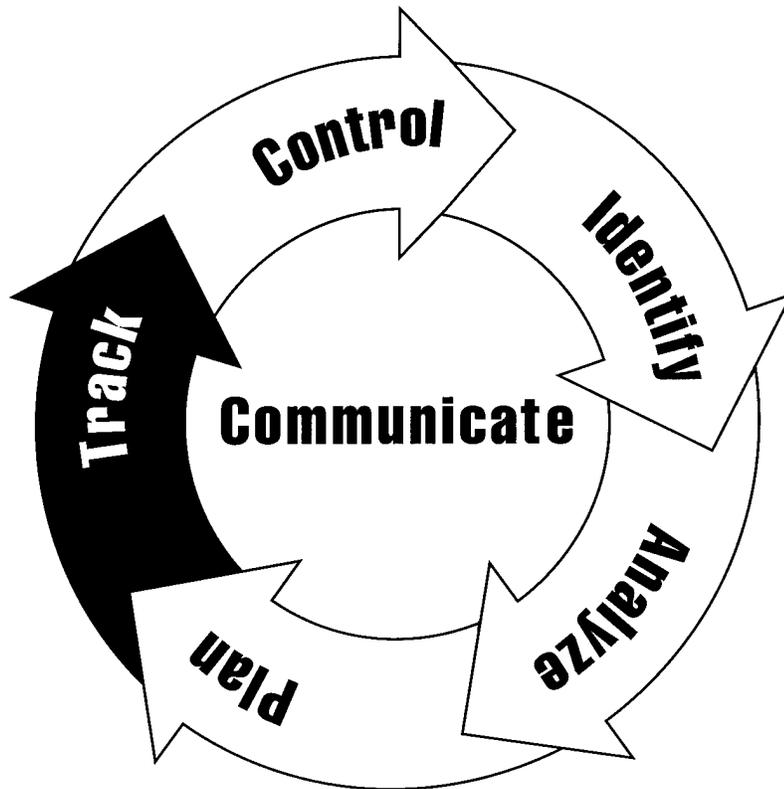
Section

Section 1

What Is Tracking?

Description   Tracking is a process in which risk data are acquired, compiled, and reported by the person(s) responsible for tracking watched and mitigated risks. The data required in status reports are defined by project personnel during the **Plan** function of the paradigm. During tracking, the data are collected and the results are compiled and presented in the reports. The generated document or presentation is input to the **Control** function, which is described in the next chapter.

Objectives   The objectives of the **Track** function is to collect accurate, timely, and relevant risk information and to present it in a clear and easily-understood manner appropriate to the person/group who receives the status report. The status reports generated during tracking are used by project personnel during control to make decisions about managing risks.

Diagram   The following diagram shows the inputs and outputs of the Track function.
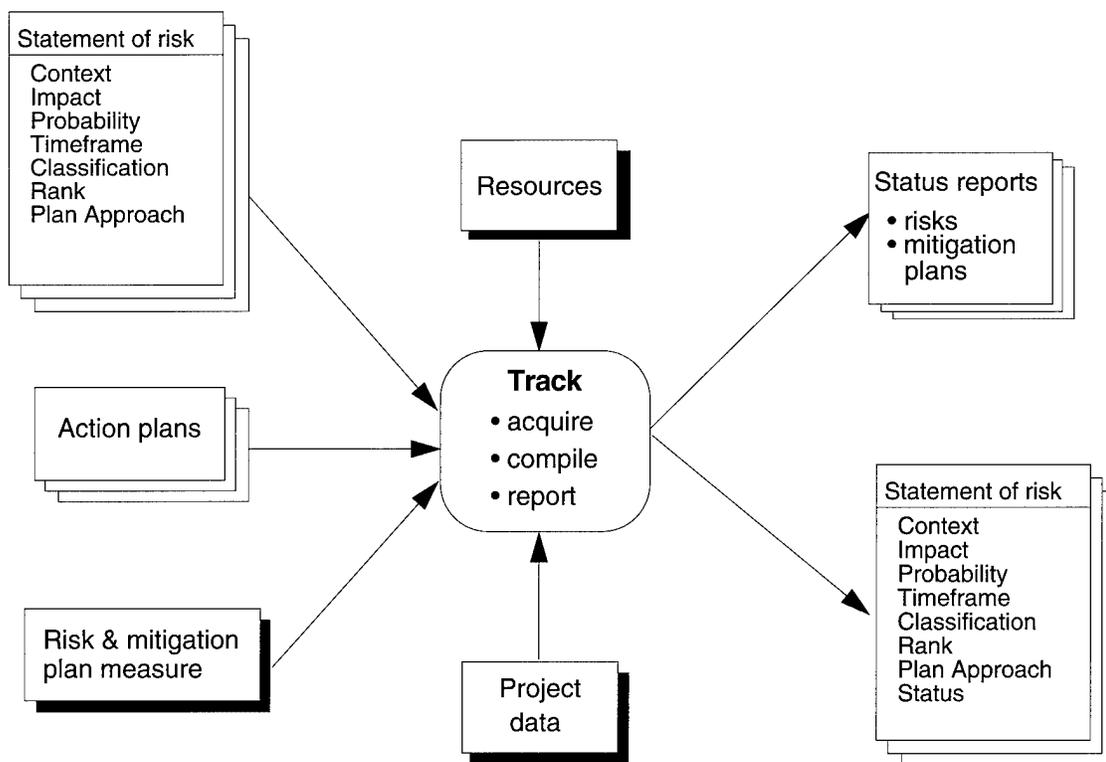
Data Items

The following table describes the data items of the Track function.

Data Item	Description
Statement of risk Context Impact Probability Timeframe Classification Rank Plan Approach	Prior to tracking, the risk information for each risk comprises the statement of risk, supporting context, impact, probability, timeframe, class, rank, and plan approach. This could be for all of the risks or for a small subset of risks targeted for risk tracking.
Action plans	Action plans describe what action will be taken to deal with the risk. Mitigation plans and tracking requirements for watched risks identify the measures, indicators, and triggers to track both the statuses of the risks and the mitigation progress.
Risk & mitigation plan measures	These consist of the current values for all watched-risk and mitigation-plan measures and indicators. These data can be used to determine the current status of the risk action plan and can be compiled and presented as part of a report.
Resources	These are the available resources for mitigation. In order to develop effective status reports, project personnel need to know the limits of the available resources to mitigate and watch risks.
Project data	Project information, such as schedule and budget variances, critical path changes, and project/performance indicators can be used as triggers, thresholds, and risk- or plan-specific measures where appropriate. This data can be used to determine the current status of the project plan as it relates to risk management and can be compiled and presented as part of a status report.
Status reports • risks • mitigation plans	The output of tracking is a variety of status reports highlighting the current values of the risk indicators and the statuses of action plans. These reports can be verbal or written, covering the status of both individual risks and aggregated risk areas as appropriate.
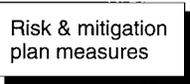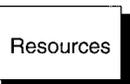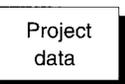
Data Item	Description
Statement of risk Context Impact Probability Timeframe Classification Rank Plan Approach Status	In addition to the delivery of status reports, tracking updates the information associated with each risk to include the current status data for the risk (e.g., measure, indicator, and trigger values).

Coordination of Tracking and Control

Risk tracking and control should be closely coordinated, because decisions that are made about risks and action plans during control require the data that are collected during tracking.

Example: The decision of whether to continue tracking a risk or to close it is made by project personnel during control, based on the data acquired during tracking.

Tracking and Control vs. Project Management

Risk tracking and control are closely related to standard project management monitoring techniques in which project data, such as schedule and cost data, are tracked. Project decisions are then based on the tracked data. When appropriate, the data used for risk management can be integrated and coordinated with existing project management activities for a project or organization.

Note: Standard project management techniques that are already being used on a project can also be employed to monitor the risk management processes (e.g., the number of risks opened and closed, changes to the risk management plan, etc.).

Sets of Related Risks

During risk identification and analysis, risks that are related can be grouped together for easier management; they can also be tracked as a set. If an overall plan has been developed for the set, then the set's mitigation plan is tracked, and risk and plan status data are reported as an aggregate. However, any individually critical risks can also be tracked separately from the set.

Approaches

There are not many tools specifically designed for tracking risks. Rather, there are approaches for tracking risks which utilize existing, general methods and tools. The following table summarizes the approaches used to support each of the tracking activities. More details on the approaches can be found in subsequent sections of this chapter and in the appendix chapters.

Activity	Approach	Method or Tool
Acquire	• Re-evaluate risk attributes (e.g., Binary or Tri-level attributes). • Interview knowledgable project personnel. • Review technical documentation and engineering summary reports (e.g., PERT charts, schedules, budgets, requirements traces, etc.). • Review status reports or meeting minutes. • Collect data from project products using automation.	Binary attribute evaluation Tri-level attribute evaluation
Compile	Data are analyzed and compiled into status reports according to the project's reporting requirements. This is the step where trends are examined. Reporting approaches supported by the compile activity may include any of the following: • mitigation plan status summaries • risk status summaries • trend summaries	Bar graph Mitigation status report Risk information sheet Spreadsheet risk tracking Stoplight chart Time correlation chart Time graph
Report	• Deliver verbal reports. • Deliver written reports. • Give formal presentations. *Note*: Any of the above reports can show status for individual risks, aggregated areas of risks, trends, or a mixture.	Mitigation status report Risk information sheet Spreadsheet risk tracking Stoplight chart

Section 2

Tracking Definitions

Description

This section defines terms and types of tracking data used in both the **Track** and **Control** chapters.

Metric

A software *metric* defines a standard way of measuring some attribute of the software development process [Grady 87]. Likewise, a risk metric defines a standard way of measuring some attribute of the risk management process.

Measure

A risk *measure* (which is synonymous with metric [Baumert 92]) defines a standard way of measuring some attribute of the risk management process. Risk and mitigation plan measures can be qualitative or quantitative.

Example: The values of the risk attributes, e.g., the impact of a risk and the probability of a risk occurring, are examples of risk measures.

Indicator

Indicators are representations of measurement data that provide insight into a process or improvement activity [Baumert 92]. They can be used to show status and, in this document, are also called status indicators. Indicators may use one or more measures, and they can give a more complex measure of the risk and mitigation plan.

Indicator Example

In the following diagram, a measure from Risk A as well as two measures from tasks in the mitigation plan are used to create Status Indicator B.

Trigger

Triggers are thresholds for indicators that specify when an action, such as implementing a contingency plan, may need to be taken. Triggers are generally used to
- provide warning of an impending critical event
- indicate the need to implement a contingency plan to preempt a problem
- request immediate attention for a risk

Trigger Example

A given risk on a project is the following:

Not all developers are trained in the new compiler; delivery of coded modules may be delayed.

This example is related to the previous diagram. Measure M3 is the number of developers trained each week; M4 is the schedule of milestones indicating the beginning of development for each module; and M5 is the number of developers required for each module. The combination of M3, M4, and M5 yields Status Indicator B, which is the available number of trained developers for modules under development. Project personnel could define the trigger in this example to be the point at which the number of available trained developers is 10% below the required number.

Measure vs. Indicator

In general, a measure reflects a characteristic of a risk, while an indicator uses one or more risk measures to provide insight into or show the status of the management of a risk.

Example: Risk exposure, which is the product of the probability and impact of a risk, can be used as a status indicator. Impact and probability are usually risk measures.

What Makes a Good Risk Indicator?

For an indicator to be categorized as "good," it needs to possess the following characteristics [Baumert 92]:
- It must be easy to derive or calculate.
- It must lend itself to straightforward or easy data collection efforts, preferably automated methods.
- It must be relevant to the mitigation goal or risk.

Note: Both qualitative and quantitative data can be used to track risks and plans. While quantitative data are more precise and more likely to be accurate, it is not always feasible or an effective use of resources to refine data to a quantitative level. Qualitative, even instinctive, evaluations of status can be used to support decision making when quantitative data are unavailable.

Effective Indicators for Risk Tracking

Effective tracking indicators focus on the anticipatory aspects of the available data. The trend of a measure over time is often a good indicator. With historical information, trends in the data are more important than the values at any one time.

Example: A useful status indicator may be the number of coding errors debugged per week, and the trend of this indicator can be used by project personnel for risk management as appropriate.

What's an Effective Trigger?

Effective triggers
- provide early warning, giving project personnel enough time to take an appropriate action or to focus extra attention on the risk
- do not trip unnecessarily
- are easy to calculate and report

**Risk Example
Background**

The following example presents a risk and a set of tracking measures, indicators, and triggers for the chosen risk.

Risk Statement: No simulation of the system's display performance has been done; we may not meet the performance requirements.

Context: During the initial phases of planning, a high-fidelity performance simulation of the system was defined but was cut due to budget considerations. Nothing was substituted, not even a limited low-fidelity simulation or an order-of-magnitude analysis. We have implemented 20% of the screen display code, and it already takes 30% of the total available frame-time for updating the sensor displays. No one is monitoring the performance.

**Risk Example
Data**

In this example, attribute values are estimated based on the AFSC/AFLC Pamphlet 800-45 [Air Force 88]. From the risk's impact and probability attribute values, project personnel determine the level of risk exposure, which will be one of the indicators used to track the risk. Next, personnel determine the trigger value for risk exposure. For this particular risk, additional measures are used to calculate a second indicator, "frametime used/code complete ratio," and project personnel determine a trigger for that indicator as well. The measures, indicators, and triggers and their values for this example are shown below.

Data	Type	Value/Description
Probability	Measure	Probable
Impact	Measure	Critical
Risk exposure	Indicator	Moderate
Trigger value for risk exposure	Trigger	If the risk exposure value becomes "High," then project personnel will consider implementing a contingency plan.
% Frametime used	Measure	30%
% Code complete	Measure	20%
Frametime used/code complete ratio	Indicator	30% / 20% = 1.5
Trigger value for frametime used/code complete ratio	Trigger	The Frametime Used/Code Complete Ratio must be 0.75 when the code is 45% finished. If it exceeds this value, then a contingency plan will be implemented.

Section 3

Acquire

Description The Acquire activity is a process which includes all of the steps associated with collecting information about and updating the values of risk measures and status indicators for watched and mitigated risks. The required data are defined by project personnel during planning and are used to track the progress of watched risks and risk mitigation plans. After the data are collected, the compile activity organizes them. This section outlines the Acquire activity.

Objective The objective of the acquire activity is to collect all relevant tracking data for a given risk.

Diagram The following diagram shows the inputs and outputs for acquiring risk data.
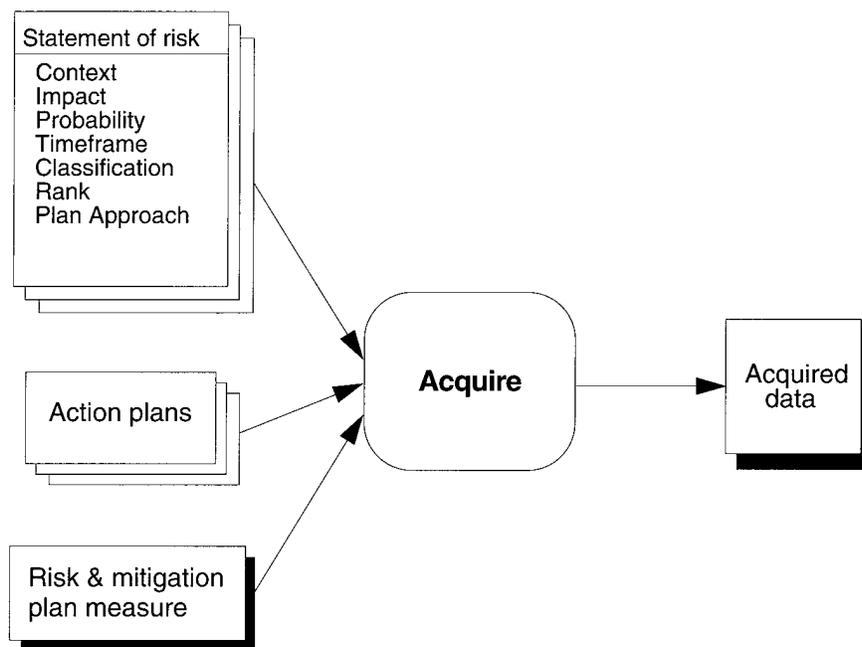
Data Acquired Risk data for watched risks, mitigation plan data, and other project data are collected during the Acquire activity. The frequency of data collection is defined in risk action plans.

Risk Data Example In **Mitigation Status Reports** [Chapter A-16], risk exposure is the indicator which is tracked over time. It is derived by using two measures: the impact level of the risk and the probability of the risk occurring. Project personnel estimate the impact (e.g., on a scale of 1 - 5) and the probability (e.g., on a scale of 1 - 10). After these data are estimated by the project personnel, the measures are considered to be "acquired" for the risk.

Indicators for Sets of Related Risks

Related risks can be grouped together and then tracked as a set. The impact, probability, and timeframe measures as well as set indicators can be estimated, and triggers, or even a set of them, can be established for the indicators. If an overall mitigation plan has been developed for the set, then it is tracked. Both set risk indicators and individual risk indicators could be acquired and reported, particularly if the set of risks includes one or more individually critical risks.

Set of Related Risks Example

There are several training-related risks associated with a project. Collectively, they represent a critical mass of potential problems that could cripple the project's schedule. The project manager has requested a weekly report on the status of the training effort. Individual measures are gathered for the types of training being provided, the personnel being trained, and the availability of self-training materials and tool documentation. A cumulative indicator is then derived from the individual measures. However, the most critical training issue is focused on compiler training. Its associated measure is the number of development programmers who have received training for the chosen compiler. That information is retained and reported as a separate indicator.

Considerations When Acquiring Data

The following considerations should be kept in mind when acquiring tracking data:
- Status information is only as good as its accuracy and timeliness.
- Stale data are more dangerous to decision makers than no data at all; a wrong decision could be made based on false assumptions.
- When a group of indicators is required (e.g., to report status of a set of risks or of a collection of plans), all of the data must be acquired from the same time period.
- The collection of tracking data is the responsibility of the person responsible for the risk or its mitigation (unless the task is delegated).

Track: Acquire Approaches

The following table summarizes the approaches, methods, and tools that can be used to acquire risk data. Detailed descriptions of the methods and tools are provided in the appendix.

Approach	Description	Usefulness
Re-evaluate risk attributes	The individual responsible for the risk should periodically re-evaluate the risk attributes to determine changes in probability, impact, and timeframe. The following methods are designed to evaluate risk attributes: • Binary Attribute Evaluation [Chapter A-6] • Tri-level Attribute Evaluation [Chapter A-38] Access to knowledgeable individuals or other data may be required.	These help project personnel understand the current values of probability, impact, and timeframe as well as evaluate the success of mitigation plans.

Approach	Description	Usefulness
Direct communication	This is informal communication with the personnel closest to the risk or risk mitigation activity. Often, the software engineers working on the project or other personnel directly responsible for actions on the risk or the plan are interviewed. In some cases, the individual who is interviewed may be the manager responsible for the risk or mitigation plan.	This provides timely communication of potential new risk areas. This provides status information for watched risks and mitigation plans.
Review of technical document-ation or engineering summary reports	This involves looking at the technical aspects of the progress of the development effort.	These reviews can be useful for technical risks but can also provide insight into general project issues. These can also be used to look for new risk information.
Review of status reports or meeting minutes	This involves a review of documentation available from the routine project status meetings.	These reviews can provide insight into general project issues. They provide status information for watched risks and mitigation plans.
Automated data collection from project products	This involves using commercially-available tools to track and collect progress and quality measures from the project's products and reports.	These tools provide consistent, often quantitative risk data. The measures collected can be used as indicators to track risks and the progress of mitigation efforts.

Section 4

Compile

Description

The Compile activity is the process in which data for a given risk is analyzed, combined, calculated, and organized for the tracking of the risk and its associated mitigation plan. The data are collected during the acquire activity and are presented during the report activity.

Note: The reporting requirements determine how project personnel compile the data.

Objective

The objective of the Compile activity is to organize the relevant tracking data for a given risk. The report can include a summary of the risk, its watch requirements or mitigation plan, and other key issues relevant to the risk or mitigation plan.

Diagram

The following diagram shows the inputs and outputs for compiling risk data.
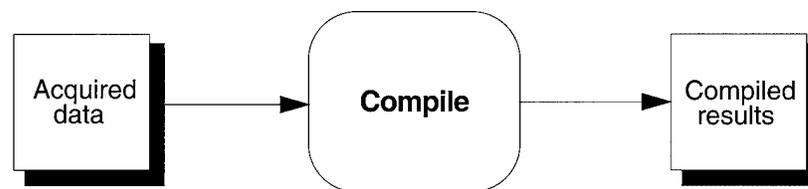
What Data are Compiled?

While data are being analyzed and compiled into reports, project personnel must keep in mind the overall strategies and goals of the watch requirements or risk mitigation plan. Paying attention to the triggers for risk indicators is only one aspect of data analysis. Other factors to keep in mind are: the mitigation goal, expected plan progress, broad-based trends, and specific milestones or events. The risk's tracking requirements and mitigation plan should identify what indicators need to be compiled.

Compiling Data for Sets of Related Risks

For a set of risks, individual risk data are combined, calculated, and reformulated to present a cohesive picture of the current risk status. Databases or appropriate analysis and reporting forms can be used to aid the compilation of data for this activity.

Report Consider- ations

Reports can be either written or verbal and can be part of either formal or informal reporting processes. The following are the primary considerations of reporting:
- What information needs to be reported?
  - status of risk
  - status of mitigation efforts
  - trends
  - significant changes
- What results are desired from review of the report?
  - management understanding
  - control decision (close, transfer, etc.)
- Does the format of the report match the desired outcome?
  - Is there enough data to support an informed decision?
  - Is there too much data to permit the appropriate points to be made?
  - Are the key points easily distinguishable from supporting data?
  - Is this the most efficient reporting mechanism?

Report Content

Report content and format should be driven by the following factors: the tracking requirements of the risk and mitigation efforts as well as the intended audience of the report (e.g., senior managers usually have limited time available and prefer abstracted, summarized reports).

Data Trends and Patterns

Trends can be observed through the evaluation of successive reports. Persistent lateness in taking action, oscillating priority values, significant changes in the number of high-impact risks or risks of a particular type, and other trends should be identified, analyzed, and evaluated for additional negative or positive indicators. These may not be trends that are specifically examined at every opportunity, but patterns that are identified over time and investigated when appropriate. Analysis of trends and patterns can also lead to the identification of new risks to the project.

Data Trend Example

A technical lead notices an unusual increase in the number of testing-related risks in the top N project risks during the last three weeks. While it might be expected that as coding progresses more testing issues will surface, software coding for this project has not begun. Analysis of the testing-related risks showed that the test plans, which have been completed and distributed for review, are perceived to be inadequate. The technical lead identifies a new risk to the program which focuses on the completeness of the test plans. The mitigation plan for the new risk calls for project personnel to receive more training in the area of software testing and in the development of test plans.

Track: Compile Approaches

The following table summarizes the approaches, methods, and tools used to compile data. Effective approaches include graphic and tabular summaries of the key measures and indicators for risks and their related mitigation actions. Effective summaries also include time history information, which facilitates the identification of trends and variations. Detailed descriptions of the methods and tools are provided in the appendix.

Approach	Description	Usefulness
Mitigation plan status summaries	Plan summaries are reports which require compiled data showing mitigation plan progress. Mitigation Status Reports [Chapter A-16] are designed to track plan status.	Mitigation status reports employ textual information and graphics (e.g., time graphs) to document detailed information on specific risk mitigation plans and are used to support decisions.
Risk status summaries	Summary tables are concise tabular compilations of key data items. The following methods and tools are designed to produce and use tabular formats: • Risk Information Sheet [Chapter A-27] • Spreadsheet Risk Tracking [Chapter A-30] • Stoplight Chart [Chapter A-31] The analysis of current status data can identify changes in priority or the need for outside help. It can also identify new risks to the project.	Risk information sheets are used to document detailed information on specific risks and to support decisions. Spreadsheet risk tracking reports are used to summarize the current status of all risks. They are best used to support routine project activities. Stoplight charts summarize the status of important risks and their mitigation efforts. They are effective tools for reporting risk information to senior management.
Trend summaries	Trend summaries are graphical representations of compiled risk data. The following are used to present risk data on graphs or charts: • Bar Graph [Chapter A-3] • Time Correlation Chart [Chapter A-35] • Time Graph [Chapter A-36]	Bar graphs are graphical representations of data across distinct categories. They highlight changes in the number of risks in individual categories and can be used to identify trends. Time correlation charts show the relationship of one indicator with respect to another over time. They are useful for identifying the trend over time in the relationship of two indicators. Time graphs are graphical representations of data variations over time. They are useful for identifying the trend over time of an indicator for a risk. They are also used in Mitigation Status Reports [Chapter A-16].

Section 5

Report

Description

The Report activity is a process in which status information about risks and mitigation plans is communicated to decision makers and team members. The delivered reports summarize the data that were analyzed and organized in the Compile activity and are the input to the **Control** function.

Note: The Compile and Report activities are related. Reporting requirements drive how project personnel compile the data.

Objective

The objective of reporting is to communicate risk status reports to support effective decision making.

Diagram

The following diagram shows the inputs and outputs for communicating risk data.
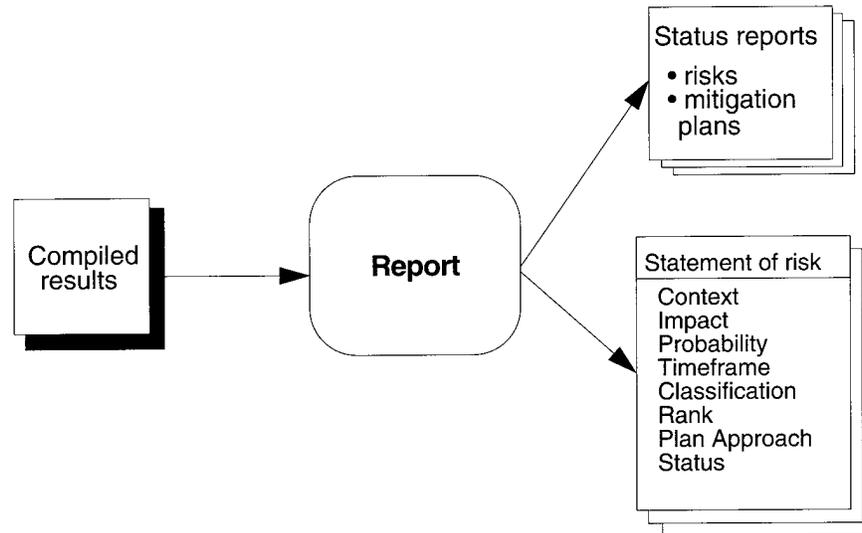
Reporting Schedule

Reports are generally delivered as part of routine project management activities (e.g., as part of a weekly or monthly project status update). The frequency of reporting depends upon the following:

- the reporting requirements for each risk or type of risk (e.g., important risks reported on weekly, others bi-weekly)
- the manner in which the report will be used
  - read-ahead material for a meeting vs. material handed out and scanned at the meeting
  - material to support the decision-making process
  - material to document current risk status for history files/records

Note: A critical event or condition may require exception reporting to management rather than waiting for the next report period.

Reporting Schedule Example

On a given project, spreadsheet risk tracking reports are normally used as read-ahead material for weekly project meetings. They contain only the important risks—those being watched and planned, as well as new risks. However, once a month, all risks are included in the report. This gives project personnel the opportunity to review the less important risks and determine whether any have become more critical.

Also, once a month, senior managers get a stoplight chart on the top N risks to the project. These charts indicate which risks may become critical and where senior management decisions are required.

Formal presentations of the important risks are made each quarter to all organizations at a site. This is done to keep other projects informed of the progress being made.

Track: Reporting Approaches

The following table summarizes the approaches, methods, and tools for reporting status. Detailed descriptions of the methods and tools are provided in the appendix.

Approach	Description	Usefulness
Verbal reporting	Verbal reports are generally informal. The people responsible for the risks give verbal reports on the general status of their risks. They may also use this forum to inform management of critical issues as they arise (written status would usually be required as a follow-up).	Verbal reports are useful for informal reporting of status to management and immediate notification of critical issues or changes.
Written reports	Written reports may be either formal or informal memoranda (e.g., electronic mail, reports, etc.). They should be integrated into the normal status reporting mechanisms used by the organization. The following can be used for this activity: • Mitigation Status Report [Chapter A-16] • Risk Information Sheet [Chapter A-27] • Spreadsheet Risk Tracking [Chapter A-30] • Stoplight Chart [Chapter A-31]	Mitigation status reports employ graphics to document detailed information on specific risks and are used to support decisions. Risk information sheets are used to document detailed information on specific risks and to support decisions. Spreadsheet risk tracking reports are used to summarize the current status of all or selected risks. They are best used to support routine project activities. Stoplight charts summarize the status of important risks and their mitigation efforts. They are effective tools for reporting risk information to senior management.
Formal presentations	Presentations use the media and format which is appropriate for the organization. Written reports are produced to support formal presentations.	Formal presentations usually contain material that explains risk management, the status of ongoing mitigation efforts, etc. This information might not be included in written reports.

Section 6

Guidelines and Tips

Guidelines and Tips for Track

Make information openly available to all project personnel.

Present data in a clear and concise manner for the intended audience.

Choose indicators that give insight into the important project risks by being predictive in nature.

Choose trigger values that give project personnel enough time to react to current conditions and to take appropriate actions in a timely manner.

References

Cited in this chapter:

[Air Force 88]   Air Force Systems Command/Air Force Logistics Command Pamphlet 800-45. *Software Risk Abatement*, September 30, 1988.

[Baumert 92]   Baumert, John H. & McWhinney, Mark S. *Software Measures and the Capability Maturity Model* (CMU/SEI-92-TR-25). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1992.

[Grady 87]   Grady, Robert B. & Caswell, Deborah L. *Software Metrics: Establishing a Company-Wide Program*. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1987.

For more information on controlling risks and the methods and tools required, see the following:

[Clark 95]   Clark, Bill. "Technical Performance Measurement in the Risk Management of Systems," Presented at the Fourth SEI Conference on Software Risk, Monterey, Ca., November 6-8, 1995. For information about how to obtain copies of this paper, contact SEI Customer Relations at (412) 268-5800 or customer-relations@sei.cmu.edu.

[Rosenau 92]   Rosenau, Milton D. *Successful Project Management: A Step-by Step Approach With Practical Examples*. New York: Van Nostrand Reinhold, 1992.

Chapter 8
Control
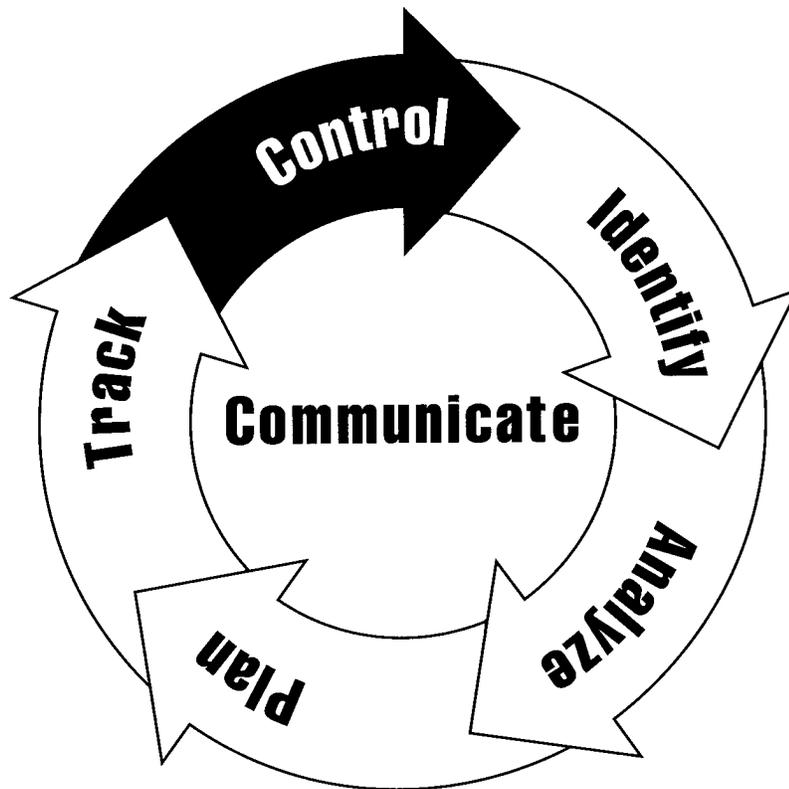
Section 1

What is Control?

Description The **Control** function is the process that takes the tracking status reports for the watched and mitigated project risks and decides what to do with them based on the reported data. The person who has accountability for a risk normally makes the control decision for that risk. The general process of controlling risks includes the following:
- analyzing the status reports
- deciding how to proceed
- executing the decisions

Objective The objective of the Control function is to make informed, timely, and effective decisions regarding risks and their mitigation plans.

Diagram The following diagram shows the inputs and outputs of the Control function.
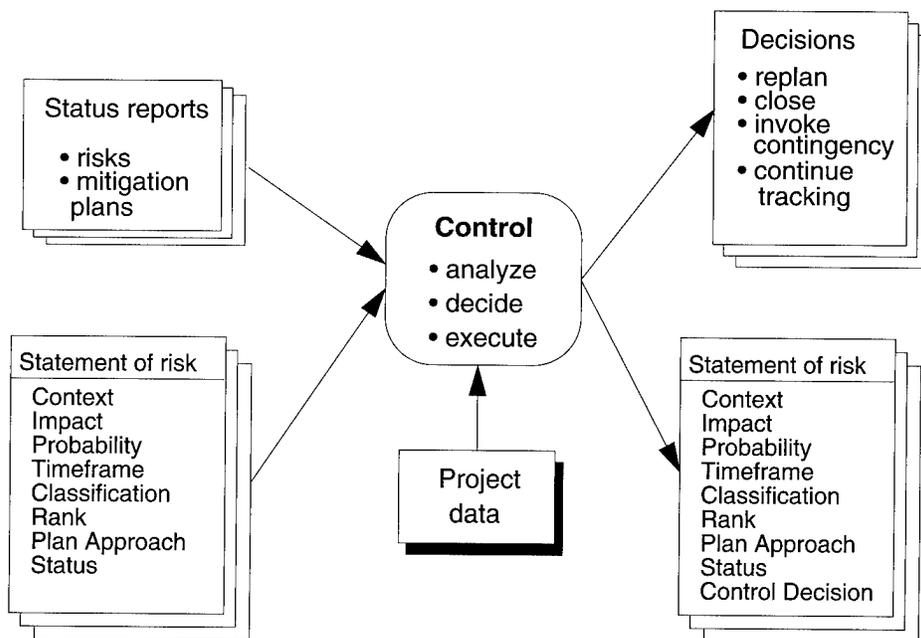
Data Items

The following table describes the data items of the Control function. The outputs are actually decisions and their related products.

Data Item	Description
Status reports • risks • mitigation plans	A variety of status reports are used to highlight the current values of the risk indicators and the statuses of action plans. These reports can be verbal or written, covering the statuses of both individual risks and aggregated risk areas as appropriate.
Statement of risk Context Impact Probability Timeframe Classification Rank Plan Approach Status	Prior to the Control function, the risk information for each risk comprises the statement of risk, supporting context, impact, probability, timeframe, class, rank, plan approach, and status. This could be for all of the risks or for a small subset of risks targeted for risk control.
Project data	Project information, such as schedule and budget variances, critical path changes, and project/performance indicators can be used to support decision making where appropriate. This data can be considered when project personnel make control decisions.
Decisions • replan • close • invoke contingency • continue tracking	The output of the Control function is a decision that determines the next action for the risk or set of risks under consideration. There are four possible decisions: • replan • close the risk • invoke a contingency plan • continue tracking and executing the current plan
Statement of risk Context Impact Probability Timeframe Classification Rank Plan Approach Status Control Decision	In addition to making a control decision, the Control function updates the information associated with each risk to include the current control decision for the risk (i.e., replan, close the risk, invoke a contingency plan, and continue tracking and executing the current plan).
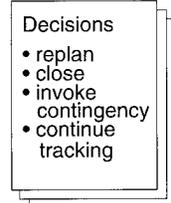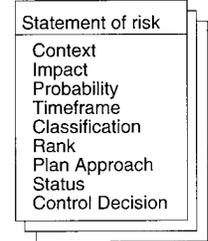
What is Effective Control?

Effective control requires anticipating and assessing the effectiveness of mitigation plans as well as monitoring the quality of executing the plans (i.e., Are the plans being executed correctly? Are the results what was expected?). It also involves assessing significant changes in risks (e.g., changes in their attribute values).

Control and Project Management

Risk control is related to standard project management monitoring techniques. These methods use project measures, such as schedule and cost metrics, for tracking, and decisions are based on the acquired data. Controlling risks is a process step that should be easily integrated and coordinated with the routine activities associated with management decision-making processes already established within the project.

Sets of Related Risks

During risk identification and analysis, risks that are related should be grouped together for easier management. For such sets, risk and mitigation plan status data are reported as an aggregate. Project personnel use the reports generated in tracking to make informed, timely, and effective decisions regarding sets of risks and their mitigation plans. The reports are analyzed and evaluated, and decisions are made and executed. When a set of risks is being analyzed and its trigger is reached, a decision should be made whether to look at individual risks. Any specific problems should be identified and addressed as appropriate.

Methods and Tools

The following table summarizes the methods and tools used to support risk control activities. More details on the methods and tools can be found in subsequent sections of this chapter as well as in the appendix chapters.

Note: Methods employed for risk control use basic techniques for analyzing and deciding on an action, documenting the decision, and proceeding with the chosen actions. Most organizations have an established suite of effective methods for such activities. If these techniques do exist within an organization, then they should also be applied to risk status information.

Activity	Method or Tool
Analyze	Cause and effect analysis Cost-benefit analysis Mitigation status reports PERT charts Spreadsheet risk tracking Stoplight charts
Decide	Closing a risk List reduction Multivoting
Execute	Closing a risk Mitigation status reports Risk information sheet Spreadsheet risk tracking Stoplight charts *Note*: Making changes to plans requires a return to planning, while taking predefined contingency actions and continuing to track risks require a return to tracking.

Section 2

Analyze

Description   The Analyze activity uses tracking data to examine project risks for trends, deviations, and anomalies. The goal is to achieve a clear understanding of the current status of each risk and mitigation plan relative to the project.

Objective   The objective of the Analyze activity is to provide information needed by decision makers to accurately determine the best courses of action for project risks. Decision makers need to know if there is a significant change in risks or if mitigation plans are ineffective within the context of project needs and constraints.

Diagram   The following diagram shows the inputs and outputs for analyzing risks.
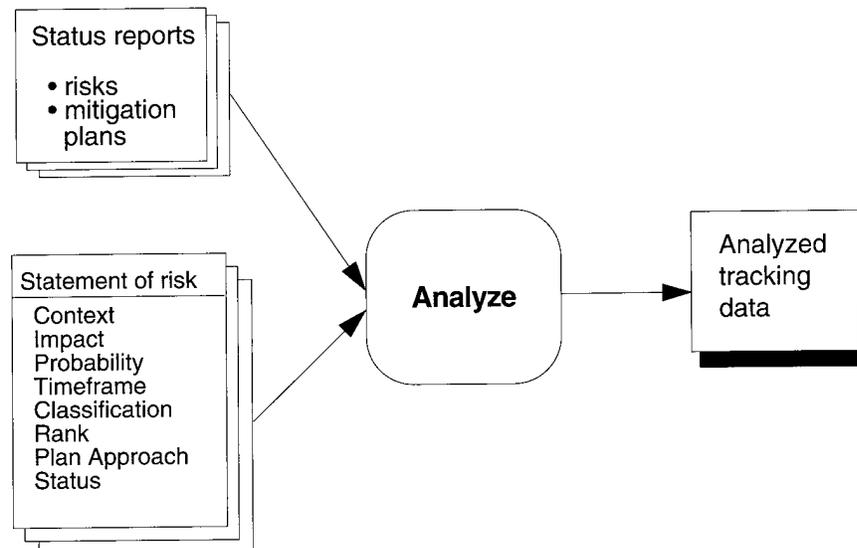
Control:
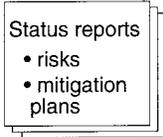**Analyze**
Methods and
Tools

The following table summarizes the methods and tools that can be used to analyze tracking data. Virtually all general methods for information analysis can be used during this activity. Detailed descriptions of the methods and tools are provided in the appendix.

Method or Tool	Description
Cause and Effect Analysis [Chapter A-8]	Analyzing the causes and effects of risks and actions may provide additional insight into their dependencies and relationships to support decisions. For example, this method can help to determine the merits of continuing with a current set of mitigation actions.

Method or Tool	Description
Cost-Benefit Analysis [Chapter A-11]	The costs and benefits of a particular mitigation strategy can be re-evaluated if the strategy is not having the expected results. This method provides the information needed by decision makers to determine whether to continue as planned or to replan.
Mitigation Status Reports [Chapter A-16]	These reports use a visual method for tracking risks. In this technique, risk exposure is tracked over time, and both the value of risk exposure and its trend are used as indicators. This method provides decision makers with the data required to determine the appropriate control actions (e.g., invoke contingency plan, replan, etc.).
PERT Charts [Chapter A-20]	These dependency and probability schedules can be used to analyze the impacts of changes in risk status and mitigation plans. For example, the effect on a project's critical path from a significant increase in the time to complete a critical system component can easily be determined from a PERT Chart.
Spreadsheet Risk Tracking [Chapter A-30]	Current and historical tracking information is provided by a spreadsheet showing major changes and significant trends. Adverse trends or changes can be highlighted, and thresholds that are reached can also be identified (e.g., estimated impact of an unmitigated risk exceeds $10,000).
Stoplight Chart [Chapter A-31]	Senior managers can use these abstract-level status reports to determine whether or not they need to take action. Red, for example, may indicate that senior management action is required for a risk or set of related risks.

Section 3

Decide

Description   The Decide activity uses tracking data to determine how to proceed with project risks. Four basic decisions can be made:

- replan
- close the risk
- invoke a contingency plan
- continue tracking and executing the current plan

Objective   The objective of the Decide activity is to ensure that project risks continue to be managed effectively. Contingency plans should be implemented as soon as indicators show that they are needed. Replanning also must be completed in a timely manner to correct deviations and to avoid further potential loss.

Diagram   The following diagram shows the inputs and outputs for making control decisions.
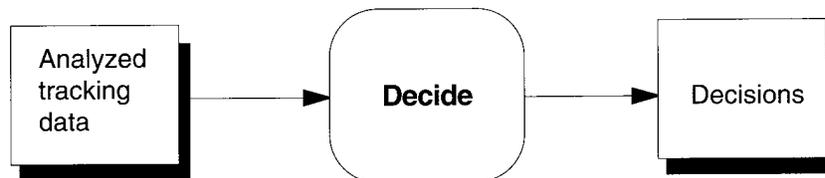
Decision Descriptions   The following table describes the decisions that can be made, lists the consequences of those decisions, and gives supporting examples.

Decision	Description	Example
Replan	A new or modified plan is required when • the threshold value has been exceeded • analysis of the indicators shows that the action plan is not working • an unexpected adverse trend is discovered	Despite efforts to get development personnel trained on the new compiler, the project is 35% short on trained personnel three months into the coding phase. The project manager asks for revisions to the mitigation plan to avoid a schedule slip.

Decision	Description	Example
Close a risk	A closed risk is one that no longer exists or is no longer cost-effective to track as a risk. This occurs when • the probability has been reduced below a defined threshold • the impact has been reduced below a defined threshold • the risk has become a problem and is now tracked as such *Note*: Closure of a risk requires the agreement of all affected parties.	Three months into coding, 100% of the development personnel are trained on the new compiler. There are no plans to bring new personnel on the project as new hires or transfers, and there are no other expected changes in personnel. Management feels that morale is good enough to allow this risk to be closed.
Invoke a contingency plan	A contingency plan is invoked when a trigger has been exceeded or when some other related action needs to be taken. The risk and its mitigation plan continue to be tracked after the contingency plan has been executed.	A contingency training plan was developed to bring short, intense (and expensive) compiler training on site if needed. With a 35% shortfall in trained personnel three months into coding, the decision is made to conduct the special training in-house.
Continue tracking and executing the current plan	No action is taken when the analysis of the tracking data indicates that all is going as expected and when project personnel decide to continue tracking the risk or mitigation plan as before.	Three months into coding, 95% of the necessary development personnel are trained. However, the plan calls for an additional 27 developers to be hired or transferred in the next two months. The new developers are largely untrained in the new compiler, and the decision is made to continue with the mitigation efforts and to track the risk.

Decision Example

The following graph is an example of a **Time Graph** [Chapter A-36] from a **Mitigation Status Report** [Chapter A-16]. The following decisions can be made at points A, B, and C:

Point A: The risk exposure has been reduced as expected after Action 1. Project personnel will continue tracking the risk.

Point B: Either the risk exposure has not been reduced after Action 2 or the action did not occur as scheduled. There may be a need to replan or to invoke a contingency plan if one is available. Project personnel must ultimately rely upon their experience and knowledge when making decisions.

Point C: The risk exposure has been reduced below a predefined threshold after Event 5. The risk can be closed.
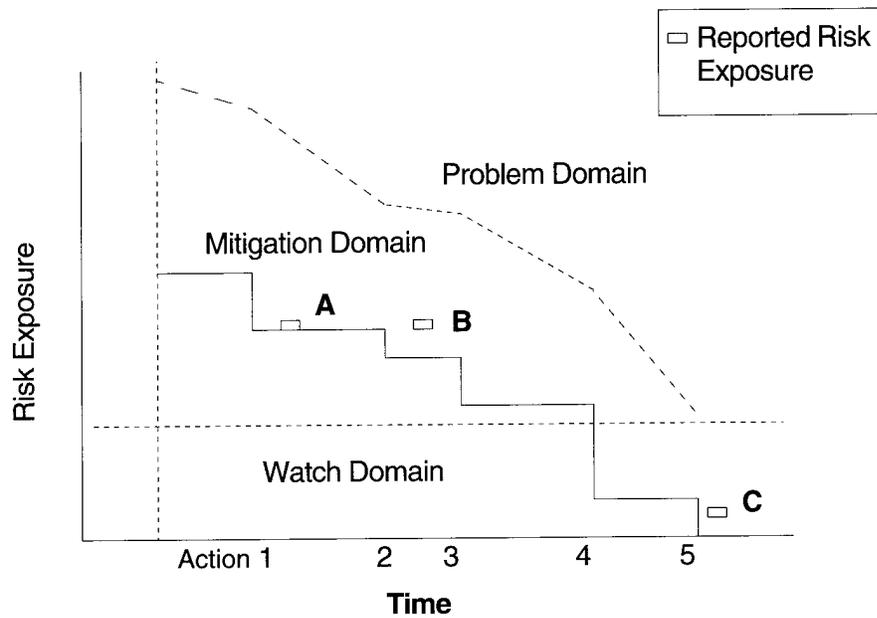
**Control:
Decide
Methods and
Tools**

The following table summarizes the methods and tools that can be used to make control decisions. Detailed descriptions of the methods and tools are provided in the appendix.

Method or Tool	Description
Closing a Risk [Chapter A-9]	Closed risks need to be documented, lessons learned incorporated, and appropriate personnel notified.
List Reduction [Chapter A-15]	This is used to reduce the number of options to an optimal few.
Multivoting [Chapter A-17]	This voting technique is used to choose a solution from a number of alternatives.

Section 4

Execute

Description
The Execute activity is the process where control decisions are implemented. If the decision is to take a planned action, then either the action is executed or the contingency plan is implemented, and the risk and its associated mitigation plan continue to be tracked. All closed risks should be documented along with the rationale for closure. However, when a decision is made to continue tracking a risk, it generally does not require documentation. Making changes to plans requires a return to the **Plan** function, while taking predefined contingency actions and continuing to track risks requires a return to the **Track** function.

Objective
The objective of the Execute activity is to implement both the decision made about a risk and mitigation plan as well as to ensure that all decisions are appropriately documented for future reference and historical record maintenance.

Diagram
The following diagram shows the inputs and outputs for executing decisions.
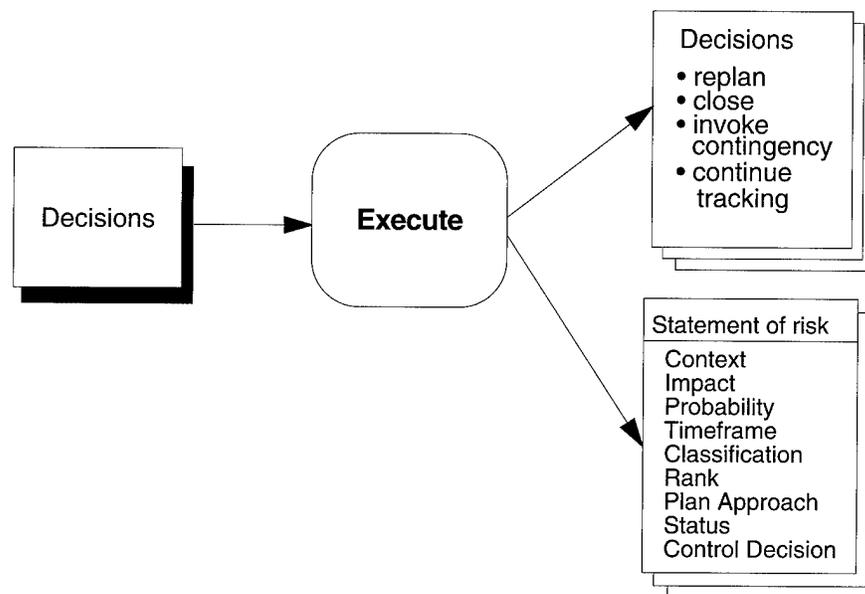
Considerations for Closing Risks
Several considerations need to be made when closing risks:
- The person responsible for the risk is the one who closes the risk.
- Personnel who either received status information or originated the risk should be notified.
- Proper approval for closing a risk (e.g., signature from responsible project member, team leader, project manager, etc.) must be obtained before it can be closed.
- If the risk being closed is a part of a set of risks, an informed decision should be made either to close the set or to close selected risks within the set.

Types of Lessons Learned

The lessons learned from watching or mitigating a risk or set of risks and the rationale for closing it should be captured upon closure. This information may be relevant to the present project or to other projects within the organization.

The following list contains examples of the types of lessons learned that should be retained:

- failed mitigation plans and the reasons for their failure. Keeping this information can prevent costly repetitions of mistakes in other projects.
- risk relationships and dependencies that were not obvious. This list will include risks which were not identified early in the process, but which surfaced later.
- successful mitigation plans and why they were successful. Keeping this information can make successful mitigation strategies available to other projects within an organization.
- relevant analysis data, especially the cost and benefits of the mitigation plan

Reopening Closed Risks

If a closed risk resurfaces at a future time, there should be a process in place indicating how to handle the situation. Either the old risk should be reopened or a new risk that references the old one should be opened. Important information and trends can be lost if the linkages are not maintained.

Control: Execute Methods and Tools

The following table summarizes the methods and tools used to document decisions which have been executed. Detailed descriptions of the methods and tools are provided in the appendix.

Method or Tool	Description
Closing a Risk [Chapter A-9]	Closed risks need to be documented, lessons learned incorporated, and appropriate personnel notified.
Mitigation Status Report [Chapter A-16]	Documentation of the contingency actions taken is added to in the status report (this may require redrawing the time graph).
Risk Information Sheet [Chapter A-27]	The risk information sheet is updated to reflect the implementation of a contingency plan.
Spreadsheet Risk Tracking [Chapter A-30]	Documentation of the action being executed and other relevant information such as the scheduled completion date is added to the spreadsheet.
Stoplight Chart [Chapter A-31]	Documentation of the action being executed, its current state of success, and other relevant information such as the scheduled completion date is added to the chart.

Section 5

Guidelines and Tips

Guidelines and Tips for Control

Make informed decisions based on explicit measures of success, defined during risk planning, for risk mitigation plans.

Make the conclusion of the mitigation activity and its associated risk an explicit activity.

Document the lessons learned and the rationale for closing a risk.

References

For more information on controlling risks and the methods and tools required, see the following:

[Arrow 88]   Arrow, Kenneth J. "Behavior Under Uncertainty and its Implications for Policy," 497-507. *Decision Making: Descriptive, Normative, and Prescriptive Interactions.* Cambridge: Cambridge University Press, 1988.

[Boehm 89]   Boehm, Barry. *IEEE Tutorial on Software Risk Management.* New York: IEEE Computer Society Press, 1989.

[Clark 95]   Clark, Bill. "Technical Performance Measurement in the Risk Management of Systems," Presented at the Fourth SEI Conference on Software Risk, Monterey, Ca., November 6-8, 1995. For information about how to obtain copies of this presentation, contact SEI customer relations at (412) 268-5800 or customer-relations@sei.cmu.edu.

[Rosenau 92]   Rosenau, Milton D. *Successful Project Management: A Step-by Step Approach With Practical Examples.* New York: Van Nostrand Reinhold, 1992.

[Scholtes 88]   Scholtes, Peter R. *The Team Handbook: How to Use Teams to Improve Quality.* Madison, Wi.: Joiner Associates, Inc., 1988.

[Xerox 92]   Xerox Corporation and Carnegie Mellon University. *The University Challenge: Problem-Solving Process User Manual.* Stamford, Ct.: Xerox Corporation, 1992.

Chapter 9

Communicate
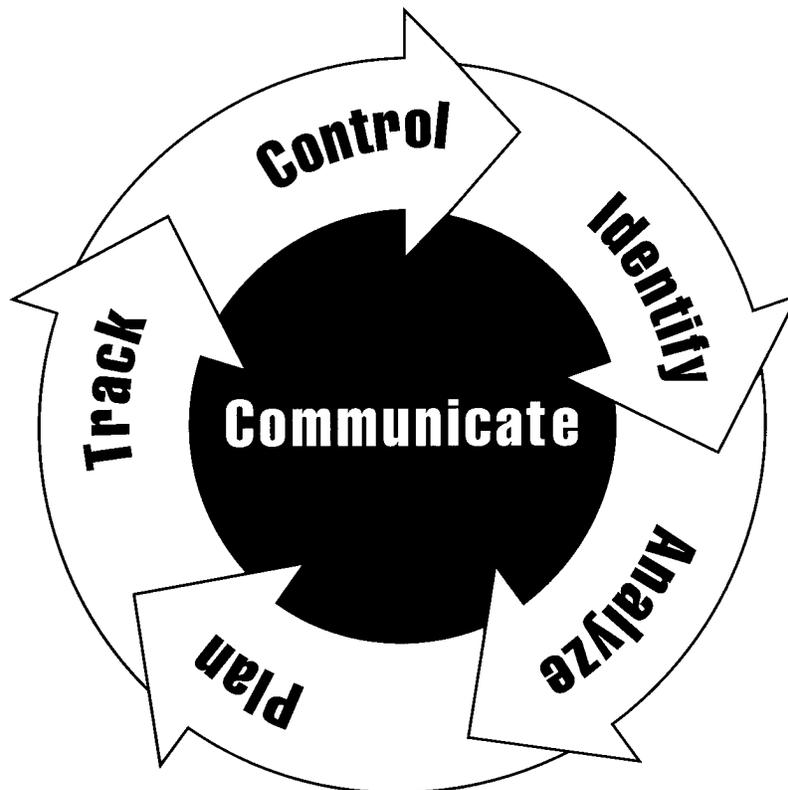
Section

Section 1

What is Communication?

Description   Communication of risk information is often difficult because the concept of risk deals with two subjects that people don't normally communicate well: probability and negative consequences. Communication is present in all of the other functions of the SEI risk management paradigm and is essential for the management of risks within an organization. It must both fit within an organization's culture as well as expose the risks which are present in an organization's projects.

Example: The interview activity used in the **Identify** function communicates risk information by determining what the project's risks are and then documenting the risk statements and their contexts.

Objectives   The objectives of communication are for project personnel to
- understand the project's risks and mitigation alternatives
- understand the risk data and make informed choices within the constraints of the project
- eliminate the barriers to effective communication.

Diagram   The following diagram exemplifies communication.
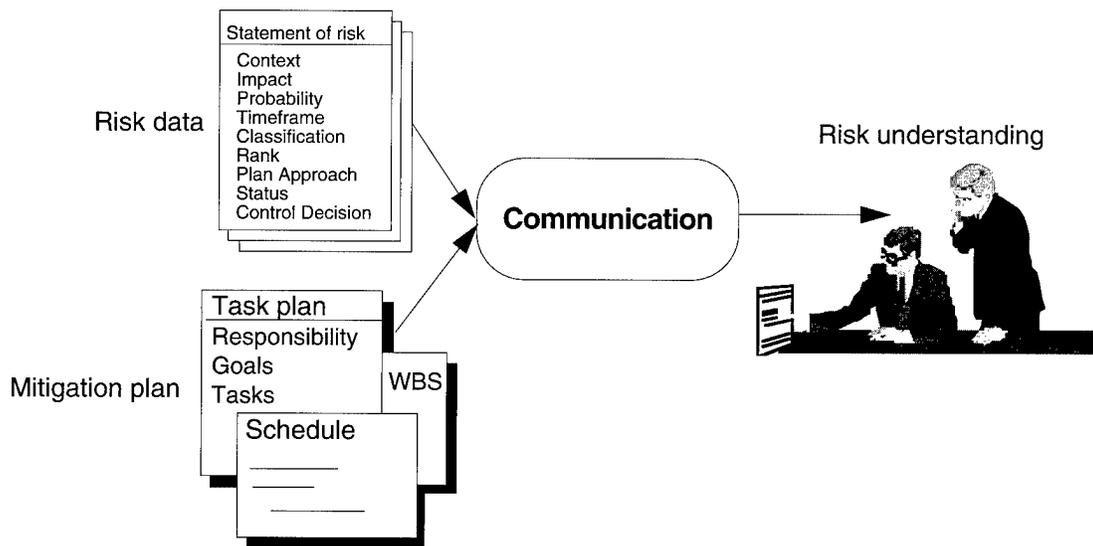
Types of Communication   There are several ways in which risk information can be shared between personnel on a project, including both formal and informal methods of communication. The categories of risk communication include: general, management, team, and external. They are defined in the following table.

Types of Communication	Description
General	General communication applies to both internal and external risk communication. It includes peer-to-peer, intra-group, and internal organizational communication. *Example*: Two software engineers informally discuss the interface between their software modules. They are interested in understanding the impact of their module designs on the interface and in identifying any risks that may be present.
Management	Management communication is for internal project communication among all levels of the project staff. *Example*: An individual reports risks to his/her supervisor.
Team	Team communication covers communication within small teams. They can be internal project teams, improvement teams, or integrated product teams. *Example*: An integrated product team is assigned the responsibility to design and develop a communication satellite operating system. The team members agree to include a discussion of the project's top N risks at their weekly team meetings.
External	External communication deals with the formal and informal communication between the project and its external customer(s), supplier(s), and senior organization manager(s). *Example*: In Continuous Risk Management, project personnel communicate risk information with a supplier who will be part of the risk mitigation strategy and with the customer who needs to be aware of how the most important risks are being mitigated.
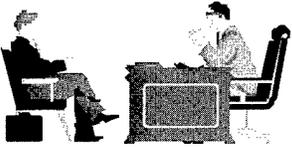
Section 2

Characteristics of Communication

Introduction

The core principle of the seven principles of Continuous Risk Management is open communication. Risk management communication requires

- a free flow of information within and between all project levels
- formal, informal, and impromptu communication
- non-attribution and trusted use of data
- processes that value the individual voice
- consensus-based processes for teams

The power of effective communication can most readily be seen when multiple viewpoints come together to form a common understanding.

Note: The formation of a common understanding does not necessarily require agreement among all parties. People can still disagree on issues, but they can also understand other points of view with respect to those issues.

Successful Communication

Successful risk communication raises the level of understanding of relevant issues or actions on a project. As a result, project personnel feel that they are adequately informed about project issues [NRC 89].

Risk Communication Characteristics

When good communication is encouraged within an organization, it provides a solid foundation for the communication of risks within the organization's projects. For risk communication to be considered "good," it must [Covello 93]

- be balanced and honest
- focus on specific issues
- focus on what the audience (e.g., the customer, the project manager, etc.) already knows
- be tailored to the specific needs of the audience
- place risks in their appropriate contexts
- contain enough specific information to describe and potentially resolve the problems facing the members of the audience
- be hierarchically organized so that people who only want a summary can find it quickly and people who want details can find them as well
- be respectful in tone and recognize that people have legitimate feelings and thoughts
- be forthright about any limitations (e.g., data limitations)
- deal with issues of trust and reliability (e.g., data reliability)

Section 3

Enablers to Communication

Introduction
Management plays a significant role in creating and sustaining an environment and culture that enhances communication, particularly risk communication.

Enablers
Each of the following environmental and cultural aspects helps to enhance risk communication in an organization.

Enabler	Description
Defining clear project roles and responsibilities	The organizational structure is clarified by defining the positions, roles, and responsibilities within the organization. Defined roles help to identify sources of information within an organization and to create a process for dealing with risks.
Making risk actions and decisions visible	Current risk status information is made available to the entire project team in an easily-understood format. This sustains the motivation of project personnel to be proactive and helps to institutionalize the practice of risk management.
Being a role model	Risk actions and decisions are communicated to project personnel. Project leaders must set an example for the project team.
Establishing an internal champion	An advocate of the risk management practice is identified. An internal champion is needed to provide the continual day-to-day encouragement to the project, to lead the drive for improvement, and to sustain the motivation for risk management.
Rewarding positive behavior	People who communicate risk information are rewarded. When behavior is rewarded, it tends to be reinforced and sustained in the future. *Example*: People should be rewarded when they identify risks, because they will have an incentive to identify more risks in the future.

Section 4

Barriers to Communication

Introduction

While management plays a significant role in creating and sustaining an environment that enhances communication, it also plays a significant role in removing barriers to risk communication.

Barriers

Barriers to risk communication along with suggested remedies are described in the following table.

Barrier	Description	Remedy
Ready-fire-aim	People provide solutions to a problem before they have assembled and understood the underlying facts and context of the problem.	Project personnel must first try to understand the issues before they draw conclusions. They need to separate fact finding from the process of generating solutions. Conducting an investigation and applying the results to potential solutions can be an iterative process.
Don't tell me your problem	People often require a solution before they even discuss an issue. *Example*: A manager says, "Don't bring me problems, bring me solutions."	Management must create an environment where issues can be raised and addressed openly. Managers need to clarify roles and responsibilities within their organizations.
Shoot the messenger	A project member who intends to inform others or who is seeking help can suffer negative consequences because he/she is communicating unpleasant information. *Example*: An individual takes an issue to the project manager and is told to bring back more information (the same information the individual was seeking).	Management must create an environment where issues, problems, and risks are discussed without assigning blame. However, actions that do not blame an individual (e.g., a request for more information) can also be a source of punishment under some circumstances.

Barrier	Description	Remedy
Liar's poker	Project personnel identify risks, but fail to communicate them to others. Instead, they wait until the risks become serious problems which impact project schedules and product quality. *Example*: Rather than communicating bad news to a manager about a potential problem, a team member waits for the problem to occur and for someone else to fail.	Management must create an environment of trust where failures are tolerated, but not repeated (lessons are then learned).
Mistrust	Individuals do not trust each other for a variety of reasons (e.g., past history, preconceived biases, personal biases, political factors, etc.). This lack of trust can reduce or destroy any credibility in the acquired risk data, which by its nature is subjective and speculative.	Management must encourage team building. Team members must develop good histories of communicating facts. This will then establish credibility and trust among the staff.
Value differences	Individuals have their own personal value systems. They measure and compare messages and information based on their individual values.	Management must identify individual values and differences. Managers must develop project values using consensus-based processes.
Hidden agendas	Situations create individual preferences for results. Individuals or groups may promote facts or arguments based on their goals rather than for the common good. *Example*: A manager may be influenced to defer a decision, asking for additional funds to resolve a problem because his/her merit increase would be affected.	Management must identify relevant interests and preferences among project personnel. Managers must build a culture where alternatives are explored, and they must also ensure that the reward system is consistent with desired outcomes.

Barrier	Description	Remedy
Differential knowledge	Each individual has a differing understanding of an issue.	Management must create cultural values that encourage individuals to share knowledge and to conduct analyses as appropriate. This will help to develop a common understanding of project issues among team members.
Placing blame	Risk information is abused because it is used to place blame on project personnel.	Management must support open communication and not use the resulting information for retribution.
Inactive listening	The audience is distracted and not listening. Effective communication requires that the audience be focused and not distracted.	Management must pay attention to both verbal and non-verbal feedback. Another key to good communication is to understand the issues which are being communicated and to test that understanding with the communicator(s). By doing this, managers can act as role models for good communication. They can also stimulate active listening by asking good questions and by giving good examples.

Section 5

Guidelines and Tips

General

Successful risk communication does not necessarily result in agreement about controversial issues or in uniform personal behavior. It is a mistake to expect that improved risk communication will reduce conflict between people and make risk management a simple exercise [NRC 89].

Risk management decisions will benefit some people in an organization, but not likely everyone. Common understanding does not necessarily lead to consensus. When evaluating choices, consider the net benefit to the project but recognize that personal values will affect the decisions which are made.

Most people have difficulty thinking in terms of probability, especially low probabilities. Establish a common reference which will enable project personnel to understand a risk as well as its associated risk exposure.

People are often tempted to quickly solve a problem without trying to identify the root causes. Risk communication must help project personnel to look at root causes and to identify potential deficiencies in the existing data.

Risks are typically identified by staff members at a lower level in an organization than is required for the management of those risks. Thus, effective communication is vital to coordinate the identification of a risk with its subsequent management.

Management

Internal communication is necessary to provide an efficient transfer of information between all levels of an organization. Details must be abstracted and filtered appropriately for each level of management.

The following list contains tips for communicating risks to managers:[1]
- Give the big picture first.
- Answer key questions.
- Provide a qualitative description, not just a number.
- Use real-life stories and powerful analogies.
- Tell not only what you know, but also what you suspect.
- Spare the minute details.
- Point out where data are weak.
- Give a sense of the uncertainty.
- Identify the positions of the stakeholders.

Team

Effective teams have good interactive skills and frequently work together to solve problems. Good discussion skills are essential for successful team meetings, and meetings are an important part of teamwork. The following table which provides guidance for team interactions is taken from *The Team Handbook* [Scholtes 88, p. 4-6 and 4-7].

---

1. *Communicating Risk to Risk Managers*, December 1992, Society for Risk Analysis Annual Meeting. For information about obtaining copies of this paper, contact the Society for Risk Analysis at (703) 790-1745 or sraburkmgt@aol.com.

Skill	Description
Ask for clarification	If you are unclear about the topic being discussed or the logic in another person's arguments, ask someone to define the purpose, focus, or limits of the discussion. Ask members to repeat ideas in different ways. Ask for examples, pictures, diagrams, data, etc.
Act as gatekeepers	Encourage more-or-less equal participation among group members by "throttling" dominators. Make openings for less aggressive members by directly asking their opinions or making a general request for input.
Listen	Actively explore one another's ideas rather than debating or defending each idea that comes up.
Summarize	Occasionally compile what's been said and restate it to the group in summary form. Follow a summary with a question to check for agreement.
Contain digression	Do not permit overly long examples or irrelevant discussions.
Manage time	If portions of the agenda take longer than expected, remind the team of deadlines and time allotments so work can be either accelerated or postponed, or time rebudgeted appropriately.
End the discussion	Learn to tell when there is nothing to be gained from further discussion. Help the team close a discussion and decide the issue.
Test for consensus	Summarize the group's position on an issue, state the decision that seems to have been made, and check whether the team agrees with the summary.
Constantly evaluate the meeting process	Throughout the meeting assess the quality of the discussion. Ask: "Are we getting what we want from this discussion? If not, what can we do differently in the remaining time?"

External

Credibility and trust take a long time to develop, but they can be eliminated in a single instant. It is important to develop trust and credibility and, once they are established, to work hard to protect them.

Base all discussions on facts, and identify any subjectivity that exists.

Establish a regular forum for risk communication. Any existing communication vehicles (e.g., weekly teleconferences) can be used as a means for communicating risks, actions, and status information.

As a supplier, know each customer's needs, wants, and desires.

As a customer, know each supplier's capabilities.

All of the previous guidelines for general, team, and management communications also apply to all external communications.

Example: When a customer becomes a part of its supplier's integrated product team, the communication guidelines for teams, which are listed above, apply to this situation.

References

Cited in this chapter:

[Covello 93]   Covello, V.T.; Fischhoff, B.; Kasperson, R. E.; & Morgan, M. G. "Comments on the 'Mental Model' Meets the Planning Process." *Risk Analysis 13*, 5 (October 1993): 493-494.

[NRC 89]   Committee on Risk Perception and Communication, Commission on Behavioral and Social Sciences Education, National Research Council. *Improving Risk Communication.* Washington, D.C.: National Academy Press, 1989.

[Scholtes 88]   Scholtes, Peter R. *The Team Handbook.* Madison Wi.: Joiner Associates Inc., 1988.

Chapter 10

Summary
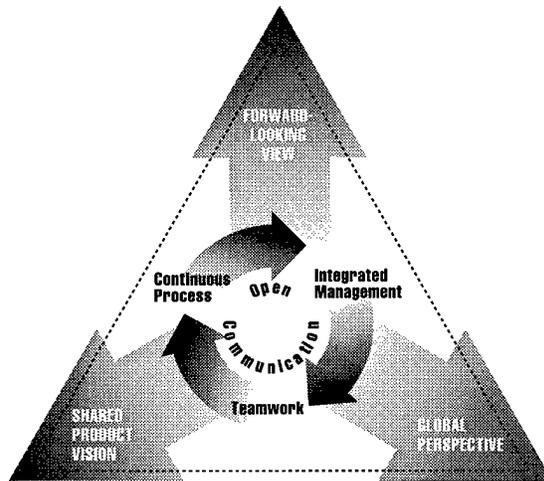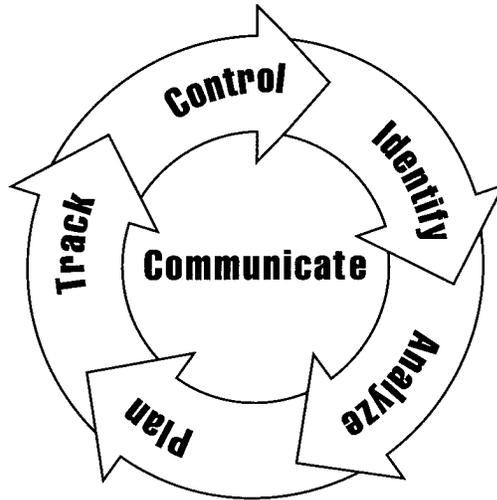
Section

Section 1

Continuous Risk Management Functions

**Continuous
Risk
Management**

Continuous Risk Management is a software engineering practice with processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making to

- assess continuously what could go wrong (risks)
- determine which risks are important to deal with
- implement strategies to deal with those risks

**SEI Risk
Management
Paradigm**

The SEI risk management paradigm is shown below. Each function in the paradigm has a set of activities backed by processes, methods, and tools that encourage and enhance communication and teamwork.
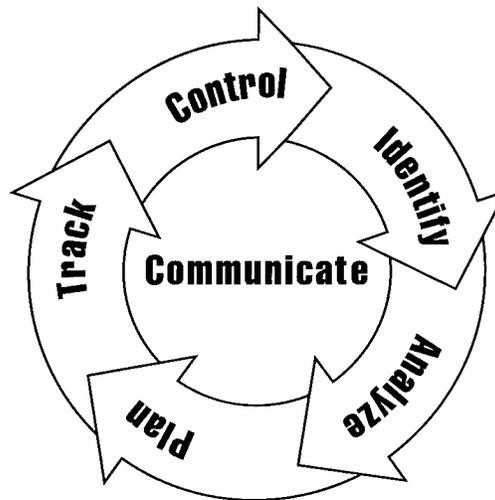
**Continuous
Risk
Management
Functions**

The table below summarizes the Continuous Risk Management functions. Communication is an integral part of all these activities. However, explicit, formal activities provide excellent communication opportunities.

Function	Description
Identify	Search for and locate risks before they become problems. Capture statements of risk and context. *Example methods and tools*: taxonomy-based questionnaire (TBQ), TBQ interviews, short TBQ, voluntary reporting, periodic risk reporting

Function	Description
Analyze	Transform risk data into decision-making information. Risk analysis is performed to determine what is important to the project and to set priorities. Evaluate impact, probability, and timeframe, classify risks, and prioritize risks. *Example methods and tools*: tri-level attribute evaluation, taxonomy classification, multivoting, comparison risk ranking
Plan	Translate risk information into decisions and mitigating actions (both present and future) and implement those actions. Produce mitigation plans for mitigating individual or groups of risks. *Example methods and tools*: goal-question-measure, action item list, problem-solving planning, cause and effect analysis, brainstorming
Track	Monitor risk indicators and mitigation plans. Indicators and trends provide information to activate plans and contingencies. These are also reviewed periodically to measure progress and identify new risks. Acquire, compile, and report data on the risk and mitigation plan. *Example methods and tools*: spreadsheet risk tracking, mitigation status reports, stoplight charts
Control	Correct for deviations from the risk mitigation plans. Actions can lead to corrections in products or processes. Changes to risks, risks that become problems, or faulty plans require adjustments in plans or actions. Analyze tracking data, decide on how to proceed, and execute decision. *Example methods and tools*: PERT charts, cost-benefit analysis, closing a risk
Communicate	Provide information and feedback internal and external to the project on the risk activities, current risks, and emerging risks. Communication occurs formally as well as informally. Communication is a key function in the Continuous Risk Management model that links to all the other functions. Therefore, each method identified previously is a vehicle for communication of risk.
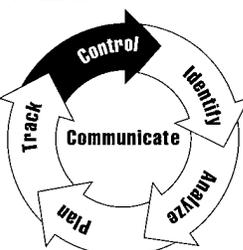
Data Flow

The diagram on the following page illustrates the data flow from one function in the paradigm to the next. It follows the data that is input to the **Identify** function through the output from the Control function.
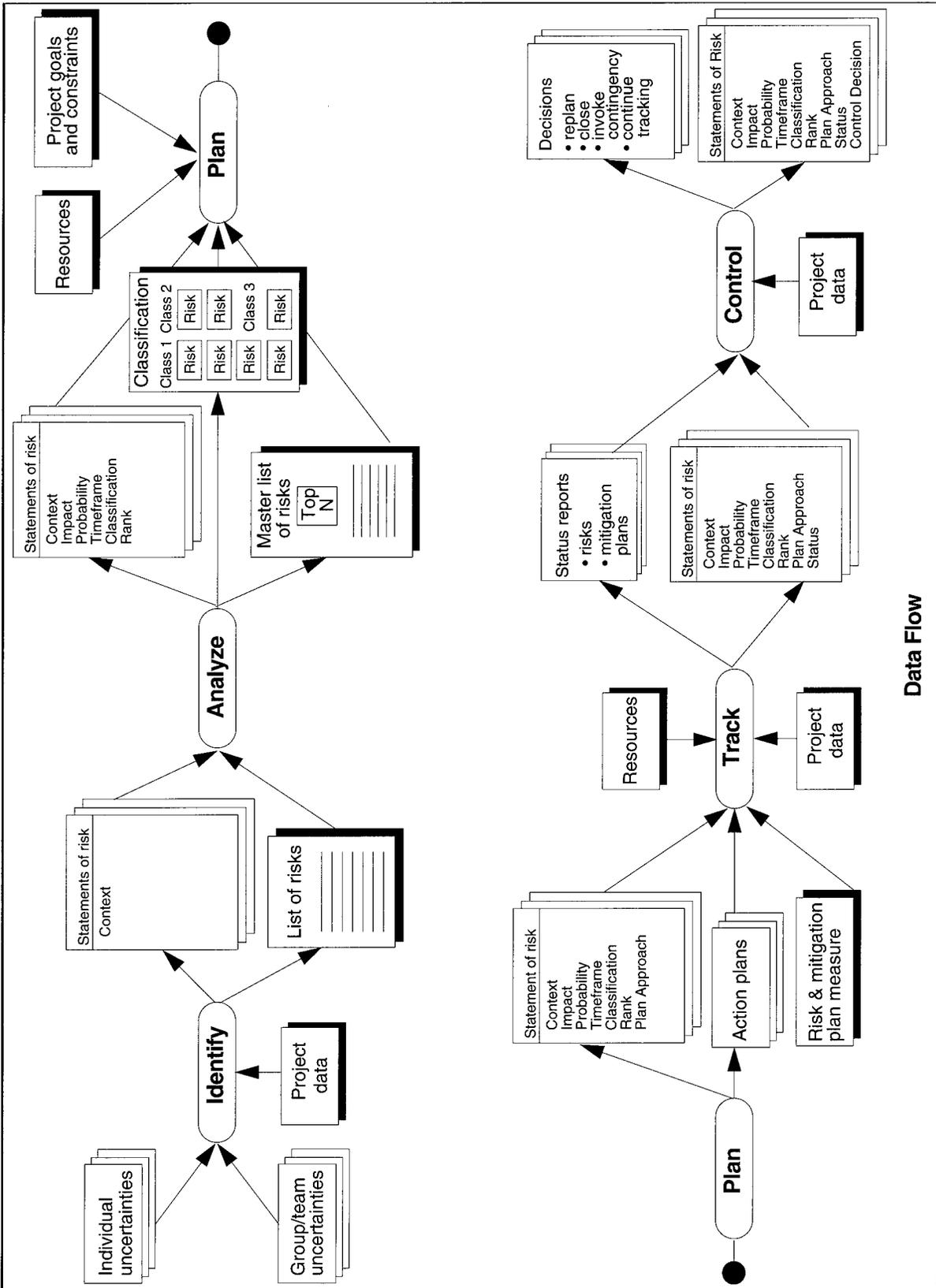
Data Flow

Section 2

Guidelines and Tips

Summary of Guidelines and Tips

The SEI risk management paradigm sets forth processes for managing risks within a project. Below is a summary of the guidelines to consider when implementing the risk management paradigm.

Identify

Develop a common understanding of the risk by sharing several points of view.

Provide an opportunity for individual contributions.

Ensure that the common view does not eliminate individual views.

State risks in objective terms which are understood by project personnel.

State risks in a way such that they can be addressed.

Analyze

Allocate scarce resources to the important issues rather than letting due dates drive resource allocation.

Address the urgent risks (e.g., near timeframe) or risks having the potential for extremely significant impact first.

Combine items that have similar origins or that are duplicates.

Reword risk statements to make them clear to all project members.

Eliminate risks that are already being addressed.

Plan

Identify specific, implementable actions which will preempt problems.

Create the desired future state; things will not get better on their own.

Integrate risk mitigation plans with project plans when those plans affect project schedules, budgets, and deliverables.

Communicate mitigation plans to all affected personnel within the project, organization, customers, subcontractors, etc.

Do not lose sight of the end product when developing mitigation plans—don't unknowingly compromise the end product while trying to fix the smaller details.

Track

Make information openly available to all project personnel.

Present data in a clear and concise manner for the intended audience.

Choose indicators that give insight into the important project risks by being predictive in nature.

Choose trigger values that give project personnel enough time to react to current conditions and to take appropriate actions in a timely manner.

Control

Make informed decisions based on explicit measures of success, defined during risk planning, for risk mitigation plans.

Make the conclusion of the mitigation activity and its associated risk an explicit activity.

Document the lessons learned and the rationale for closing a risk.

Communicate

Do not insist on agreement about controversial issues or uniform personal behavior. Successful risk management does not necessarily result in these.

Establish a common reference which will enable project personnel to understand a risk as well as its associated attributes.

Communicate effectively: effective communication is vital to coordinate the identification of a risk with its subsequent management.

Abstract and filter information appropriately for each level of management.

Make sure individuals have good discussion skills; these skills are essential for successful team meetings, and meetings are an important part of teamwork.

Remember that credibility and trust take a long time to develop, but they can be eliminated in a single instant.

Base all discussions on facts, and identify any subjectivity that exists.

Establish a regular forum for external risk communication.

Part 3

Continuous Risk Management: Example Implementation
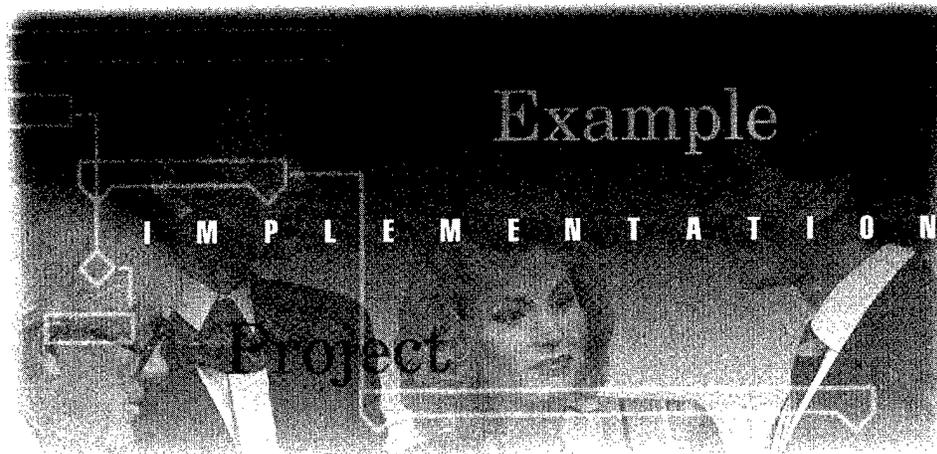
Introduction

Part 2 described the concepts, processes, methods, and tools for Continuous Risk Management. Part 3 provides an example of how Continuous Risk Management looks when implemented in a typical project—in other words, it shows how a selected subset of the methods and tools could be collectively used to manage risk on a continuous basis within a typical project. The example implementation is based on a composite of SEI work with several clients in industry and defense.

Chapter

Chapter 11

An Implemented Continuous Risk Management Practice

Example Project

Project Management

Control
Identify
Track
Communicate
Analyze
Plan

Section

Section 1

What Is an Example Implementation?

Description

An example implementation shows a view of how a Continuous Risk Management practice (processes, methods, and tools) would look when fully implemented in a project. It has the following components:

- the organizational structure of a typical project
- an internal communication framework which identifies the risk management activities associated with different project roles
- a high-level process and data flow
- a meeting structure where much of the coordination and communication occurs
- methods and tools used for the activities
- communication which is external to the project

Chapter 12 provides a scenario for the life-cycle of a risk in this project.

Overview

The components of an implementation of Continuous Risk Management are shown in the following diagram. The organization's structure combined with the risk management paradigm produces the internal communication framework, which then drives external communication. The organization's structure and the internal communication framework provide the basis for the process and data flow. The framework for the methods and tools is then provided by the defined process and data flow.
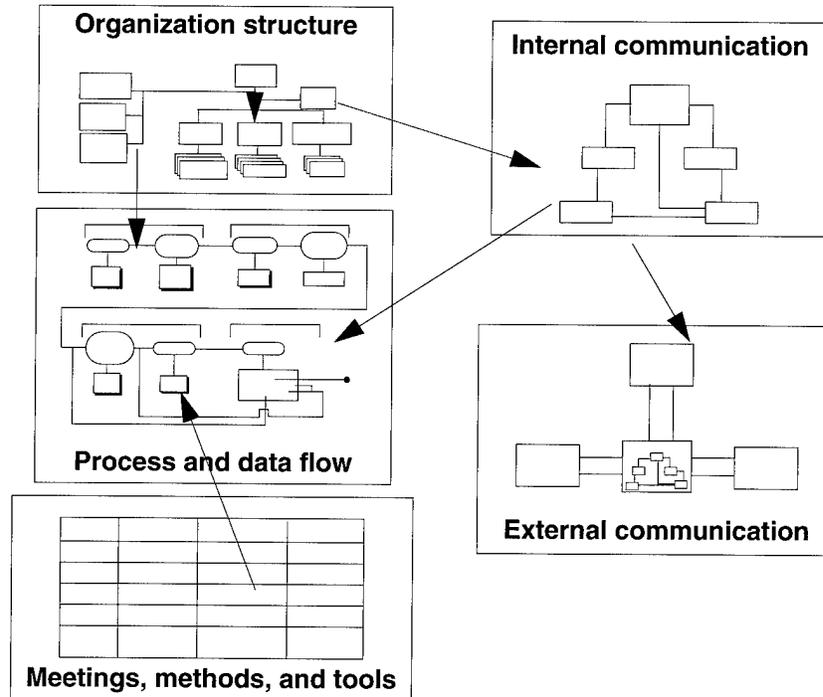
From Practice to Activities

The following diagram illustrates the relationships between a practice, as used in this guidebook, and the other terms used to describe its components in this part. There is an overall process for this implemented version of Continuous Risk Management, and there would be lower level processes for each function (e.g., the **Track** function). Each of the processes in the practice are made up of activities accomplished by project members, using the methods and tools. Each method has steps that are performed by project personnel.

```
                        ┌──────────────┐
                        │   Practice   │
                        └──────┬───────┘
            ┌──────────────────┼──────────────────┐
    ┌───────┴──────┐   ┌───────┴──────┐   ┌───────┴──────┐
    │  Processes   │   │   Methods    │   │    Tools     │
    └───────┬──────┘   └───────┬──────┘   └──────────────┘
    ┌───────┴──────┐   ┌───────┴──────┐
    │  Activities  │   │    Steps     │
    └──────────────┘   └──────────────┘
```
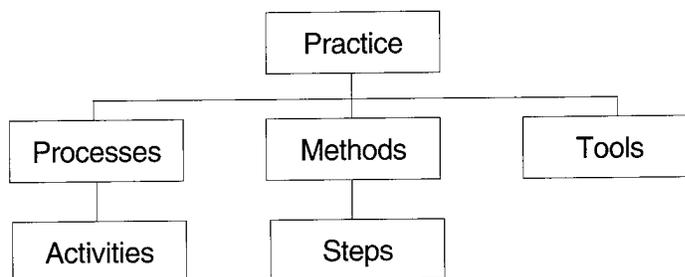
What Is its Basis?

The model described in this chapter is based on several years of experience with clients who have worked with the SEI to establish risk management in their projects and organizations. Their efforts, as well as their successes and failures, have provided much of the material in this guidebook and are the basis for the model.

Why Have One?

Part 2 of the guidebook describes the theoretical and conceptual framework for Continuous Risk Management. It also identifies a set of alternative methods and tools for Continuous Risk Management which are outlined in the appendix. The conceptual framework by itself could confuse practitioners because of the variety of choices which are presented. The example outlined in this chapter provides one perspective of how to implement Continuous Risk Management in a project.

How to Use This Example

The example implementation which is discussed in this chapter is not the answer nor the solution for all projects, but it does provide a basis for differentiation. It forms the foundation for a target, goal, or end point for any project attempting to implement a risk management practice. Each project and each organization must determine the specific implementation that will work best for them (see Part 4).

The example can also be used to help clarify the concepts, principles, and functions of Continuous Risk Management as described in Part 2.

Section 2

Organization Structure, Internal Communication, and Project Operations

Description

In any organization, activities and communication occur within a defined structure or framework. Likewise, risk management activities and communication about risks must also be performed within this framework.

Organization Structure

The following diagram shows a typical hierarchical organization for a project.
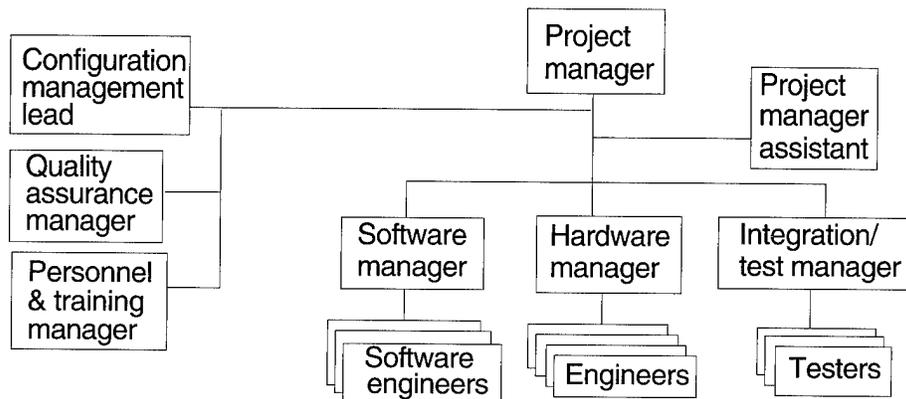
Risk Management Plan

The plan outlining how a project performs Continuous Risk Management is documented in a **Risk Management Plan** [Chapter A-28], which is part of the overall project management documentation. The plan specifies

- the processes, methods, and tools to be used
- the roles and responsibilities of project personnel
- the deliverables and risk information retention requirements
- the assumptions and constraints
- the budget, schedule, and resource requirements

Note: The risk management plan is maintained and controlled by the same configuration management and quality assurance processes that maintain and control other project management plans.

Internal Communication

In this project, the risk management processes are implemented through specific activities and responsibilities at each level of the project organization. Risk-related activities and communication paths are defined to enable the free flow of risk information. The following diagram depicts the internal communication framework for a hierarchical organization. The responsibilities and activities are further elaborated in succeeding paragraphs.
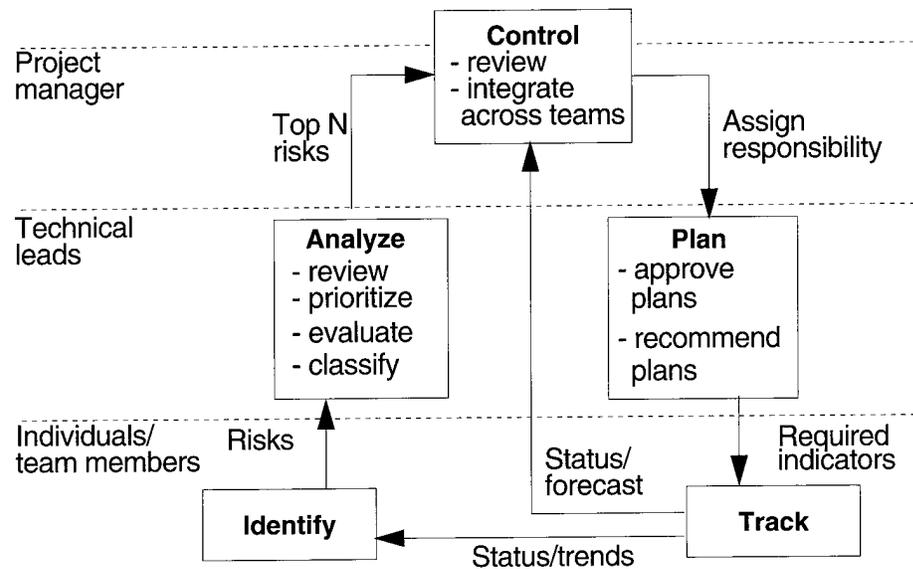
At the Individual Level

Individuals (e.g., software engineers, hardware engineers, testers, technical leads, and the project manager) in this project are responsible for these activities

- identifying new risks
- estimating the probability, impact, and timeframe of risks (evaluation)
- classifying risks
- researching and recommending mitigation plans
- tracking risks and the progress of mitigation plans

Example: Software engineers have identified fifteen new risks (including the estimations of probability, impact, and timeframe) to add to the thirty that they already have. They have also proposed mitigation strategies and actions for ten of the existing risks and expect that their software engineering team lead will review those plans for approval. Nineteen risks are still being watched, and the software engineers have collected and prepared status reports for these risks. At this point, one risk has already been accepted and closed.

At the Technical Lead Level

The technical leads (e.g., software manager or configuration management lead) in this project are responsible for these activities:

- ensuring that the probability/impact/timeframe estimates as well as the classification of the risks are accurate
- modifying and approving recommended mitigation plans
- prioritizing the risks which are managed within their team
- reporting their top N risks and issues to the project manager
- collecting and reporting general risk management measures (e.g., resources expended in mitigation, number of risks open and closed at key project milestones, etc.) which are acquired during each quarter

Example: The software engineering team has 45 risks. Twelve of the risks are prioritized into software engineering's top 12 risk list and are reported to the project manager. Twenty two risks are being watched, while eleven are accepted and closed.

**Project
Manager
Level**

The project manager is responsible for these activities:

- integrating risk information from all of the technical leads or teams
- reprioritizing all risks to determine the top N project risks
- controlling where major mitigation resources are spent
- assigning or changing the responsibility for risks and mitigation plans within the project
- handling communication that is external to the project (see Section 5)
- reviewing general risk management measures (e.g., resources expended in mitigation, number of risks open and closed at key project milestones, changes to the risk management plan, etc.) with the quality assurance representative during each quarter to evaluate the effectiveness of the risk management practice

Example: The hardware manager reports 11 important hardware risks as well as one risk which should be transferred to the software engineers. In addition, the software manager reports 12 risks, the quality assurance manager reports 4 risks, the configuration manager reports 2 risks, the personnel and training representative reports 5 risks, and the testing lead reports 6 risks. Thus, a total of 41 risks were reported to the project manager, which is more than the project can afford to mitigate at this time. The project manager and the technical leads then reprioritize the risks to identify the top 15 risks to the project. The risks on the top 15 list will be allocated mitigation resources. Also, the risk that the hardware team wanted to transfer to the software engineers is reassigned to and accepted by them.

Section 3

Process and Data Flow

Description

The SEI risk management paradigm provides a conceptual view of the Identify, Analyze, Plan, Track, Control, and Communicate functions. A defined process and data-oriented view provides an alternative view of the functions for this example implementation.

Top N vs. Non-Top N

Due to budget constraints, only the top N risks to the project will be mitigated, and the number of risks that are on the top N list will vary over time.

Reviewing Risks

The top N risks are either mitigated or watched and are reviewed weekly. Risks that are on the non-top N list are reviewed once a month for progress or significant changes. New risks are added to the top N list when they have a high probability, a high impact, and a near-term timeframe; otherwise, they are added to the non-top N list. New and watched risks may move between the top N and non-top N lists when all of the risks are re-prioritized or when significant changes occur which warrant review. Researched risks are treated as watched risks until the research is completed, and transferred risks are reviewed once a month to determine what progress is being made by the transferee.

The following diagram illustrates the constraints on the management of risks for this project.

Mitigated
Watched
New

Top N risks

Watched
Transferred
New
Accepted
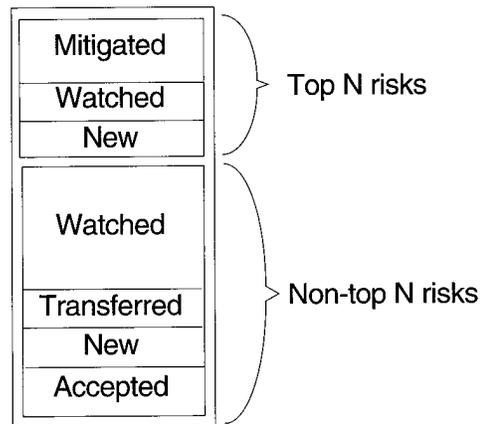
Non-top N risks

Process and Data Flow

The diagram on the following page is a combined high-level process and data flow.

Individual activities

Identify risks

Risk
statement
& context

Analyze:
Classify risks
Evaluate risks

Risk class,
probability,
impact, &
timeframe

Weekly and monthly meetings

Analyze:
Prioritize risks

Prioritized
list of risks

Plan:
Assign
responsibility
Approve plans

Assignments,
approved plans

Individual activities

Plan:
Define mitigation
approach
Determine
mitigation plan

Risk
mitigation
plans

Track risks

Status
reports

Weekly and monthly meetings

Control risks

Decision
Close risk
Take planned action
Continue tracking
Replan

Legend:

Process
activity

Output
or data

Decision

Implemented Continuous Risk Management Process and Data Flow

Hierarchy of Top N Lists

For this project, only the top N risks are mitigated. However, there is a hierarchy of top N lists, which is illustrated by following diagram. Major resource commitments for mitigation can only be allocated to the project's top N risks. Discretionary or minor resource commitments for mitigation can be made by each team for risks which appear on its individual top N lists.
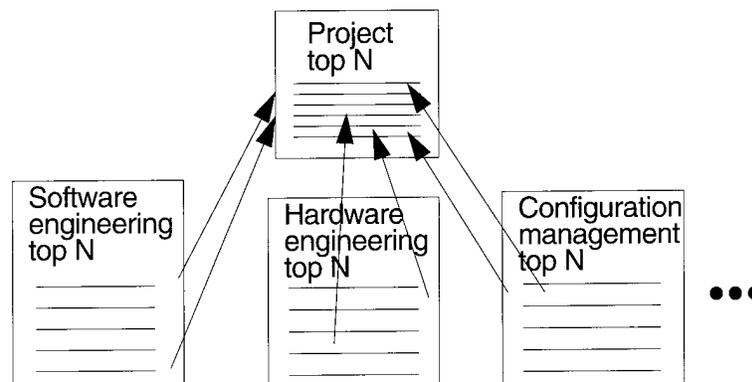
Activity Settings

Continuous Risk Management activities occur in three basic settings:

- individual activities performed on any given day by programmers, software engineers, hardware engineers, technical leads, managers, etc.
- weekly team meetings led by technical leads
- monthly project meetings led by the project manager and attended by the technical leads and other key representatives

Day to Day, Individual Activities

Individuals are responsible for identifying new risks, for classifying them, and for estimating the impact, probability, and timeframe for each new risk. Once an individual has been assigned responsibility for a risk, he or she will be required to decide if the risk needs to be researched, accepted, watched, or mitigated. If the risk needs to be mitigated, the individual determines the scope of the mitigation effort (i.e., action items or a task plan) and develops the mitigation plan. Individuals also track the risks that are assigned to them as well as produce status reports for the risks. When necessary, individuals can form small subteams to deal with their risks (e.g., when a complex risk requires team expertise to develop mitigation plans).

Weekly Team Meetings

At weekly team meetings, the technical lead establishes a priority of the team's risks (both new and existing) to determine which ones are most important and which ones must be reported to the project manager. Also, the technical lead either assigns responsibility for new risks to team members or transfers the risks to another team or to the project manager. Mitigation plans which are developed by team members are reviewed and approved by the technical lead during this meeting. If a mitigation plan is not approved, it is subsequently revised by a selected subteam. Status reports for risks and mitigation plans are presented at this meeting, and the team decides if the risks can be closed, if the mitigation plans need to be changed, if contingency actions are now required, or if risk tracking should continue. Decisions concerning risks that are currently being reported at monthly project reviews cannot be made at weekly team meetings. Control decisions for those risks must be approved at monthly project reviews.

Monthly Project Meetings

At monthly project meetings, the technical leads bring the top N risks from their teams to review and prioritize at the project level. The project manager and technical leads decide if the risks can be closed, if the mitigation plans need to be changed, if contingency actions are now required, or if risk tracking should continue. The project manager determines where to allocate significant project resources for mitigation; however, technical leads also have an "allowance" of discretionary mitigation resources. All mitigation plans that exceed the mitigation allowance for a team must be approved by the project manager. Successful mitigation efforts are recognized at the monthly project meeting, and informal rewards in the form of "honorable mentions" in monthly project status reports are also provided.

Note: Priority changes at the project level may affect priorities at the team level.

Risk Database

The project has chosen to expand its problem database to include risk data. As risks and problems are closed and solved, the lessons learned associated with risks and their mitigation plans as well as with problems and their solutions are added to the database. The project manager wants the organization to adopt the process of adding lessons learned for both problems and risks. Having a repository of risk and problem data would support the ability to do cross-project lesson learned analyses as well as general trend analyses (e.g., identify patterns, common mitigation strategies, etc.).

Section 4

Methods and Tools

Description

This section describes the methods and tools used to perform the Continuous Risk Management activities as well as the rationale for selecting them for this project.

Methods and Tools for Individuals or Subteams

The following table illustrates the methods and tools that can be used by individuals or subteams to complete the identification, analysis, planning, and tracking activities that are assigned to them. The tools listed in the table are database reports or data entry forms (or both).

Individual Risk Management Activities	Methods and Tools
Identify, classify, and evaluate new risks.	Risk information sheet Taxonomy classification Tri-level attribute evaluation
Plan assigned risks: determine approach and scope, develop mitigation plans, and identify indicators to track risks and plans.	Action item lists Planning worksheet
Track assigned risks and plans and develop status reports.	Spreadsheet risk tracking

Methods and Tools for Weekly Team Meetings

The following table describes the methods and tools used during (or to support) weekly team meetings. The methods and tools are used to review risks and their status reports, to prioritize risks, to assign responsibility, and to take controlling actions.

Weekly Team Meetings: Risk Management Activities	Methods and Tools
Meet to discuss progress and problems and to assign new tasks.	Risk information sheets Spreadsheet risk tracking
Prioritize risks within the team.	Multivoting
Assign responsibility (planning step): keep risks, delegate risks to another team member, or transfer risks out of the team.	Document decision on risk information sheet
Control risks: close risks, take planned actions (contingencies), continue tracking and executing the current plans, or replan if the current mitigation efforts are not succeeding	Closing a risk Document decision on risk information sheet
Select risks to report at the monthly project meetings.	Spreadsheet risk tracking

Methods and Tools for Monthly Project Meetings

The following table describes the methods and tools used during (or to support) monthly project meetings. The methods and tools are used to review risks and their status reports, to prioritize risks, to assign responsibility, and to take controlling actions.

Monthly Project Meeting: Risk Management Activities	Methods and Tools
Meet to evaluate the progress of all teams, to correct project plans, and to prioritize the use of project resources.	Spreadsheet risk tracking Stoplight chart
Prioritize risks within the project.	Cost-benefit analysis Multivoting
Assign responsibility (planning step): keep risks, delegate risks to another project member, or transfer risks out of the project.	Document decision on risk information sheet
Control risks: close risks, take planned actions (contingencies), continue tracking and executing the current plans, or replan if the current mitigation efforts are not succeeding.	Document decision on risk information sheet
Select risks to report externally.	Spreadsheet risk tracking for details Stoplight chart to summarize

Why These Methods and Tools?

The following table outlines the rationale used to select the set of methods and tools for the example project. A similar type of rationale for choosing methods and tools should exist for any project that is using Continuous Risk Management.

Method or Tool	Selection Rationale
Action Item List [Chapter A-1]	Action item lists are used to document the selected set of mitigation actions. If a risk or set of risks is so complex that a formal task plan is needed for mitigation, it will be added as a task to the project plan and tracked as a project task with a pointer to the risk.
Closing a Risk [Chapter A9]	Other managers would like their projects to learn from the experiences of this project. The lessons learned which are captured by this method are a key part of the learning experience.
Cost-Benefit Analysis [Chapter A-11]	A corporate tool already existed as an aid to developing cost-benefit analyses, and no tailoring was necessary to support the evaluation of mitigation costs and benefits. The project manager requires this type of analysis before major resources for mitigation are committed.

Method or Tool	Selection Rationale
Multivoting [Chapter A-17]	Multivoting is a standard voting method that was already used and taught as part of the project's quality improvement initiatives.
Planning Worksheet [Chapter A-22]	A planning worksheet is used to help planners consider all aspects of a risk that might influence its mitigation. It is also used as a checklist to document comprehensive strategies and actions and to document planning decisions.
Risk Information Sheet [Chapter A-27]	The project uses this tool as the primary documentation for an individual risk. The project wanted a one-page description of information for each risk to complement the summarized spreadsheet (e.g., as back-up documentation during meetings if detailed information on a particular risk is needed).
Spreadsheet Risk Tracking [Chapter A-30]	Risk tracking spreadsheets are used to summarize the current statuses and priorities of all of a team's or project's risks. It supports a quick, high-level review of risks during meetings.
Stoplight Chart [Chapter A-31]	The project manager was already required to use the simple red-yellow-green metaphor for reporting status for problems, schedules, and budgets. The extension to risk was intuitive.
Taxonomy Classification [Chapter A-34]	The software development risk taxonomy was chosen as the classification method for software engineering, quality assurance, configuration management, personnel, and testing risks. A tailored set of additional classes was added for hardware risks.
Tri-level Attribute Evaluation [Chapter A-38]	Binary evaluation did not provide a sufficient level of discrimination, so a tri-level evaluation was chosen.

Section 5

External Communication

Description

The project manager often communicates with people external to the project about status information, problems, schedules, budgets, as well as other relevant topics. Risk information is a part of the project manager's external communication because it keeps people who are external to the project informed and aware of potential problems. External communication is also used to elicit additional information that is needed to understand risks or to acquire additional resources or assistance when mitigating risks. The project manager believes that open communication about the project's risks will help to foster effective risk management and will decrease the likelihood of creating unpleasant surprises for customers, suppliers, and the site manager.

Communication Paths

There are three basic external paths for communicating risk information: senior managers, customers, and suppliers. The following diagram shows the relationships between the external parties and the project.
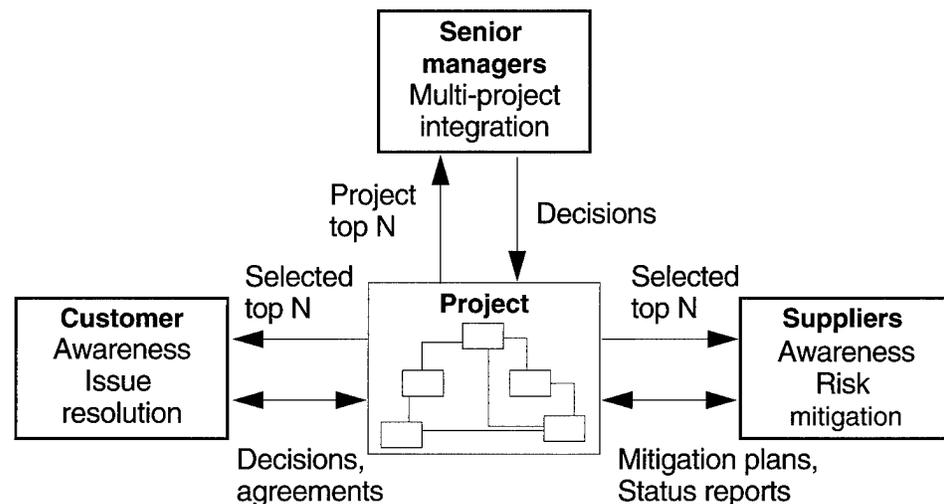
Senior Manager

The site manager is the senior manager in the company and gets quarterly status reports from all of the projects at the site. The site manager's goal is to understand the risks facing projects and to determine whether the risks are under control. If extensive resources are needed for mitigation or if serious problems are about to occur despite mitigation efforts, it is the responsibility of the site manager to decide how to proceed. Detailed status information, plans, and progress reports are normally not required, unless they are specifically requested. The site manager is primarily interested in issues which may significantly affect the quality, cost, or schedule of delivered products.

Site risks, those common to multiple projects, may also be identified at the quarterly meetings and may be assigned to project representatives or other staff members for resolution.

Customers

Selected risks are chosen from the project's top N list and discussed with the customer. The risks which are reviewed are those that may cause the customer to see a difference in the budget, schedule, or quality of the product. The objective is to inform the customer and to prevent any future surprises. The customer is kept aware of the most important risks and how they are being mitigated. If decisions or agreements are required to change the contract or project plan, then they are negotiated with the customer.

Note: Many risks, even if they become problems, can still be absorbed by the project without the customer seeing any impact. These are normally not reported to the customer.

Suppliers

There are several suppliers who are subcontractors for this project. Some of the risks that were identified by project personnel affect the suppliers, who need to be kept aware of progress. A few risks will even have to be mitigated or partially mitigated by the suppliers, so these risks need to be delegated or jointly managed. Selected risks (i.e., those that may impact a supplier's cost, schedule, or product quality) are shared with the appropriate supplier during routine meetings and through status reports. Suppliers provide mitigation plans and status reports on delegated risks when appropriate.

Meetings and Other "Events"

External risk management communication occurs during routine meetings and project events (e.g., system design review) between project personnel and senior managers, customers, or suppliers. Standard reports are another vehicle which enhance external communication. The following table shows the types of activities which might occur during typical meetings to address risks as well as the methods or tools which are used to support those activities.

Meetings	Description	Methods and Tools
Quarterly site manager's reviews	Quarterly site manager's reviews are multi-project meetings to apprise the site manager of progress and issues. Risk specific activities include • identifying or discussing new risks, especially site risks • reporting the status of each of the project's top N risks • getting decisions/resolutions for risks which are not being successfully controlled • approving mitigation plans and resources Output • an informed site manager • decisions about additional resources • assigned responsibility for site risks	(As needed) Cost-Benefit Analysis [Chapter A-11] Risk Information Sheet [Chapter A-27] Stoplight Charts [Chapter A-31] (which are used for top N risks in each project) are integrated into standard project status reports

Meetings	Description	Methods and Tools
Weekly teleconferences with customers and suppliers	Teleconferences with customers and suppliers are used to review current progress, issues, and problems. Risk-specific activities include • reviewing risk and mitigation plan status • identifying and discussing new risks Output • an informed customer and supplier • approved supplier mitigation plans • new risks which are assigned and prioritized	Risk Information Sheet [Chapter A-27] Spreadsheet Risk Tracking [Chapter A-30] is faxed or e-mailed prior to teleconference
Customer's project milestone reviews (e.g., system requirements review)	The customer's project milestone reviews are major meetings to review progress with respect to the project schedule. Risk specific activities include • reviewing progress on selected top N risks • identifying new risks Output • an informed customer • decisions or agreements concerning project plan changes	Risk Information Sheet [Chapter A-27] Stoplight Charts [Chapter A-31]
Supplier's project milestone reviews (e.g., system requirements review)	The supplier's project milestone reviews are major meetings to review progress with respect to the project schedule. Risk specific activities include • identifying new risks • reviewing status reports for selected top N risks • reviewing supplier mitigation plans Output • an informed supplier • approved supplier mitigation plans • decisions or agreements concerning project plan changes	Risk Information Sheet [Chapter A-27] Stoplight Charts [Chapter A-31]

Section 6

Continuous Risk Management Principles

Principles Implemented

The key to practicing effective Continuous Risk Management is to adhere to the principles when performing the paradigm functions. The project or organization needs to choose and adapt the methods and tools which meets its own requirements, needs, and standards. Personnel in a project or organization should also consider who uses the methods and tools as well as how risk data are collected and stored. All selections and adaptations must be made with the principles in mind. The following table summarizes how the example implementation which was discussed in this chapter demonstrates the principles of Continuous Risk Management.

Principle	Implementation
Open communication	During weekly and monthly project meetings, risk information is included as an agenda topic, encouraging open communication about risk within the project.
	Sponsorship by the project manager and the site manager as well as rewards for successful risk management encourage others to begin dealing with their risks and communicating about their progress.
	Adding risk information to external communication increases the openness with which issues can be discussed and successfully resolved with the site manager, customers, and suppliers.
Forward-looking view	As risk communication becomes a part of the project's culture and as risk management is openly rewarded and appreciated, project personnel will begin to look further into the future when thinking about and identifying new risks to the project.
	The integration of risk information with the problem database encourages project personnel to consider the long-range effects of problems and problem resolution. It has also provided a link between risks and problems which enables trend analyses to be performed on risks data.
Shared product vision	Project personnel can achieve a shared vision of the real goals, priorities, critical issues, and desired end state of the project by integrating risk management with the project meetings.
	Project personnel can achieve a shared vision of the real goals, priorities, critical issues, and desired end state of the project by including risk information when communicating with customers and suppliers.

Principle	Implementation
Global perspective	The monthly project meetings provide a broader view of all of the project's risks.
	A more global perspective of the issues, priorities, and desired mitigation goals are obtained by adding customers and suppliers to the risk management process.
	A global perspective of the organization's risks can be achieved when all of the projects report risks. This happens when the top risks are communicated to the site manager.
	Risks which are identified by project personnel can be understood more globally from a system perspective by including information from all of the project members, not exclusively from software engineers.
Integrated management	Risk information is added to the project's problem database. The addition of lessons learned for risks and problems results in the integration of risk management with problem solving.
	During weekly and monthly project meetings, risk information is included as an agenda topic, integrating risk management with routine project work. The discussion of risk information is not scheduled as a separate meeting that could easily be ignored by some project personnel.
Teamwork	The weekly team meetings and the monthly project meetings bring project personnel together to discuss and understand issues, to set more realistic priorities, to improve mitigation plans, and to exchange information and knowledge.
	The personnel responsible for risks use small subteams when developing complicated or costly mitigation plans. Small subteams require team synergy to identify risks and to collect and analyze tracking information.
	External communication with customers, suppliers and senior management enables broad-based teamwork through the exchange of expertise as well as through the joint development of cooperative mitigation actions and mitigation plans.
Continuous process	Risk management is not a one-time only activity. The ongoing individual activities as well as the weekly and monthly meetings are part of a continuous process.

Chapter 12

Life-Cycle of a Risk

Section

Section 1

Introduction

Risk Scenario

This chapter introduces a scenario from the project discussed in Chapter 11 and demonstrates how a risk is managed across its entire life-cycle. Sample templates are used to illustrate how the methods and tools contained in the appendix can be used during risk management. The scenario gives the reader a complete example of a risk and all of the data that are developed as it is managed. This is a more extensive and complete example than the smaller, individual examples provided throughout the rest of the guidebook.

Example Contents

The risk management example outlined in this chapter includes the following:

- *identification and analysis*: the person who identified the risk, the risk's estimated probability, impact and timeframe, the risk information sheet used to document the risk, and the results of meeting discussions
- *planning*: the decisions made by the person responsible for mitigating the risk and the information that led to the decisions; an action item list documents the mitigation plan
- *tracking and control*: the accomplished actions, the status reviews, and the changes in circumstances as time progresses; status reports are provided to show what would be documented and reported
- *closure*: the circumstances and mitigation success that lead to closure

Who's in This Scenario?

The following diagram shows the scenario participants and their positions in the organization using the organizational chart introduced in Chapter 11.

Project ABC Organization Chart
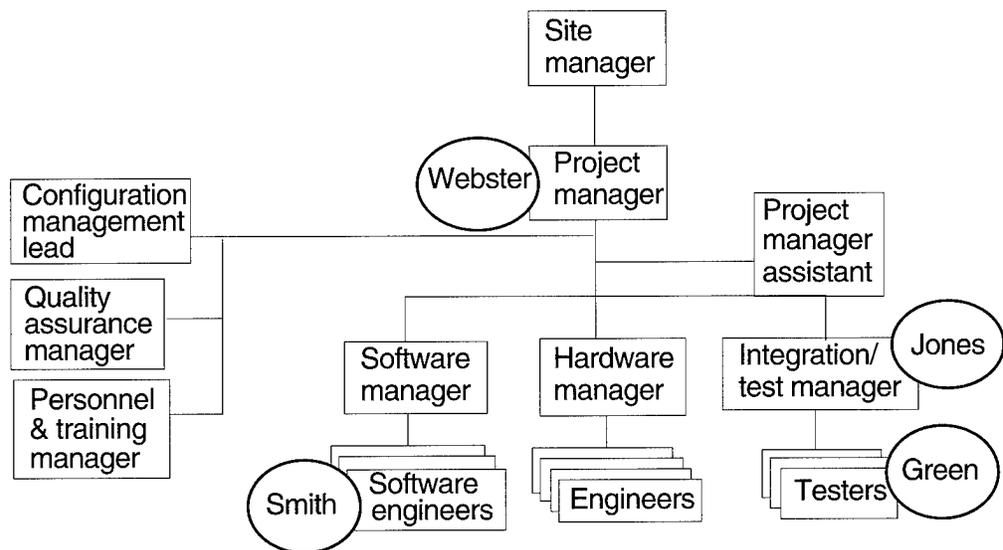
Section 2

Identification and Analysis

Software Engineer Smith

Smith has taken some of his own time to peruse the company's new lessons learned files from the risk/problem database. He knows that the original schedule and resource allocations for integration and testing of System ABC was based on that of a previous project, System LMN. According to the lessons learned report, System LMN ran into a lot of trouble with integration testing schedules. Smith's review of System ABC's allocated time at the test facility makes him very uneasy, but he doesn't know if there are any better estimates for the time required to fully test the system. He discusses the issue with the other software engineers, decides to identify a risk, and submits a **Risk Information Sheet** [Chapter A-27] to the database.

Risk Statement

The allocated schedule and resources for integration and test at the test facility may be inaccurate; delays in testing and insufficient testing time could lead to a defective product.

Risk Context

The estimates used for System ABC were based on those used for the LMN Project, which, at the time, appeared to be good estimates. However, the lessons learned from that project included one about inadequate time and resources at the test facility. LMN is similar to System ABC.

Risk Classification

Smith, using **Taxonomy Classification** [Chapter A-34], decides that the risk is a *Program Constraint, Resources* type of risk because it includes schedule and facility concerns.

Risk Attribute Evaluation

Using **Tri-level Attribute Evaluation** [Chapter A-38], Smith decides that the probability for this risk is high, the impact is high, and given the long lead time necessary to reschedule the test facility, the timeframe is near-term.

Weekly Team Meeting

Smith brings the risk to the software group's weekly team meeting and proposes to transfer it to the integration and test group. Everyone agrees, and they decide to discuss the risk at the next monthly project meeting.

Monthly Project Meeting

At the next monthly meeting, the risk is brought up and discussed. The project manager and technical leads are concerned, and they decide that the risk is important enough to add to their top N list. Using **Multivoting** [Chapter A-17], they place the new risk at fifth (5) on the project's Top N list. The integration and test manager, Jones, is given responsibility to investigate and mitigate the risk.

Risk Information Sheet

The following form is the modified risk information sheet which was submitted by Smith. It was modified after the monthly meeting to include the *Priority* and *Assigned To:* fields as well as additional context.

ID ABC104	**Risk Information Sheet**		**Identified**: 2/14/96
Priority 5	**Statement** The estimated schedule and resources for integration and test at the test facility may be inaccurate; delays in testing and insufficient testing time could lead to a defective product.		
Probability High			
Impact High			
Timeframe Near	**Origin** Smith	**Class** Program Constraint: Resources	**Assigned To:** Jones

Context

The estimates used for System ABC were based on those used for the LMN Project, which, at the time, appeared to be good estimates. However, the lessons learned from that project included one about inadequate time and resources at the test facility. Project LMN's delivered system is similar to System ABC and we're going to be using the same test facility.

Mitigation Strategy

Contingency Plan and Trigger

Status   **Status Date**

Approval	**Closing Date**	**Closing Rationale**
_____	__/__/__	

Section 3

Planning

**Mitigation
Approach:
Research**

Jones decides that he needs to research the risk and arranges to meet with the former manager of the LMN project. Jones is interested in obtaining more information about the test facility scheduling problems for Project LMN. He learns that they failed to allow sufficient time for unit testing, that too many modules went into integration with errors, and that their project management processes failed to detect or prevent the problems.

In addition, Jones learns that the test facility was undergoing upgrades at the time and that the upgrades were not going well. Project LMN lost a lot of its allocated time to finding problems with and waiting for corrections to the test facility equipment. Jones feels a little better because he believes that ABC's configuration management, quality assurance, and unit test processes are excellent. However, he is concerned about whether enough time for unit testing has been allocated in System ABC's schedule. Jones is also worried that the upgrades to the test facility are still in progress.

**Accept,
Watch, or
Mitigate?**

Given what he's learned, Jones believes that risk must be mitigated. There are just too many unknowns and potential issues that he can't control. The risk will need a mitigation plan; accepting or watching the risk would not be appropriate in this case.

**Action Items
or Task Plan?**

Jones is sure that he can handle the risk by employing a series of coordinated action items; a complete task plan is not required for this particular risk. He decides to construct an action item list and will use a **Planning Worksheet** [Chapter A-22] to help identify alternative contingency plans. Two of Jones' senior testers work with him to develop the mitigation plan.

**Planning
Worksheet**

The planning worksheet on the next page shows the results of the planning session. Several causes are identified and seven alternative actions are documented. Four of the actions are selected as the final mitigation strategy, while one of the remaining actions is designated as a contingency plan.

**Documenting
and
Approving**

Jones adds the mitigation plan (list of actions) to the risk information sheet. He decides to take the mitigation plan directly to the project manager because time is a critical issue, and the next monthly meeting is three weeks away. Project manager Webster approves the plan but also asks Jones to send copies to the other technical leads for their immediate review. All of the technical leads agree with the plan and send electronic mail indicating their approval to both Jones and the project manager by the end of the day.

Planning Worksheet	
Risk ID ABC 104	**Responsibility** Jones

Risk Statement   The estimated schedule and resources for integration and test at the test facility may be inaccurate; delays in testing and insufficient testing time could lead to a defective product.

Mitigation Goals and Constraints (in observable terms)
Integration testing completed with less than 1% error correction needed; negotiate and successfully use a revised schedule at the test facility.

Additional Data (e.g., root causes, impacted elements)
1. assumed accuracy of estimation method
2. didn't check for lessons learned before using estimation method
3. didn't ask about test facility upgrade schedule (didn't know there was an upgrade schedule)
4. test facility manager did not communicate upgrade schedule
5. LMN had CM and QA problems that made things worse

Related Risks   none

Alternative Strategies/Actions
1. Revise estimates—use successful projects' methods and LMN lessons learned.
2. Find out what upgrade schedule is and how it impacts us.
3. Reschedule test facility based on new estimates.
4. Check on our QA and CM for potential problems.
5. Look for alternate test facilities.
6. Request a delay in project schedule now, just in case the other actions fail.
7. Delay the test facility upgrade until after we're done testing.

Related Mitigation Plans   none

Strategy Evaluation Criteria
Can we control the action? Can we avoid impacting the customer? Can we avoid significant increases in budget? Can we get it done before unit testing?

Chosen Strategy/Actions	**Success Measures**
1. Revise estimates—use successful projects' methods and LMN lessons learned	1. Site experts like the revised estimates.
2. Find out what upgrade schedule is and how it impacts us	2. Impacts are identified.
3. Reschedule Test Facility based on new estimates	3. New schedule is approved/met.
4. Check on *our* QA and CM for potential problems	4. QA/CM have no problems we can't fix.

Contingency Strategy	**Contingency Trigger**
Request a delay in scheduling from the customer equal to 1/2 the % slip seen by LMN project (assuming 50% slip due to CM/QA problems we don't have).	If we can't get accurate estimates or the revised schedule is rejected.

Mitigation Actions

The following risk information sheet is a modified version which shows Jones' list of actions as well as the due dates for mitigating the risk.

ID ABC104	**Risk Information Sheet**		**Identified**: _2/14/96_
Priority 5	**Statement** The estimated schedule and resources for integration and test at the test facility may be inaccurate; delays in testing and insufficient testing time could lead to a defective product.		
Probability High			
Impact High	**Origin** Smith	**Class** Program Con-straint: Resources	**Assigned To:** _____ Jones
Timeframe Near			

Context

The estimates used for System ABC were based on those used for the LMN Project, which, at the time, appeared to be good estimates. However, the lessons learned from that project included one about inadequate time and resources at the Test Facility. Project LMN's delivered system is similar to System ABC and we're going to be using the same test facility.

Mitigation Strategy

1. Jones will review/revise unit and integration testing estimates based on LMN and 2 successful projects. Due 4/15.
2. Green will get current status and projected completion dates for test facility upgrades. Due 3/11.
3. Jones will check with QA and CM about how well things are going in their areas. Due 5/1.
4. Jones will revise and resubmit Test Facility schedules based on above actions. Due 6/20.

Contingency Plan and Trigger Request a delay in scheduling from the customer equal to 1/2 the % slip seen by LMN project (assuming 50% slip due to CM/QA problems we don't have).	If we can't get accurate estimates OR the revised schedule is rejected.

Status	**Status Date**

Approval _____	**Closing Date** __/__/__	**Closing Rationale**

Section 4

Track, Control, and Track Again

Reporting Progress

Jones uses **Spreadsheet Risk Tracking** [Chapter A-30] to report the status of the risk as well as the statuses of the other risks for which he has responsibility. The spreadsheet is generated by the risk/problem database at Jones' request. The following excerpts from the monthly risk spreadsheets show the progress that is being made in mitigating the risk as well as the changes that are necessary upon completion of the actions.

March 12 and March 15

At the weekly meeting on March 12, test engineer Green reports that the test facility manager has ordered the wrong software version for one part of the upgrade (Software Z). Green also reports that the revised software acquisition is being delayed by corporate headquarters due to a budgetary shutdown of all new COTS purchases, and there is no estimate of when corporate headquarters will release the paperwork. System ABC must use the part of the test facility that requires Software Z no later than July. Jones reports this information at the monthly project meeting on March 15, and Webster, the project manager, takes an action to see if he can get the paperwork process restarted.

Test and Integration Risk Spreadsheet						3/15/96
Risk ID	**Priority**	**Risk Statement**	**Status Comments**	**Proba-bility**	**Impact**	**Assigned To**
ABC 104	5	Estimated schedule and resources for I&T at the test facility may be inaccurate; delays in testing and insufficient testing time could lead to a defective product.	Green: Software Z purchase delayed indefinitely. Webster to try and free up paperwork (due 4/15/96)	high	high	Jones, A.

April 19

Jones has collected lessons learned from successful projects within the company as well as from external sources, and he now feels more confident with the revised unit and integration testing estimates. Unfortunately, the revised estimates delay the start of integration testing by two months and nearly double the original amount of testing time. Project manager Webster calls for a special meeting with the technical leads to review the project plan and to see what impact the revised estimates will have on the project.

Webster has had no success getting the test facility's paperwork for Software Z released. He asks Jones to review the integration test plan to determine how to proceed if the software doesn't arrive in time.

The priority for this risk is increased; it is now second on the top N list.

Test and Integration Risk Spreadsheet						5/5/96
Risk ID	**Priority**	**Risk Statement**	**Status Comments**	**Proba-bility**	**Impact**	**Assigned To**
ABC 104	2	Estimated schedule and resources for I&T at the test facility may be inaccurate; delays in testing and insufficient testing time could lead to a defective product.	Jones: personnel adjustments and overtime = no schedule slip. Completion sequence changed. Jones to review Test Facility request to see if this affects it. (due 5/27) Jones: Software Z available elsewhere. Trying to transfer licensing (due 5/27). Jones: CM and QA check out fine.	high	high	Jones, A.

May 5

A review of the project plan has resulted in adjustments to personnel and overtime requirements; no delay in the schedule will be necessary for unit testing. However, the sequence of actions is now different; as a result, the integration test sequence has changed. Jones reviews the recommended changes and revises the test facility request. The configuration management and quality assurance leads report that the changes do not affect their procedures.

Jones determines that there is no way to proceed without the acquisition and installation of Software Z. He also discovers that Software Z has been purchased by another test facility in the company, but that it has not been installed. Negotiations are underway to transfer the licensing agreements to Project ABC's test facility. The team anticipates no problems in doing this.

Test and Integration Risk Spreadsheet						4/19/96
Risk ID	**Priority**	**Risk Statement**	**Status Comments**	**Proba-bility**	**Impact**	**Assigned To**
ABC 104	2	Estimated schedule and resources for I&T at the test facility may be inaccurate; delays in testing and insufficient testing time could lead to a defective product.	Jones: I&T estimate revisions are sound, but means delay in testing start (2 months) and doubles integration time. Special meeting called (due 4/24) to review project impacts. Webster: Software Z paperwork still locked up. Jones to look for work-around (due 4/27)	high	high	Jones, A.

June 30   Software Z has been installed, tested, and approved.

Jones' request for additional test facility time is immediately approved by the facility manager during the weekly schedule review meeting. The risk is moved to the *Watch* category and is no longer on the top N list. The probability is now low, although the impact is still considered to be high.

The site manager has publicly congratulated Project ABC for its foresight and hard work.

Test and Integration Risk Spreadsheet						6/30/96
Risk ID	**Priority**	**Risk Statement**	**Status Comments**	**Proba-bility**	**Impact**	**Assigned To**
ABC 104	24	Estimated schedule and resources for I&T at the test facility may be inaccurate; delays in testing and insufficient testing time could lead to a defective product.	Jones: System Z installed, tested, and approved for use. Jones: revised facility request approved.	low	high	Jones, A.

Section 5

Closure

Keeping Watch

Because he is concerned that other things could affect the test facility schedule as well as ABC System's schedule requirements, Jones keeps the risk on the *Watch* list as a reminder to continually pulse the facility manager and the testers for progress and issues.

September 12: Closure

Integration testing is successfully completed and System ABC is going into its acceptance phase. The risk was watched throughout integration testing, and no other problems surfaced. As part of the closure process, all relevant information about the risk is documented. Jones adds several personal lessons learned comments concerning the risk to the risk/-problem database and is writing a short paper for the company newsletter on estimating integration test schedules.

What Was the Benefit?

The project manager estimates that identifying and dealing with the risk saved the organization at least 10% of the project's budget. If project personnel had decided not to mitigate the risk, integration testing would have been delayed by three months (accounting for the 10% estimate), and the customer may have had to accept a low-quality system (an incalculable loss in customer satisfaction). Mitigation of this risk alone was worth the extra time and effort that was spent performing risk management (estimated at 1% of the project budget—i.e., risk management required that an additional 1% of the project resources be spent on project management activities than originally estimated).

Sponsorship and Rewards

To continue inspiring other projects to actively deal with their risks, the site manager chooses Project ABC, Smith, and Jones for recognition in the corporate newsletter. He also submits Smith's and Jones' names for year-end bonuses. Smith has already taken his lessons learned about risk management to a new project and is helping that project to begin its own risk management practice.

Closed Risk: Risk Information Sheet

The risk information sheet for the closed risk, including the appropriate closure information, is shown on the following page.

ID ABC104	Risk Information Sheet		Identified: 2/14/96
Priority 5	**Statement** The estimated schedule and resources for integration and test at the test facility may be inaccurate; delays in testing and insufficient testing time could lead to a defective product.		
Probability High			
Impact High	**Origin** Smith	**Class** Program Constraint: Resources	**Assigned To:** Jones
Timeframe Near			

Context

The estimates used for System ABC were based on those used for the LMN Project, which, at the time, appeared to be good estimates. However, the lessons learned from that project included one about inadequate time and resources at the Test Facility. Project LMN's delivered system is similar to System ABC and we're going to be using the same test facility.

Mitigation Strategy

1. Jones will review/revise unit and integration testing estimates based on LMN and 2 successful projects. Due 4/15.
2. Green will get current status and projected completion dates for test facility upgrades. Due 3/11.
3. Jones will check with QA and CM about how well things are going in their areas. Due 5/1.
4. Jones will revise and resubmit Test Facility schedules based on above actions. Due 6/20.

Contingency Plan and Trigger

Request a delay in scheduling from the customer equal to 1/2 the % slip seen by LMN project (assuming 50% slip due to CM/QA problems we don't have).	If we can't get accurate estimates OR the revised schedule is rejected.

Status	**Status Date**
Software Z purchase delayed indefinitely. Webster to try and free up paperwork (due 4/15/96)	3/15/96
I&T estimate revisions are sound, but means delay in testing start (2 months) and doubles integration time. Special meeting called (due 4/24) to review project impacts. Software Z paperwork still locked up. Jones to look for work-around (due 4/27)	4/19/96
Personnel adjustments and overtime = no schedule slip. Completion sequence changed. Jones to review test facility request to see if this affects it. (due 5/27). Software Z available elsewhere. Trying to transfer licensing (due 5/27). CM and QA check out fine.	5/5/96
System Z installed, tested, and approved for use. Revised facility request approved.	6/30/96
Risk closed - integration and testing successfully completed. Risk no longer exists.	9/12/96

Approval A. Jones Mr. Webster/PM	**Closing Date** 9 / 12/ 96	**Closing Rationale** all testing completed successfully; probability = 0.

**Lessons
Learned**

Jones documented the lessons learned for the risk in the risk/problem database. The following is what Jones included.

Lesson Type	Lesson
Integration and testing estimation method	The old method has been used for a long time but now appears to be outdated. We have documented a new method (see corporate post 1034) and it seems to have an increased accuracy (45% improvement) based on our experience and the judgement of Wiley and Stone, our site experts.
Test facility schedule communication	There was no formal mechanism for communicating test facility upgrade schedules that we know about. This is a hole in the site management procedure that the site manager has corrected, as of this date. It does prove, however, that making assumptions about other managers' schedules without verifying those assumptions is unwise.
Budget impacts on tool purchases	When corporate headquarters shut down the budget on tool purchases and Software Z could not be purchased, word was not communicated to all site and project managers. This gap in policy has been corrected, but it highlights the need for all managers to verify all interdependencies and communicate issues to other project managers. It would have been helpful if the test facility manager had known which other project managers were dependent upon the purchase of Software Z.
Return on mitigation investment	We estimate our savings from mitigating this risk as at least 10% of our project budget—$250,000. This is based on our estimation that the delay in integration testing would have been 3 months and the customer would have had to accept a less than desired product. This customer dissatisfaction is an incalculable cost—they do a lot of work with us and might have felt it necessary to look elsewhere. Three pending contracts might have been affected (total $14.3 million).

Part 4

How to Get Started in Continuous Risk Management

Introduction

This part of the guidebook is a detailed description of how an existing project could apply Continuous Risk Management. A scenario is provided to show how Project ABC, introduced in Chapter 12, started, installed and improved their Continuous Risk Management practice. The summary also includes some considerations for new projects and organization-based improvement efforts.

Chapter 13

Overview
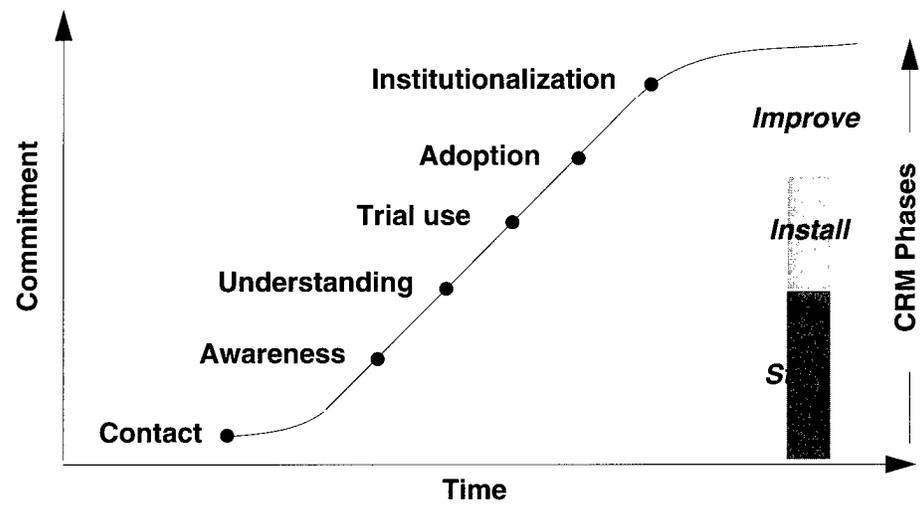
Section	
Applying Continuous Risk Management	160
Who Is Involved in Applying Continuous Risk Management?	163
References	165

Section 1

Applying Continuous Risk Management

Introduction

This part of the guidebook describes one process for successfully installing Continuous Risk Management in an ongoing project. The central focus of this chapter is on a "roadmap" for applying Continuous Risk Management. It will provide a framework for those activities needed to establish Continuous Risk Management. While the roadmap presents a linear view of the process, some activities can occur in parallel or overlap. These activities are described in detail within this chapter.

Objectives

The objectives of applying Continuous Risk Management are to establish a continuous and effective risk management practice in a project organization, and to have an ongoing proactive and accountable exchange of risk information between the project and its stakeholders.

Technology Transition

The phases in the application of Continuous Risk Management can be mapped to a more general technology transition model.

The general relationship between time and commitment (by the people in an organization) to bring about a successful technological change is described by the following technology transition or commitment curve[1] [Myers 92]. The Continuous Risk Management application phases of *Start* ("contact," "awareness," and "understanding"), *Install* ("trial use"), and *Improve* ("adoption" and "institutionalization) are mapped to the technology transition curve.
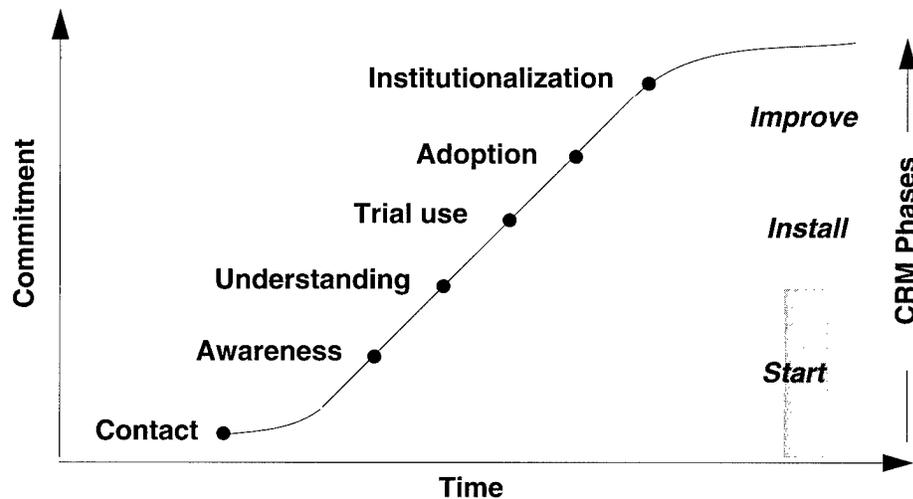
Application Roadmap

A "roadmap" of a successful application is presented on the following page to set the readers' expectations for the task ahead in applying Continuous Risk Management in their project.

---

1. This technology transition or commitment curve was adapted by Charles Myers and John Maher of the SEI from work originally done by Daryl R. Conner and Robert W. Patterson.

Continuous Risk Management Application Roadmap

START

Build
Infrastructure

Conduct
Infrastructure
Training

Establish
Risk
Baseline

INSTALL

Adapt to
Project

Install
Support
Tools

Train
Project
Personnel

Install
Basic
Practice

IMPROVE

Improve
Continuous
Risk
Management

Expand
Continuous
Risk
Management
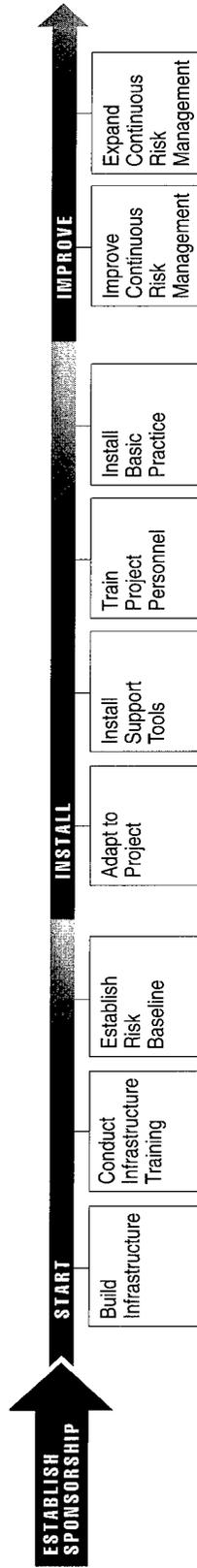
ESTABLISH
SPONSORSHIP

The following paragraphs describe some key features of the application roadmap.[1]

The Three Phases

There are three phases of time shown on the roadmap:
- Start (including establishing sponsorship)
- Install
- Improve

Start

The first phase in applying Continuous Risk Management involves several basic steps necessary for any successful technology transition.
- A decision and commitment to improve needs to be made—typically, sponsorship of and commitment to applying Continuous Risk Management in a project begins with the project manager.
- Initial awareness and understanding within the project must occur, followed by a desire to use the new technology.
- An infrastructure to support the transition needs to be built.
- Awareness and understanding of the basic concepts and principles needs to be grown within the project.
- A critical mass of initial risks and mitigation plans needs to be established and used as impetus for moving forward.

Install

The second phase corresponds to the level of commitment labeled "trial use" on the Technology Transition Curve. At this point, the project is actually trying the change in its own environment. This is usually done with both a "wait and see" attitude and a great deal of attention to the integration of the change with the unique organizational environment. For Continuous Risk Management, this is the critical phase when the project goes from theory to application, and serious resistance can be expected to begin. During this phase
- Continuous Risk Management is adapted to the project and a **Risk Management Plan** [Chapter A-28] is developed.
- Support tools are installed.
- Project personnel are trained.
- A basic risk management practice is installed in the project.

Improve

At the level of commitment labeled "adoption," the basic Continuous Risk Management has moved out of initial use and is being successfully used in the entire project. Improvements to the processes, methods, and tools are now being tried and expansion of Continuous Risk Management into other projects has begun. Resistance to the change may still be high, especially in other projects. At the level labeled "institutionalization," the change has moved into the organization and is accepted everywhere.

---

1. This roadmap and the application activities described in this Part are derived from the SEI experience at transitioning risk management into client organizations and projects as well as related work on general technology transition models and the IDEAL[SM] model for software process improvement [Fowler 90], [Fowler 93], [Myers 92], and [Radice 94]. (IDEAL is a service mark of Carnegie Mellon University.)

The Change to Continuous Risk Management

Installing a Continuous Risk Management practice in a project will change the way the project anticipates its future and plans its work. The principle of open communication is the life-blood of Continuous Risk Management, and how this change will affect a project depends on the how well the project communicates today (both internally and in its dealings with the customer or supplier(s)). If communication is not open now, members of the project may feel stress and uncertainty as they adjust to new relationships, and this will lead to resistance. This transition and the stress it imposes is well documented and normal for organizations. It is important to see resistance to change as normal, so that it does not derail the effort before the change process has become self-sustaining.

Common Risks

There are risks that are common to any type of improvement endeavor such as applying Continuous Risk Management [Radice 94]:
- insufficient sponsorship, especially senior managers
- resistance by middle managers (e.g., project managers)
- lack of motivation for improvement or change
- inadequate resources allocated to the effort
- inappropriate goals
- termination of activities before the practice is institutionalized
- lack of sustained focus on improvement

These are risks that need to be avoided or mitigated in order to be successful at implementing improvements such as Continuous Risk Management.

Why Isn't There an End to the Map?

No end to the roadmap is shown, because with full institutionalization of the Continuous Risk Management practice, the effort will outlive the project and be incorporated as part of the day-to-day management activities of the organization's projects, indistinguishable from "business as usual." Improvements and adjustments, expansion into other new projects, will continue as long as the corporation exists.

Section 2

Who Is Involved in Applying Continuous Risk Management?

Everyone Is Involved

Continuous Risk Management is not a job for only the manager or a designated technical lead (e.g., a risk manager). Applying Continuous Risk Management is also not the job of a single person. The principles of open communication and teamwork are directly related to the fact that it takes everyone on a project to successfully install Continuous Risk Management and then manage the risks. No single person knows everything; synergy is what enables the project to function.

Does Everyone Do Everything?

Although everyone is involved in applying Continuous Risk Management, it does not mean that every task is carried out by every person. As with any improvement or transition effort, there are tasks and activities which are best suited to different parts and individuals in the project. The following table summarizes the roles and responsibilities found throughout the remaining chapters for all of the types of people involved in applying Continuous Risk Management.

Role/Description	Responsibilities and Tasks
Project personnel (e.g., software engineers, hardware engineers, testers, etc.)	Attend training sessions. Contribute to baseline identification, analysis, and planning. Add Continuous Risk Management activities to day-to-day operations. Maintain open communication about risks. Ask for help rather than abandoning the process.
Sponsor (e.g., senior manager—publicly advocates and supports change)	Provide visible support and encouragement. Reward effective management of risks. Empower people to act within their designated roles. Evaluate Continuous Risk Management installation progress.
Project manager (responsible for the successful completion of the project)	Provide encouragement to project personnel. Provide required resources and funding. Support open communication. Designate a champion within the project. Reward effective management of risks. Monitor progress.
Champion (advocate or supporter of the new technology or process within the project)	Encourage project personnel involvement. Publicize and promote Continuous Risk Management. Coordinate changes and improvements in the project. Report progress to project manager. Prepare tool recommendations and implementation plan.

Role/Description	Responsibilities and Tasks
Change agents (plan and implement organizational and project changes (e.g., Software Engineering Process Group (SEPG) personnel))	Assist champion in preparation of recommendations and implementation plan. Work with champion to develop training plan. Evaluate existing and new tools with champion. Make recommendations for new tool purchases or tool modifications.
Technical managers (team or functional leads, such as software manager, test manager, etc.)	Encourage and support use of Continuous Risk Management within their teams. Report risk information to project manager. Evaluate progress within their teams.
Facilitator, facilitation team, baseline team (personnel trained in meeting skills, conflict resolution, tools, group mechanics, etc., who act individually or as a team to lead specific efforts or methods)	Assist in adaptations of methods and tools. Monitor and evaluate progress. Report progress to sponsor. Conduct training sessions. Provide Continuous Risk Management expertise. Provide consulting during evaluation of progress. Coordinate, conduct, and report on baseline activities.
Other projects	Implement Continuous Risk Management. Coordinate risks across projects. Make use of lessons learned.
Customers, senior managers, suppliers	Learn about Continuous Risk Management. Accept risks reported by project with open minds. Work with the project to resolve risks. Reward the activity.

Section 3

References

Cited in this chapter:

[Fowler 93]   Fowler, Priscilla & Levine, Linda. *A Conceptual Framework for Software Technology Transition.* (CMU/SEI-93-TR-31). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

[Fowler 90]   Fowler, Priscilla J.; Rifkin, Stan; & Card, David N. *Software Engineering Process Group Guide* (CMU/SEI-90-TR-24, ADA 235784). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1990.

[Myers 92]   Myers, Charles R.; Maher, John H.; & Deimel, Betty L. *Managing Technological Change.* Course materials. Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1992. For information about this course, contact SEI Customer Relations at (412) 268-5800 or customer-relations@sei.cmu.edu.

[Radice 94]   Radice, Ron & Garcia, Suzie. *An Integrated Approach to Software Process Improvement (SPI).* Tutorial presented at the Software Technology Conference, April 1994, Salt Lake City, Utah. For information about this tutorial, contact The Utah State University, Continuing Education/Conferences at (801) 797-0423.

Chapter 14

Getting Started
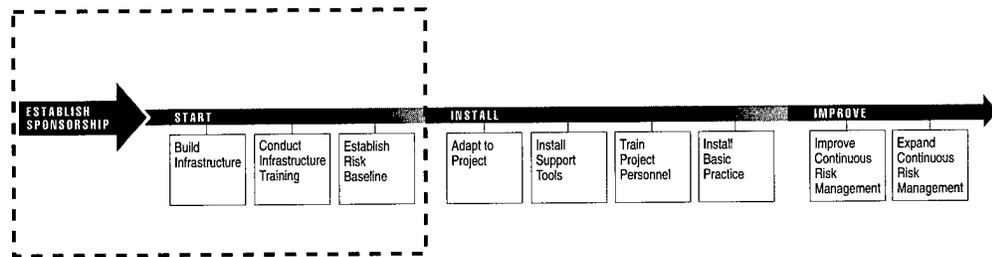
Section 1

Establish Sponsorship

Description

Successful organizational change requires commitment from the top. Change begins when someone in the project perceives a need and locates a potential solution. Once the desire to change exists, that person needs to *Establish Sponsorship* for the change. This means convincing the appropriate persons in the organization about the value of the change to the project, and they then decide to sponsor adoption of the change. Generally, the project manager is the sponsor, although risk management can be successfully sponsored at a higher level in the organization (e.g., vice president of projects, chief executive, program executive officer), particularly if the goal is to apply Continuous Risk Management throughout the organization.

Purpose

The purpose of the Establish Sponsorship activity is to show informed commitment to Continuous Risk Management and clarify the sponsor's expectations about risk management and the roles that personnel both inside and outside the project organization are to play in its success. Sponsorship is a public decision by a suitably authoritative and influential manager showing

• the belief that Continuous Risk Management is critical to the project

• the willingness to commit suitable resources to it

• the determination to see it succeed

Key Considerations

The key considerations when establishing sponsorship are

• Commitment from key stakeholders (anyone who depends on or requires project success) must be obtained and made clear to all groups.

• Sponsorship must be established and continuously reinforced at all levels of the organization.

• The sponsor should have control of (or be willing to allocate) the resources (people, funds, time) needed to successfully manage risks.

Diagram

The following diagram shows inputs and outputs for this activity.
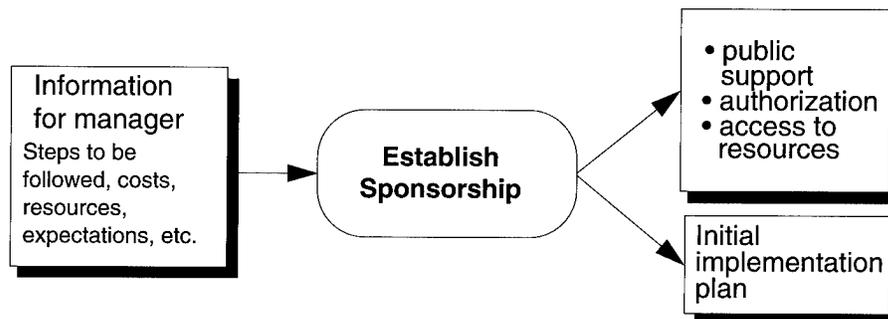
Why Use Continuous Risk Management?

The sponsor may decide to adopt the practice of Continuous Risk Management for one or more reasons. This decision can come through various rationale.

Reason	Rationale
Integration	Multiple interfaces and external suppliers need to be managed.
Competitive edge	Advantage over a competitor may be gained.
Customer direction	Continuous Risk Management is part of a contract solicitation and is an expected part of contract performance.
Self-motivation	A credible and competent person in the organization champions the cause for adopting Continuous Risk Management.
Expected financial benefit	Mitigating today's risks is expected to be more cost effective than solving tomorrow's bigger problems.
Early warning	An "early warning" system is needed to avoid problems before they happen.

When to Start Continuous Risk Management

The best time to initiate Continuous Risk Management is as early in the project life-cycle as possible. Here are some opportune times to start the Continuous Risk Management activities.

Opportunity	Actions
Pre-contract activity	Include risk management provisions in the solicitation and statement of work.
Major project milestones (e.g., contract award or design reviews)	Prepare for a major project decision point, and the need to increase knowledge about risks for improved strategic planning.
Major project review	Prepare for a major review, such as design reviews, functional tests.
New manager	Use risk data information as an effective way to bring a new manager "up to speed" on the project.

Procedure

The following table describes a typical procedure by which a sponsor would decide to undertake a risk management effort and begin that commitment.

Step	Action
1	**Learn about Continuous Risk Management**. Someone in the project or organization learns of the benefits of organized, project-wide Continuous Risk Management. This information may come from any trusted source: peers, superiors, trade conferences, journals, "champions" from within the organization, and so forth.
2	**Gather information**. Information needed for a potential sponsor to make a decision is gathered. Estimates of benefits, projected costs, resources needed, and support available from outside the project are examples. Outside experts might be consulted, literature searches can be conducted, and other successful projects within the organization can be interviewed. *Note*: This is where a corporate "lessons learned" database would be useful.
3	**Present information**. The information is presented to the potential sponsor for a decision. Emphasis should be given to benefits, costs and required resources (especially long-term). If risk management will provide a competitive advantage, or is now required by customers, that should be discussed.
4	**Make decision**. The sponsor decides to give the risk management effort full support. The necessary infrastructure (including any outside support) is built, subordinates are consulted and informed of their initial roles in implementation of the effort, and a suitable time for initiation is selected. Because no effort such as this is without risk, the major risks and mitigation plans associated with this effort should be identified.
5	**Build implementation plan**. The sponsor, facilitator, and project manager create a plan and schedule for implementing Continuous Risk Management.
6	**Inform project**. The sponsor informs the entire project organization of the decision and the reasons for it, communicating the level of commitment. The sponsor describes the initial activities with projected dates for each.

Roles and Responsibilities

The following table describes the roles and responsibilities of personnel during this activity.

Role	Responsibilities
Change agent (this could be any person, inside or outside the project)	Learn about risk management and processes for implementing it in the project.
	Gather information needed for sponsor's decision.
	Read this guidebook—learn about and understand Continuous Risk Management, be able to answer any questions the sponsor may have.
	Make contacts with other organizations who know about or use Continuous Risk Management.
Sponsor	Decide; then communicate that decision.

What's in an Implementation Plan?

The implementation plan directs all of the activities discussed in this part of the document: the activities associated with Start, Install, and Improve. It should include

- roles and responsibilities
- schedule and milestones
- allocated budget and resources
- measures to be collected, evaluated, and reported.

Note: Any change effort such as this will have associated risks. The facilitator and the change agent should help the sponsor and project manager identify, mitigate, and track those risks.

Section 2

Build Infrastructure

Description

To support any change, an infrastructure is needed to support the project in carrying out the new activities, measuring their success, and monitoring progress. Infrastructure is particularly necessary to maintain momentum as project personnel strive to become proficient in the new activities.

Purpose

The purpose of this activity is to make sure all of the right people and support processes are in place before beginning to implement Continuous Risk Management in a project. This infrastructure includes

- champion internal to the project
- change agents
- facilitators
- special teams

Key Considerations

Key consideration when building an infrastructure are

- Change has to be supported for it to be successful.
- An internal champion is needed to provide the continual, day-to-day encouragement to the project and to lead the drive for improvement.

Diagram

The following diagram shows the inputs and outputs for this activity.

```
Organization's
resources
                              ┌──────────────┐          • champion
Infrastructure        ───▶    │    Build     │   ───▶   • change agents
roles and                     │Infrastructure│          • facilitators
responsibilities              └──────────────┘          • special teams

Initial
implementation
plan
```
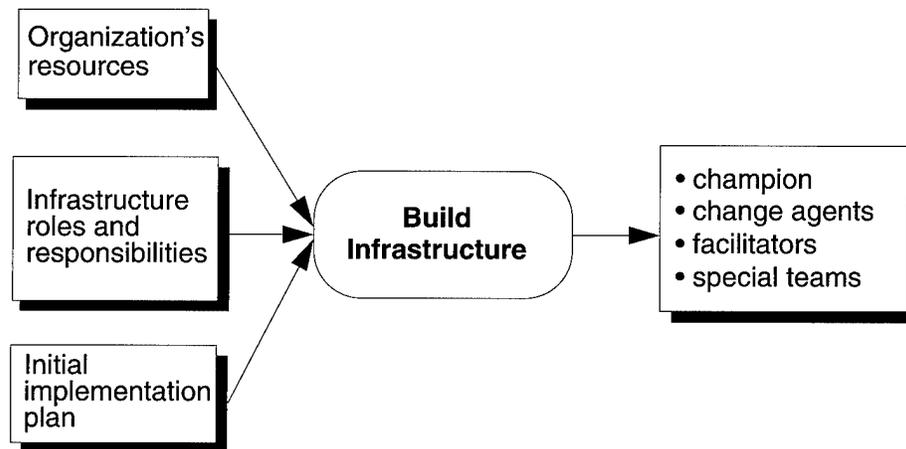
Procedure

The following table describes a general procedure for building an infrastructure to support installing Continuous Risk Management.

Step	Action
1	**Identify required roles**. The infrastructure will need people to fill the roles of champion, change agent, facilitator (and facilitation and baseline teams). The sponsor and project manager will have to consider when to have the various roles filled, and for how long.

Step	Action
2	**Select candidates for the roles**. Based on the required time commitments and necessary skills, identify potential candidates for the roles. Sponsor and project manager must then decide which personnel to seek.
3	**Secure commitment from candidates for the roles**. Once the candidates have been identified, notify them of the possible work and secure their commitment. Negotiations among managers will likely be necessary. Alternative candidates may be needed if first choices are unavailable.

Selection Criteria

The following table outlines some of the selection criteria that can be used in selecting personnel to fill the infrastructure roles. Other considerations such as workloads, availability, career development, team interaction, etc., should also be used.

Role	Criteria
Champion	Strong advocate of improvements
	Influential within the project
	Recognized leadership skills
	Recognized source of expertise and help
	Note: Champion and change agent can be the same person.
Change agent	Strong advocate of effective, controlled change
	Recognized training skills
	Recognized leadership skills
	Works well with the sponsor
Facilitator	Strong facilitation and conflict resolution skills
	Trained in meeting management and group mechanics
	Recognized leadership skills
	Can serve as a resource or source of expertise for Continuous Risk Management
	Note: To ensure non-attribution, the facilitator should not be a project member.
Special teams: • facilitation team • baseline team	Facilitators who help with implementation. Facilitation team provides assistance whenever more than one facilitator is required. The baseline team is a short-term team to help conduct the baseline activities. Team members should • understand software engineering and Continuous Risk Management • understand corporate processes • be trained in the Continuous Risk Management methods and tools *Note*: They need not be expert in the project's technology.

Roles and Responsibilities

The following table summarizes the roles and responsibilities of personnel during this activity.

Role	Responsibilities
Sponsor	Empower subordinates to act within the designated roles.
Project manager	Work with the sponsor (unless sponsor and project manager are the same person, in which case, the project manager will work with senior managers) to identify and select candidates for the infrastructure roles.

Section 3

Conduct Infrastructure Training and Project Familiarization

Description *Conduct Infrastructure Training and Project Familiarization* encompasses all of the training activities needed to set the stage for Continuous Risk Management and ensure that the necessary skills exist for the *Start* and *Install* phases. The infrastructure members (e.g., special teams, facilitators, change agents, internal champion) need to have the required skills and method training to help the project. Every member of the project needs to know about Continuous Risk Management, understand why the organization is adopting it, what changes to their worklife may result, and what roles they will play in it.

Purpose The purposes of this activity are the following:
- provide infrastructure members with the information necessary to support this change
- provide the baseline team members with the needed skills to lead the establishment of a risk baseline
- give project personnel a common vision of the goal and a roadmap for Continuous Risk Management
- begin the process of establishing a common understanding of risk management in the project so that project communication of risks is enhanced

Key Considerations Key considerations when conducting infrastructure training and project familiarization are
- Training must be provided for the application of Continuous Risk Management to succeed—personnel need timely information and skills training.
- People at all levels in the project need to buy in to Continuous Risk Management.
- Concepts and terms, such as *risk*, *risk management*, and *risk baseline* must be understood to support Continuous Risk Management activities.
- Training is a key component in establishing and maintaining the Continuous Risk Management principle of open communication in the project.

Diagram The following diagram shows the inputs and outputs for this activity.
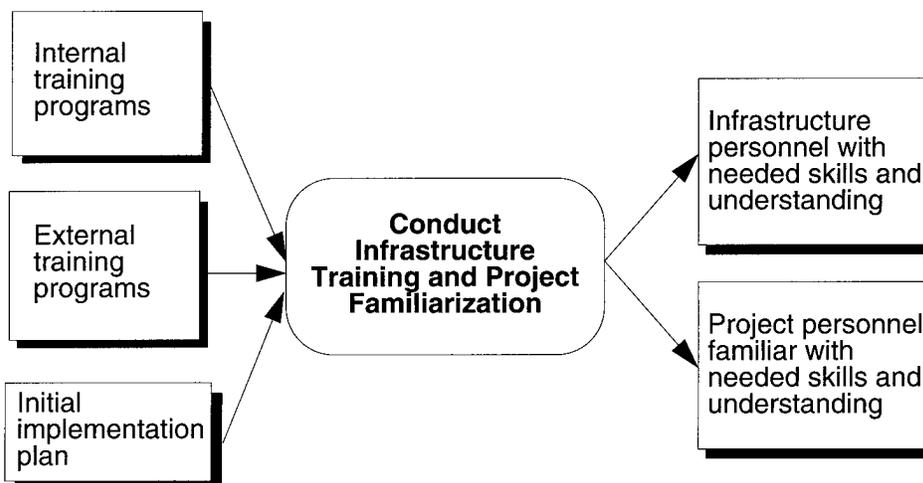
Procedure   The following table describes a typical procedure by which a project would go about completing this activity.

Step	Action
1	**Assign responsibility for training.** The project manager delegates responsibility to the champion for planning the training of infrastructure members and project personnel.
2	**Review training programs.** The champion determines the requirements and reviews the training and familiarization programs that are available from internal training organizations as well as external sources, such as vendors or training providers.
3	**Compile and develop training for project.** Select from external training and internal training programs and create a training agenda as needed to fill gaps. If external training has to be scheduled, make sure the schedule will support the project needs or consider having it brought on site.
4	**Select and schedule training.** The champion consults with change agent(s) to determine an appropriate training program and schedule, along with an estimate of the resource time and costs involved in training.
5	**Approve training.** The information is presented to the project manager for approval.
6	**Complete training arrangements.** The project manager gives the go-ahead, and arranges change agent support from the organization. The champion makes final arrangements for the training and publicizes the schedule to the infrastructure members and the project personnel.
7	**Conduct training.** The training plan is carried out, building the key skills in the infrastructure personnel and familiarizing the project with Continuous Risk Management and their expected roles in the change effort.

Roles and Responsibilities

These following table summarizes the roles and responsibilities of personnel during this activity.

Role	Responsibilities
Project manager	Designate a champion for Continuous Risk Management within the project and delegate responsibility and authority for planning the training to the champion.
	Review and approve training plan; help revise plan to make it consistent with budget limitations and time constraints.
	Secure change agent support from the organization.
	Make needed funding and resources available.
Champion	Gather training information.
	Prepare training plan.
	Identify change agent candidates from outside the project.
	Publicize and promote.
Change agents, special team members	Be aware of plans—make interest and capabilities known to the champion.
	(Optionally) provide some of the training.
Project personnel	Learn and understand the key concepts and terms of Continuous Risk Management.

Section 4

Establish a Risk Baseline[1]

Description

A risk baseline gets a project started in risk management. A risk baseline should have the following:

- list of known risks to the project clearly stated and accompanied by additional clarifying information (context)
- estimate of probability, impact, and timeframe for each risk
- sets of related risks
- prioritization of risks based on their importance to the project.

Purpose

The purpose of this activity is to

- generate a critical mass of risks for the project (a snapshot of all risks known to the project at this time)
- begin the practice of Continuous Risk Management

Key Considerations

The key considerations when establishing a risk baseline are

- Establishing a baseline set of risks can provide the critical mass of information needed to inspire risk management and provide the project with a place to start.
- Capturing risk information from a broad spectrum of project personnel is the key to getting as complete a set of risks as possible.
- Classification of risks into groups provides the foundation for maximizing the effectiveness of mitigation strategies developed during planning.
- Prioritizing risks provides the basis for effective utilization of scarce resources.
- The most important risks should be planned as soon as possible.

---

1. There are many ways to establish a baseline set of risks. The most effective appear to be defined, group events that use a set of sequential activities to build the list of risks and then process that information. This section describes the types of activities and results that are required for the establishment of an effective risk baseline. See **Baseline Identification and Analysis** [Chapter A-4] and **Baseline Planning** [Chapter A-5] for details.

Diagram   The following diagram shows the inputs and outputs for this activity.
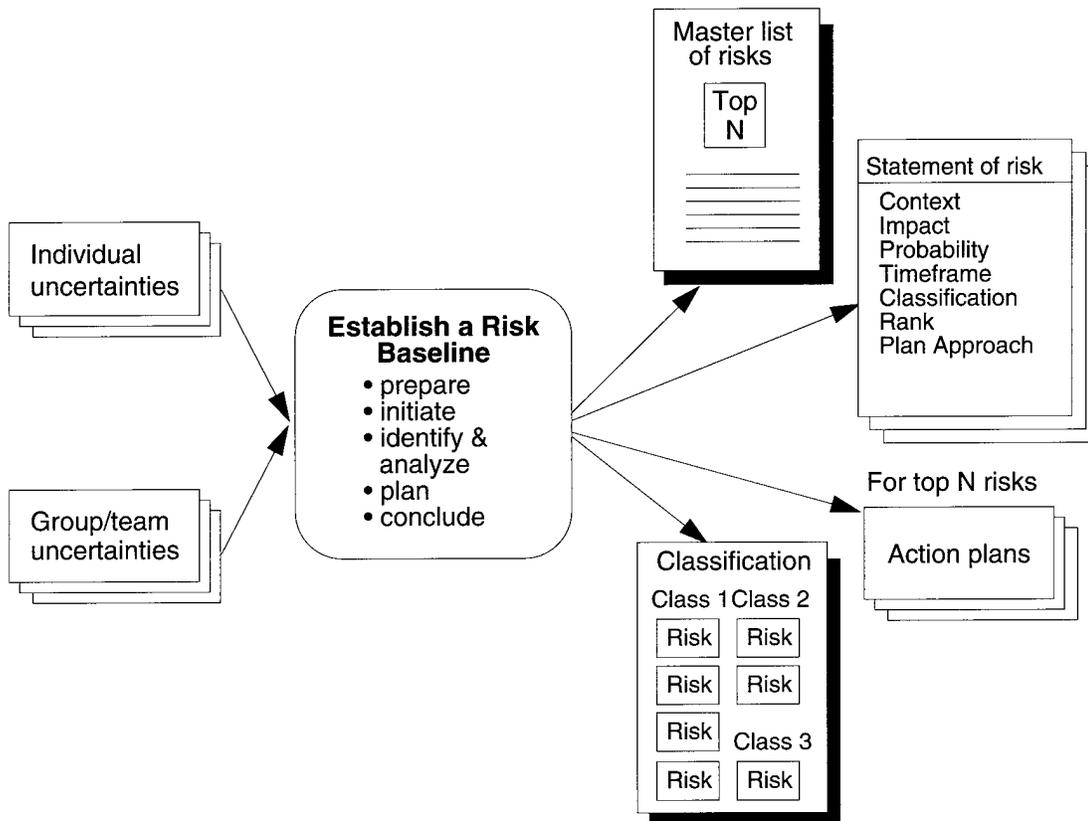
Procedure   Establishing a risk baseline consists of an ordered sequence of activities, as summarized below. This procedure presumes the use of a baseline team (facilitators trained in the methods) to lead the activities.

Step	Action
1	**Preparation**. The project manager and baseline team identify participants. The baseline team arranges logistics for the event.
2	**Initiating activities**. The baseline team provides an overview of the method to all of the participants and prepares them for their roles in that method. These sessions begin to establish a commitment to the Continuous Risk Management practice.
3	**Identification and analysis**. The baseline team conducts activities where risks are identified and analyzed by personnel throughout the project.
4	**Planning**. The baseline team conducts activities to help the project develop mitigation plans for the most important risks (generally the top N).
5	**Concluding activities**. The baseline team presents the results of the event. Interim presentations may occur before the planning activity in step 4.

Roles and Responsibilities

The following table summarizes the roles and responsibilities of personnel during this activity.

Role	Responsibilities
Participants—personnel from the project that will participate in one or more of the activities	Actively contribute to the identification and analysis of risks. Help develop mitigation plans. Maintain open communication.
Project manager	Identify participants. Review and approve mitigation plans.
Baseline team	Coordinate and conduct all activities. Report results to the project.

Methods and Tools

This table identifies a set of two methods (which use other methods and tools in turn) for conducting an entire baseline event. Detailed descriptions that include alternatives for specific methods and tools are provided in the appendix.

Activity	Methods
Establish a Risk Baseline	Baseline Identification and Analysis [Chapter A-4] Baseline Planning [Chapter A-5]

Note: The SEI Software Risk Evaluation (SRE)[1] is a collection of methods that establishes a baseline set of risks. The SRE structures many of the methods and tools described in **Baseline Identification and Analysis** [Chapter A-4] and **Baseline Planning** [Chapter A-5] into a concentrated timeframe to produce a risk baseline and mitigation strategies. It also includes the use of external expertise to assist in the classification, prioritization, and development of mitigation strategies.

---

1. See [Sisti 94] for a detailed description of the SRE, Version 1. Version 2 is in development.

Section 5

Guidelines and Tips

General

Learn from past experiences with adopting change in the organization.

Get commitment from key stakeholders and make this commitment clear to all groups.

Minimize the conflict between the change and the organization's values, behaviors, and "unwritten rules."

Ensure that transition managers and affected personnel have the skills and motivation to manage the change.

Resistance

Anticipate that there will be resistance that will emerge from all groups affected by the change.

Attempt to elicit or surface and constructively deal with the inevitable resistance.

Establish Sponsorship

Sponsorship of a Continuous Risk Management effort requires public commitment at or above the project manager level.

A change in sponsors requires educating and encouraging the new sponsor(s) or potential sponsor(s) to maintain sponsorship for the implementation effort.

Build Infrastructure

A "risk manager" or a "risk management board" (similar to a change control board) is sometimes used as means of centralizing risk management activities and overhead. However, there is a tendency to rely on that person or board to do all risk management activities, thereby losing the knowledge and expertise of the rest of the personnel on the project. This also violates the premise that risk management, to be effective, must involve everyone.

Conduct Infrastructure Training and Project Familiarization

Basic skills are needed for the project to launch a Continuous Risk Management effort. These skills may already be available in some project personnel; if so, they should be reinforced. If they are not available, appropriate personnel should be chosen to receive the necessary training.

This is only the beginning of training. It is critical that skills are maintained and improved after the **Install** [Chapter 15] phase of Continuous Risk Management is completed. The **Improve** [Chapter 16] chapter discusses this further.

Depending on the size of the project and the number of champions and change agents involved, the project may choose to send out only one or two people for training in the skills of facilitation, team building, and guiding organizational change, and then use the people sent for training as internal trainers to the rest.

Establish a Risk Baseline

Teams can be more effective than individuals.

Don't use too detailed a method for evaluation at this point—many of the risks will not be significant enough to justify the time. Quickly sort the risks to filter out the most important ones.

Capture the context first, then craft a statement of risk, if difficulty is encountered while trying to write a risk statement.

Make sure the consequences, if stated, are specific. The phrase "may impact the schedule" is not adequate.

Don't analyze risks while identifying—identify all issues first, then look for what's currently most important.

Classify to get trends and patterns in the project.

Don't retain control over risks that cannot be mitigated by you; transfer or delegate as appropriate.

Simple mitigation approaches generally work best. Don't use a cannon when a fly-swatter will do.

Trust your instincts and experience and don't forget to think "outside the box" for innovative solutions.

Never take mitigation goals and constraints for granted. Things change.

Make sure all important risks become the explicit responsibility of someone in the project.

Remember that in eliminating or reducing one risk you may introduce others. Consider the consequences of any action when dealing with a set of related risks.

References

Cited in this chapter:

[Sisti 94]   Sisti, Frank J. & Joseph, Sujoe. *Software Risk Evaluation Method Version 1.0* (CMU/SEI-94-TR-19, ADA290697). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

For more information on technology transition, see the following:

[Fowler 93]   Fowler, Priscilla & Levine, Linda. *A Conceptual Framework for Software Technology Transition* (CMU/SEI-93-TR-31). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

[Myers 92]   Myers, Charles R.; Maher, John H.; & Deimel, Betty L. *Managing Technological Change.* Course materials. Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1992. For information about this course, contact SEI Customer Relations at (412) 268-5800 or customer-relations@sei.cmu.edu.

Chapter 15

Install a Basic Risk Management Practice
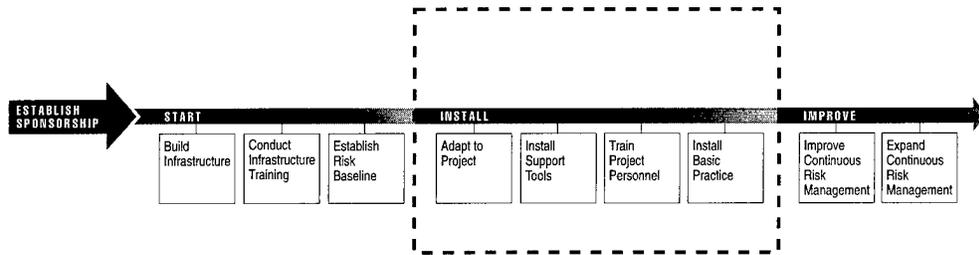
Section

Section 1

Adapt Continuous Risk Management to Project

Description

Having committed to the practice of Continuous Risk Management, and having estab-
lished a baseline set of risks upon which to begin risk management, it is time to make
Continuous Risk Management fit into a specific project organization and culture. The
Adapt Continuous Risk Management activity documents the practice (**Risk Management
Plan** [Chapter A-28]) and determines what basic processes, methods, and tools to begin
using in the project. Further refinement and improvement will occur later, during the Im-
prove phase.

Purpose

The purpose of this activity is to
* make maximum use of existing, effective project management processes and methods
  while integrating a set of proactive risk management activities
* define a set of Continuous Risk Management processes that can be used now
* document the processes in a risk management plan or practice description for the
  project
* define a schedule for implementing or transitioning specific methods, tools, and
  activities into the project

**Key
Considerations**

Key considerations when adapting Continuous Risk Management to a project are
* Continuous Risk Management must be adapted to the organization and project to
  integrate it with existing project management processes and methods.
* As the recommendations of this guidebook are superseded by locally-developed
  approaches, these new approaches should remain true to the principles of Continuous
  Risk Management.
* Define an approach that will work for the project for the next six months to a year, to
  help build momentum for the change.
* Develop a plan for transition or implementation that can be accomplished in small
  steps.

Diagram

The following diagram shows the inputs and outputs for this activity.

CRM = Continuous Risk Management

Procedure

The following table outlines typical steps required to complete this activity.

Step	Action
1	**Establish current state of project practice.** Review the project and the organization with respect to any existing risk management policies, methods, or tools as well as related processes such as project management, configuration control, quality management, problem reporting and tracking.
2	**Evaluate against Continuous Risk Management.** Identify gaps, differences, and similarities between what the project does now and Continuous Risk Management.

Step	Action
3	**Define adaptations and changes.** Adapt existing project management processes and methods to fill the gaps and correct the differences identified in step 2. This includes • customization of Continuous Risk Management processes, methods, and tools for this project • recommendations for changes to project management • templates and reports needed to manage risks • project roles and responsibilities for managing risks
4	**Document adapted risk management practice.** Document the revised processes, methods, and tools to be used in this project. This includes • practice description, or • Risk Management Plan [Chapter A-28]
5	**Refine implementation plan.** Starting with the overall implementation plan developed during the Start phase, refine it by deciding what steps to take, when to take them, and when to put the adapted practice in place within the project, with specific attention to • the basic practice and follow-on improvements and enhancements • roles and responsibilities of managers and key project personnel • which processes, activities, or methods to put in place and when • defining measures of success and how to evaluate them • establishing checkpoints for periodic progress reviews • identifying sources of expertise for consulting during the implementation • identifying and developing mitigation plans for any known risks or barriers to this change
6	**Review plans.** A final meeting of the project manager, champion, change agent, and any other available sources of expertise, is held to assure that there is no misunderstanding about what will happen and how progress will be measured and evaluated.

Roles and Responsibilities

The following table summarizes the roles and responsibilities of personnel during this activity.

Role	Responsibilities
Sponsor	Review recommendations for adaptation and the revisions to the implementation plan.

Role	Responsibilities
Project manager	Review recommendations for adaptation.
	Review and revise implementation and risk management plans.
	Help champion modify the implementation and risk management plans until it they are mutually satisfactory.
	Translate the revised implementation plan into action with champion and change agent.
Champion	Recommend revisions to the implementation plan.
	Review and revise recommendations for practice adaptation and document them in the risk management plan.
	Assure complete common understanding of the adaptations and implementation and risk mitigation plans with the project manager.
	Translate the revised implementation plan into action with project manager and change agent.
Change agent	Assist champion in preparation of the practice adaptation recommendations and implementation and risk management plans.
	Follow the revision of the implementation plan.
	Commit fully to the final implementation plan (as revised).
	Translate the revised implementation plan into action with the project manager and champion.
Facilitation team	Provide Continuous Risk Management expertise during development of practice adaptation recommendations and implementation plan.
	Provide consulting during evaluation of progress.
Project members	Provide information relative to current practice.
	Assist as needed in defining practice adaptations.

Cultural Considerations

Successfully implementing Continuous Risk Management in a project is dependent largely on the organization's culture and recent history, particularly with respect to the application of quality and process improvements. If changes such as total quality management (TQM) or software process improvement (SPI) initiatives have been successfully implemented already, the adjustments for Continuous Risk Management will be minimal.

**Process
Maturity
Considerations**

The level of complexity in the adapted Continuous Risk Management practice may be more ambitious than can currently be supported by the project's maturity level [Paulk 93]. Application of Continuous Risk Management may require more of a staged implementation to achieve a basic level, with a long-range plan for continued improvement and expansion until the target goal is reached. For example, if a project has not reached the point where problems and action items are documented and tracked, formally documenting and tracking risks with a database is too much of a stretch. A paper-based action item, problem, and risk tracking list may be a better starting point.

Section 2

Install Support Tools

Description Continuous Risk Management is an information-intensive practice that is most efficient when supported by tools, particularly automated tools. The most common tool is a database for risk information. Other tools might include risk analysis tools, report generators, and trend analysis tools. The simplest, non-automated tool is a blank paper form for recording risk information. All tools, even non-automated tools, need to be defined before beginning risk management, although automation can be phased in.

Purpose The purpose of this activity is to make sure that project personnel will have the tools they need before they begin to try to manage risks.

Note: It is useful to have some kind of tool used during the *Establish a Risk Baseline* activity to ensure the resulting information can be easily transferred or automated.

Key Considerations Key considerations when installing support tools are
- Tools should be in place before activity begins.
- Tool maintenance and training should be provided.

Diagram The following diagram shows the inputs and outputs of this activity.

Procedure The following table outlines the typical steps required to complete this activity.

Step	Action
1	**Evaluate existing tools against the needs for risk management**. It is generally easier and less expensive to adapt known, existing tools to manage risks than acquire a completely new set. Weigh the return on investment carefully. If this will be an organization-wide improvement activity, investment in specific tools may be worthwhile.

Step	Action
2	**Investigate other tools**. Where requirements cannot be met by existing tools, evaluate what is available on the market or from other internal sources within the organization and determine what can be used.
3	**Acquire necessary tools and maintenance contracts**. Contract for or purchase tools, including maintenance contracts.
4	**Adapt existing tools**. Where existing tools are being used, adapt or modify them to meet the needs of Continuous Risk Management. Database reports for example, may need to be modified to include risk information.
5	**Acquire or develop tool training**. Purchase or develop tool training for the project. A refresher course may be needed for existing tools.

Roles and Responsibilities

The following table summarizes the roles and responsibilities of personnel during this activity.

Role	Responsibilities
Sponsor	Approve and fund plans for new tool acquisition if these will support multiple projects.
Project manager	Approve plans and funding for new tool acquisition and modification for existing tools.
Champion	Evaluate existing tools with change agents.
	Review recommendations for new tool acquisition and modifications of existing tools.
	Review recommendations and plan with the project manager.
Change agent	Work with champion in evaluating existing and new tools.
	Make recommendations for tool modifications or purchase.
Facilitation team	Develop and conduct tool training sessions.

Section 3

Train Project Personnel

Description

Once the adapted practice is defined, project personnel need to be trained in how to accomplish the Continuous Risk Management activities. While generic training can be acquired from sources external to the project or organization, tailored training for the specific adapted practice will likely have to be developed. Training can be provided on an as needed basis, tied to the implementation plan. The extent of training needed will vary with each project. If good project management skills and methods are in place and routinely used, adding risk management requires less training.

Purpose

The purpose of this activity is to make sure that the project personnel understands their roles in Continuous Risk Management:
- what activities are to be performed
- by whom
- using what methods and tools
- what to do with the results

Key Considerations

Key considerations when training project personnel are
- Train personnel in the processes, methods, and tools before they begin using them.
- Train personnel on where they fit into the whole practice.
- Train project personnel on the principles, not just the steps.

Diagram

The following diagram illustrates the inputs and outputs of this activity.
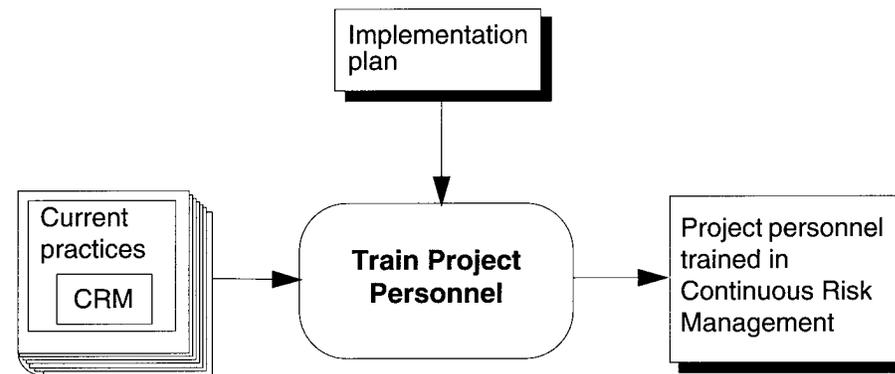
Procedure

The following table outlines the typical steps required to complete this activity.

Step	Action
1	**Develop training materials**. Develop or tailor Continuous Risk Management and tool training to meet the needs of the project. External sources of training material can be used but are likely to need adaptation.
2	**Define training schedule**. Identify who needs what training and when. Training the whole project all at once is not necessary. Training should support the implementation plan.
3	**Conduct training**. Follow the training schedule.
4	**Improve training as required**. Gather feedback from personnel and improve the training as needed.
5	**Provide refresher training**. New personnel and project personnel who need to be reminded of the practice should receive training.

Roles and Responsibilities

The following table summarizes the roles and responsibilities of personnel during this activity.

Role	Responsibilities
Sponsor	Provide funds for training courses, especially courses or material to be used for multiple projects.
Project manager	Approve and fund training schedule. Require attendance at training sessions. Make sure personnel schedules have adequate time allocated for training.
Champion	Prepare training schedule plan with change agents. Review plan with the project manager.
Change agent	Work with champion to prepare of the training plan. Conduct or observe training sessions.
Facilitation team	Conduct training sessions (optional).
Project members	Attend training sessions. Provide constructive feedback on the adequacy and effectiveness of the training.

Section 4

Install a Basic Practice

Description   Once the Continuous Risk Management practice has been adapted and defined, the supporting tools installed, and project personnel trained, the basic practice can be installed and personnel can begin performing the activities. The basic practice, as used here, refers to the minimum set of risk management activities defined in the implementation plan to accomplish risk management. As with any improvement effort, start simple, get the culture in place, and then improve.

Purpose   This activity addresses getting a basic set of activities in place to support all phases of the risk management paradigm:
- identify
- analyze
- plan
- track
- control
- communicate

Key Considerations   Key considerations when installing a basic practice are
- The baseline set of risks is only those risks known at that time—new risks will continue to be identified after that.
- The project must become "risk aware" and cease to ignore risks before risk management can be fully realized.
- Start with simple methods to identify new risks, analyze them, develope mitigation plans, track and control risks, and communicate about risks.
- Add improvements and more complex processes, methods, and tools later.

Diagram   The following diagram shows the inputs and outputs for this activity.

Procedure

The following table outlines the typical steps required to complete this activity.

Step	Action
1	**Review the basic practice.** Review the basic Continuous Risk Management practice description in the implementation plan.
2	**Set up checkpoints to review progress.** Determine the frequency of progress review for implementation of the basic practice. Identify success criteria for review at those checkpoints.
3	**Follow implementation plan.** Add risk management activities to the project's operations according to the plan.
4	**Review and revise plan as needed.** At the checkpoints, review progress and success of the implementation plan. Where difficulties exist, the facilitation team and champion should provide assistance in getting the risk management activities in place or in making additional adaptations.

Roles and Responsibilities

The following table summarizes the roles and responsibilities of personnel during this activity.

Role	Responsibilities
Project manager and sponsor	Continue to provide encouragement. Monitor implementation plan progress and reward success.
Project personnel	Add risk management activities into project operations according to the plan. Ask for help rather than abandoning the practice when problems arise.
Champion and facilitation team	Provide inspiration and encouragement. Assist in further adaptations of the processes, methods, or tools as needed. Monitor and evaluate progress and report to project manager.

Section 5

Guidelines and Tips

General

Do what's necessary to get started; don't get bogged down in trying to build a perfect procedure and forget about the risks.

Document and retain all decisions and information.

Use paper to start with if it will take too long to get a database started—recognize that it is time-consuming to transition from paper to electronic.

A corporate-wide database provides the best opportunity for sharing costs and gaining the benefits of lessons learned and risk trend analysis.

The *Install* activities can be done in almost any order, even concurrently—the key is to minimize the passage of time after establishing the baseline set of risks before beginning this phase.

Formal methods can come later—it is important to establish the habit or routine as early as possible.

Adapting the Processes

Enlist project personnel in the definition of the risk management processes. They will put more into the processes and the practice of them if they own them.

Install Basic Practice

Personnel responsible for risks should start with verbal status reports to become accustomed to reporting on their risks.

Begin by setting a scheduled time period in project meetings to open the floor to new risks.

The existing list of risks can serve as an inspiration simply by being reviewed.

It is important not to get caught up in a "numbers game" where the quantity of risks being managed and closed becomes more important than the effectiveness of the project in dealing with major risks.

References

Cited in this chapter:

[Paulk 93]   Paulk, Mark; Curtis, Bill; Chrissis, Mary Beth; & Weber, Charles V. *Capability Maturity Model for Software, Version 1.1* (CMU/SEI-93-TR-24, ADA263403). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

For more information on technology transition, see the following:

[Fowler 93]   Fowler, Priscilla & Levine, Linda. *A Conceptual Framework for Software Technology Transition* (CMU/SEI-93-TR-31). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

[Myers 92]   Myers, Charles R.; Maher, John H.; & Deimel, Betty L. *Managing Technological Change*. Course materials. Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1992. For information about this course, contact SEI Customer Relations at (412) 268-5800 or customer-relations@sei.cmu.edu.

[Radice 94]   Radice, Ron & Garcia, Suzie. *An Integrated Approach to Software Process Improvement (SPI)*. Tutorial presented at the Software Technology Conference, April 1994, Salt Lake City, Utah. For information about this tutorial, contact The Utah State University, Continuing Education/Conferences at (801) 797-0423.

Chapter 16

Improve and Expand Continuous Risk Management
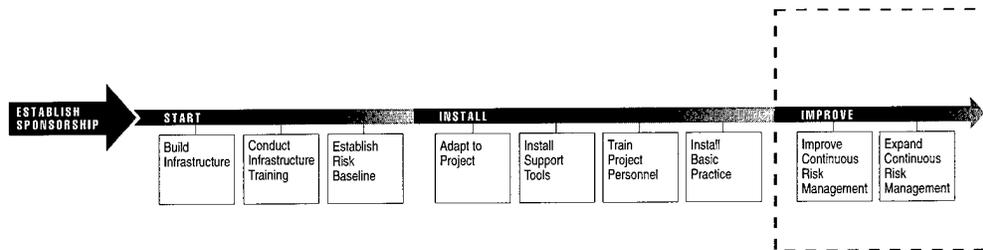
Section 1

Improve Continuous Risk Management

Description

The end goal of establishing Continuous Risk Management in a project is to integrate routine risk management activities into routine project practice. Managing risks is not a stand-alone practice; it is an integral part of project management. Risk identification, analysis, planning, tracking, control, and communication must be established as continuous activities by all project personnel to be effective. Improvements to add needed complexity or formality, to better match routine project management practice, to increase efficiency of risk management activities, and to increase the forward-looking viewpoint (look further ahead) are key elements in making Continuous Risk Management more effective.

Purpose

The purpose of this activity is to improve the basic Continuous Risk Management practice implemented during the **Install** [Chapter 15] phase.

Example: In a culture where risks are not openly discussed or communicated, where risks are ignored or people fear to bring up issues without resolutions, the anonymous aspect of identifying risks (submittal of risk forms) may be the best alternative with which to start. As the project becomes more attuned to and comfortable with dealing with risks, new risks can be reported more openly as a routine part of everyone's standard progress report.

Key Considerations

Key considerations when improving Continuous Risk Management are
- Risk management must eventually be integrated into project management for maximum effectiveness; as a separate activity, it is too easily overlooked.
- Continuous improvement is a mark of a mature project.
- Organizations and projects are dynamic—change must be viewed as a normal part of the environment.
- Nothing is perfect the first time; expect to make changes to the basic practice.
- During the *Install* phase, project personnel are more likely to identify near-term risks and only mitigate the top N risks; as they improve, they will see risks that are far-term and be able to deal with more than just the top N.
- Delegation is a powerful tool for empowering risk management within all levels of the project.

Diagram   The following diagram shows the inputs and outputs for this activity.

CRM = Continuous Risk Management

Procedure   The following table outlines typical steps required to complete this activity.

Step	Action
1	**Maintain continued sponsorship.** Make sure the sponsorship that has existed for the implementation of Continuous Risk Management continues. Ensure that sponsors and champions understand what is required of them to help maintain momentum.
2	**Identify periodic checkpoints.** Determine when to review progress, lessons learned, and issues. Measures of success should be identified to help evaluate progress at those checkpoints.
3	**Document and heed lessons learned.** Document lessons learned as the project and change effort proceed. Re-evaluate those lessons periodically and select improvements that should be made on this project and its processes, methods, and tools.
4	**Provide continued coaching or consulting.** The facilitation team should continue to periodically coach the project by providing • expertise on Continuous Risk Management as adapted to the project • facilitation, as needed, for specific methods or meetings • evaluation of progress • revisions to adapted Continuous Risk Management processes, methods, and tools • instruction on new methods and tools • training, refresher courses, familiarization for new personnel • support for sponsors and champions • "lessons learned" from other projects

Step	Action
5	**Review effectiveness of support tools**. Review how useful the database reports are, how easy the tools are to use, and so on. Look for • improvements in the tools • changes that can be made to support process improvements • additional uses for the tools

Roles and Responsibilities

The following table summarizes the roles and responsibilities of personnel during this activity.

Role	Responsibilities
Project manager and technical managers	Continue to provide commitment and required resources. Support open communication. Reward effective management of risks.
Sponsors	Continue to provide visible support and reward for performance of Continuous Risk Management activities and results.
Champions	Encourage project personnel involvement. Make successes visible. Coordinate improvements and changes.
Change agents and facilitation team	Coordinate refresher and new training for project. Support sponsor and project manager. Provide continuous consulting and expertise to project. Coordinate changes to adapted Continuous Risk Management processes, methods, and tools.
All project personnel	Identify, analyze, plan, track, control, and communicate risks.

Section 2

Expand Continuous Risk Management

Description

Once routine processes for Continuous Risk Management have been established in a project, risk management can be expanded to other projects within the organization and an organization standard for risk management can be developed. A project that has successfully implemented risk management will stand as a model for other projects. Communication about risks will have raised the awareness in the organization.

Purpose

The purpose of this activity is to enable the expansion of risk management to other projects in the organization.

Key Considerations

The methods and tools identified in this document can be tailored to match the particular needs of an organization's current processes. As risk management becomes more routine and the organization's culture more risk aware, the methods being used to manage risks can be adapted to other projects.

Diagram

The following diagram shows the inputs and outputs for this activity.

CRM = Continuous Risk Management

Procedure   The following table outlines typical steps required to complete this activity.

Step	Action
1	**Increase awareness.** Use formal and informal means to increase awareness of risks and risk management processes throughout the organization. Reporting risks to senior managers at multi-project meetings is one example. Generation of progress reports for organization review is another alternative.
2	**Stand as an example.** The project that successfully implements and makes use of risk management to help deliver a system on time and within budget will be a good model for other projects.
3	**Make rewards visible to organization.** Sponsors and senior managers should publicly recognize and reward successful risk mitigation efforts.
4	**Refine practice into an organization standard.** As other projects begin to implement Continuous Risk Management, continue to refine and adapt the risk management practice description until an organization standard or recommended practice exists. This will give other projects a target to aim for.

Roles and Responsibilities

The following table summarizes the roles and responsibilities of personnel during this activity.

Role	Responsibilities
Project manager and sponsor	Report successes and failures to senior managers.
All project personnel	Communicate informally about what works and does not work in risk management with other projects.
Other projects	Consider implementing risk management.
	Review existing practice description and determine the degree of adaptation that might be needed.
	Contact facilitation team members and change agents for help.
Change agents and facilitation team members	Report successes to senior management
	Communicate informally and formally about risk management
	Coordinate the collection, documentation, analysis, and reporting of "lessons learned"
	Coordinate changes to adapted Continuous Risk Management practice for use on an organizational basis

Section 3

Guidelines and Tips

General

Periodic or continuous review of the effectiveness of the processes, methods, tools, and products being used should point the way towards improvements.

To reinforce the performance of risk management, management (both project and senior level, including sponsors) should ask for an evaluation of significant problems to determine whether or not they could have been foreseen and mitigated.

Continued sponsorship is required—it takes time for risk management (or any change) to become routine. Any break in sponsorship and encouragement allows project personnel to backslide; recovery will be difficult after that.

Reward Risk Management

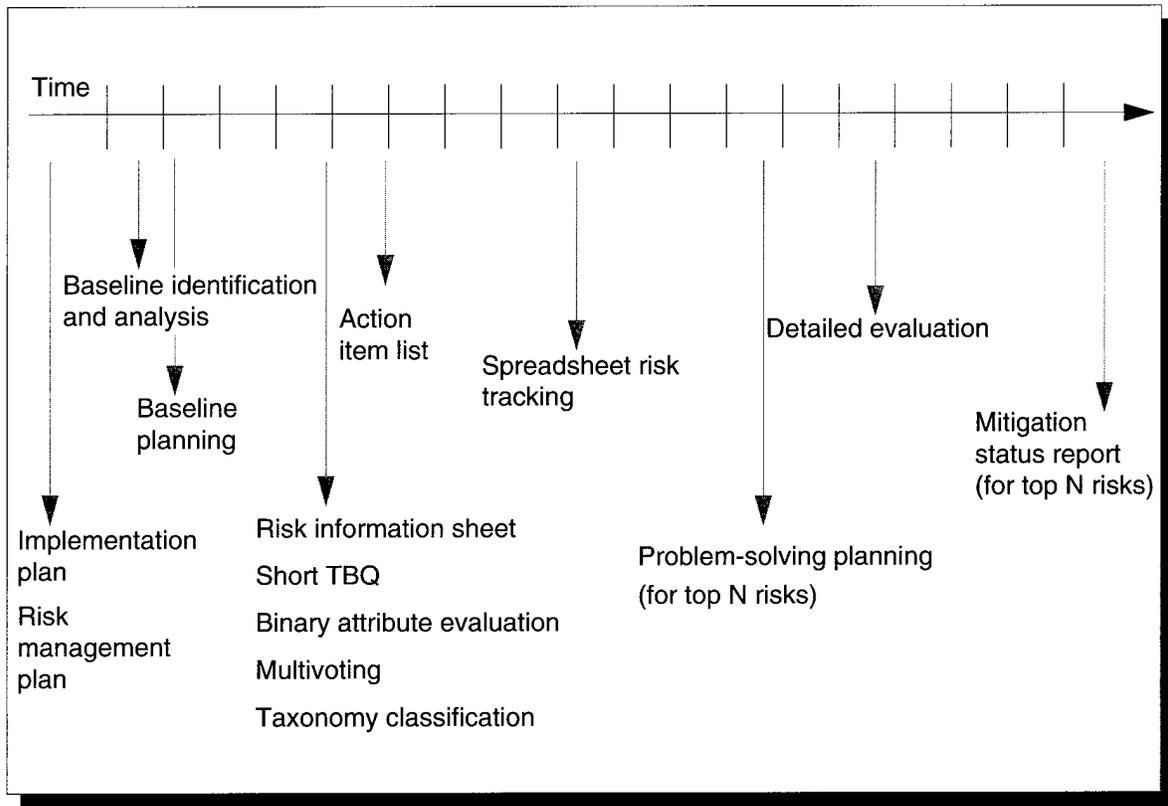Make sure that what is rewarded within the project includes risk management. For example, if problem solvers are rewarded, but not problem avoiders (i.e., those who manage their risks), there is little incentive to identify risks and mitigate them.

Reward the performance of risk management by publicly acknowledging the successful mitigation of significant risks on projects to the rest of the organization.

Chapter 17

Transition Scenario

Time

Baseline identification
and analysis

Action
item list

Baseline
planning

Spreadsheet risk
tracking

Detailed evaluation

Mitigation
status report
(for top N risks)

Implementation
plan

Risk
management
plan

Risk information sheet

Short TBQ

Binary attribute evaluation

Multivoting

Taxonomy classification

Problem-solving planning
(for top N risks)

Section 1

Overview

What's in This Scenario?

This is a "precursor" of the example implementation described in Part 3, which provided a vision of successful Continuous Risk Management in the ABC Project. Here, the steps by which that vision became reality are described. This scenario will follow the same steps outlined in the previous chapters and show how Project ABC, and, eventually, how its parent organization, RST, Inc., institutionalized Continuous Risk Management.

Background

RST, Inc. has been working to improve its software engineering practice for about two years. Personnel are encouraged to find not only proven technology, but also promising or emerging technologies that might help RST, Inc. get ahead of its competitors. Their culture encourages change, although the sponsorship is sometimes erratic and crises still tend to dominate and overtake many of their improvement efforts.

Who's Who

The following organization chart illustrates the players in this scenario, and their role within the company and project.

Project ABC Organization Chart
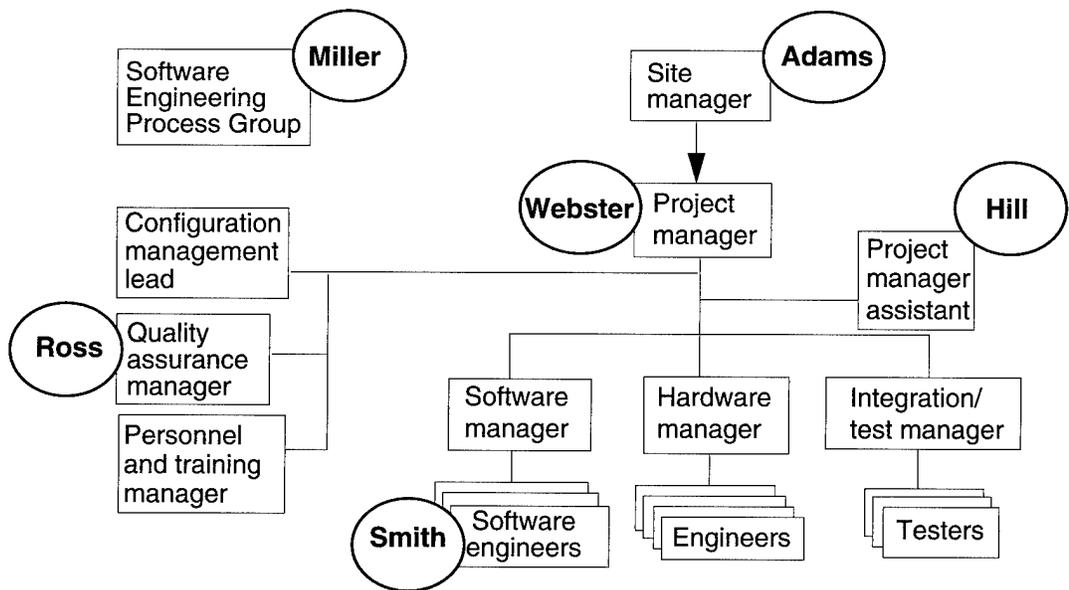
Why Risk Management?

One of Project ABC's customer requirements was a risk management practice (or process, as it is sometimes referred to by customers). There were, however, no specific requirements for what this process might entail and only minimal effort was ever put into this activity. In fact, the proposal team spent a half an hour brainstorming a list of three big risks, described how they were avoiding them through their design and test processes, and then forgot about them. Miller, from the Software Engineering Process Group (SEPG), has talked to site manager Adams about putting a more formal Continuous Risk Management practice in place in RST, Inc.'s projects. He pointed out that their chief rival made a presentation last year at a major conference about their risk management process and how it was helping them improve their business. Adams has called Webster in and asked if they could use the ABC Project as a pilot test. Webster, wanting to do a better job of meeting the spirit of the customer's requirements, agrees. The incentive to change, for this scenario, is both external and internal to the project.

Section 2

Getting Started

Motivation

Webster, the project manager, talks to the Software Engineering Process Group representative, Miller. They decide to gather information, evaluate it, and then set up a group of experts and resources to help them put Continuous Risk Management in place in the project as soon as possible.

Gather Information

Smith, a senior software engineer, is assigned the task of working with Miller to evaluate the following information about risk management:

- available experts (internal or external)
- documented processes, methods, and tools
- cost-benefit data
- "lessons learned" and case studies from projects that have successfully implemented and used Continuous Risk Management.

Present Information

Smith and Miller spend two weeks evaluating several reference books, a lot of articles from conferences, and information on the World Wide Web. They also talk to several external experts who would be willing to consult with RST, Inc., including one they've worked with many times before and can be brought on board very rapidly. Smith and Miller propose to get an outside consultant to come in and help them get the started on Project ABC, and then use that experience to get other projects up to speed.

Make the Decision

Webster and Adams liked the proposal and have heard good things about the external consultant, so the consultant is brought in to start working on an implementation plan and provide guidance for a **Risk Management Plan** [Chapter A-28].

Implementation Plan

The implementation plan calls for the following milestones:

- *within two weeks*: Identify and train infrastructure members, inform project, establish baseline set of risks.
- *within the next month*: Adapt Continuous Risk Management to the project, document a risk management plan, refine the implementation plan with details, install required tools, train project personnel, and get started performing the basic practice.
- *within the next six months*: Fully implement practice and revise as necessary.
- *ten months after the effort begins*: Evaluate this pilot and make a final set of recommendations for risk management within the organization.

Inform the Project

In the meantime, project personnel are informed by Adams and Webster that they will be putting a new practice in place with this project, and that more information will be supplied later. The managers emphasize that they know it will be a short-term burden on everyone to get this practice going, but they also promise to reward success.

Infrastructure

Adams, Webster, and Miller decide the following infrastructure is needed:

- *sponsors*: Adams and Webster
- *change agent*: Miller
- *facilitation team*: Miller leads the team, adding one more member from the SEPG as well as the external consultant.
- *champion*: Hill, the assistant project manager, is very enthusiastic about the risk management initiative, having seen it used by a competitor to their advantage. Hill volunteers to be the champion.

Baseline Team

The consultant recommends they establish a baseline set of risks as soon as possible. This will bring an awareness of risk to the project team and help them get going with the improvement effort. A baseline team (a subset of the facilitation team) is identified to lead this activity.

Training and Familiarization

The consultant is brought in to train the project manager, champion, and facilitation team in risk management concepts, principles, and the general processes. The baseline team is trained in the methods and tools for establishing the baseline. Familiarization on the general concepts is provided for the rest of the project team and Adams. The facilitation team is trained to assist with the establishment of the baseline set of risks, and will be expected to act on their own in re-establishing the baseline at later, significant points in the project schedule.

Establishing a Baseline Set of Risks

The consultant and facilitation team lead the project through the **Baseline Identification and Analysis** [Chapter A-4] and **Baseline Planning** [Chapter A-5] activities. The resulting set of risks were classified into related groups, evaluated for probability, impact, and timeframe, and then ranked to identify the top 14 risks. Finally, mitigation plans for the top 14 risks were developed.

Section 3

Installing

Addressing the Top N Risks

Using the consultant's recommendations, Webster and Hill decide to have the top N risks reported on every week during their project status meetings. Hill gets Ross, the quality assurance person, to add the top N risks to his action item database so they can have some record of what they're doing while other support tools are built. During the first weekly project meeting, Webster assigns responsibility for each top N risk to someone in the team to implement the plan and report on progress.

Adapting Continuous Risk Management

The consultant, Miller, and Hill begin working on a Continuous Risk Management standard practice adapted to the ABC project and RST, Inc. They use four focus groups of project personnel to compare the Continuous Risk Management processes, methods, and tools to what they're already doing for project management:

- weekly project meetings
- written team status reports
- project, problem, and action item databases
- formal task plans for major tasks as well as the project plan

With this information, Miller, Hill, and the consultant develop a draft standard practice description and integrate it into a **Risk Management Plan** [Chapter A-28]. The members of the four focus groups review and comment on the draft plan. Their comments are included in the final version, which is reviewed and approved by Webster. Miller, Hill, Webster and the consultant decide which activities will be in the basic process and when to install them. The implementation plan is revised with details addressing the implementation of the specific activities and tools.

Basic Practice

The basic practice is defined with a simple process/data flow. Task assignments are then made. At this point, the intention is to only deal with top N risks and ignore the rest, although the consultant has vigorously disagreed with that limitation.

Who Does What?

The following diagram illustrates the *initial* concept for who would perform specific risk management tasks.
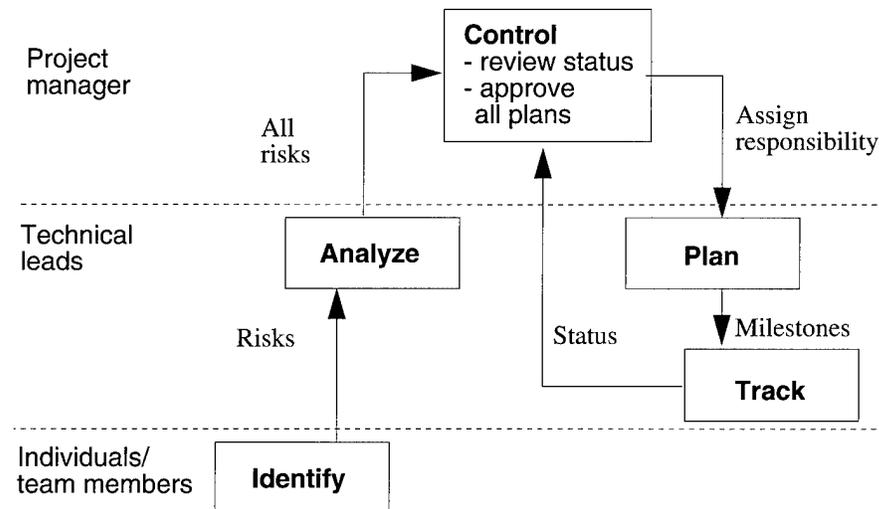
Task Descriptions

The tasks associated with the previous diagram, as envisioned at this point, are described in the following table. All activities will take place during the weekly project meetings, which will be lengthened to include these activities.

Who	What
Individuals or team members (anyone on the project)	Identify new risks during the weekly meetings and are prepared to discuss them.
Technical leads	Evaluate and prioritize all risks, develop mitigation plans, and report status.
Project manager	Review status reports, assign responsibility for risks and approve all mitigation plans.

Methods and Tools

The following table identifies the basic set of methods and tools that the ABC project will start with.

Purpose	Method or Tool
Risk documentation	Risk Information Sheet [Chapter A-27] and a database built from that sheet
Identification	Short TBQ [Chapter A-29] as a prompt for open discussion during the weekly meeting
Analyze	Binary Attribute Evaluation [Chapter A-6] Multivoting [Chapter A-17] Taxonomy Classification [Chapter A-34]
Plan	Action Item List [Chapter A-1]
Track and control	Updates to risk information sheet to report status on all top N risks and mitigation plans on a weekly basis

Support Tools

Ross, in quality assurance, keeps the project database. He is tasked with building a database for the risk information and maintaining it. This only takes one week to bring online; however, Ross is the single point of contact for getting information in or out. One report format, the risk information sheet, is built to document a risk.

Train Project Personnel

Since all of the activities are to take place during the weekly meeting, one meeting is set aside for training in the new processes and use of the risk information sheet. The training goes well, but many project team members are a bit skeptical.

Monitoring the Installed Basic Practice

Miller and the consultant attend the weekly meetings to evaluate progress and deal with any issues, including resistance on the part of project personnel.

Section 4

Improving and Expanding

Week 1

At the first weekly meeting, Webster ensures that someone is assigned to all the top N risks and asks how things are going on the mitigation plans. Progress is slow, because responsibility was not always clear after the baseline was established. No one has any new risks to bring up. Project personnel are largely taking a "wait-and-see" attitude.

Week 4

Two of the mitigation plans have been completed and progress is being made, but two of the software engineers have been identifying a lot of risks at the meetings. This is causing the meetings to exceed their allocated time due to increased conversation. Decisions are not being made due to the need for more information. Miller and the consultant decide to give it two more weeks to see if things improve.

Week 6

Frustration is starting to build as more risks are identified than can be handled during this meeting. There isn't enough time to discuss, evaluate, prioritize, develop plans, and report progress on the risks and still get the rest of the meeting's agenda accomplished. Miller and the consultant recommend some immediate process changes:
- Identify and document new risks off-line and submit them as read-ahead before the meeting.
- Require the originator to make an initial evaluation of the probability, impact, and timeframe and determine a classification.
- Allow only critical risks to be raised in the meeting without prior documentation.
- Review the evaluation and classification during the meeting only if the technical leads disagree with the evaluation results and risk classification.
- Limit discussion of possible mitigation strategies to five minutes per risk.

Week 9

The changes have made the weekly meetings easier to bear. Project personnel had a little trouble with the evaluation, but the project manager provided recommended schedule and budget ranges to define likely, significant, near-term, and critical. This helped the evaluation process considerably. A critical risk was defined as a likely, significant, near-term risk that may cause the project to fail if not mitigated.

With the evaluation being done before the meeting, only the important risks (all yes's from binary attribute evaluation) are being discussed and assigned responsibility. Discussion of possible mitigation strategies still tends to exceed the allotted five minutes.

Week 15

More refinements have been made:
- All mitigation discussion is done off-line with the responsible person and other required personnel.
- Only the final (not proposed) mitigation plans (documented as an action item list) are brought back for approval.
- Success measures for the mitigation action items are now required, after two mitigation plans failed when the planner and the project assumed success because the actions were completed, but didn't really check to see if the risk was, in fact, gone.
- A **Spreadsheet Risk Tracking** [Chapter A-30] report is now used to summarize progress information for the top N risks and handed out as read-ahead.

Week 22	One of the non-top N risks, identified during the baseline, has turned into a problem that is significantly greater than believed during the baseline. This has impacted the schedule and is making the company look bad to the customer. Miller talks to the consultant, who reminds them, gently, that they decided to ignore the rest of the risks against the consultant's recommendations. The lesson is learned and all non-top N risks are re-evaluated/re-prioritized once a month for significant changes in importance.

Week 35	At Webster's request, Miller, Hill, and the consultant sit down and evaluate the processes being used and make a final set of recommendations for process improvements, including those that may not be appropriate for ABC Project, but might be useful for RST, Inc. as a whole.

Several top N risks have required more detailed estimates of probability and impact. The consultant works with Miller and Hill to adapt the Air Force's Pamphlet 800-45 [Air Force 88] to RST, Inc. Two of these risks also had very complicated, long-range mitigation plans with several contingency plans for specific triggers. **Problem-Solving Planning** [Chapter A-24] is required for complex risks. Webster had difficulty trying to evaluate and follow mitigation progress for these risks. The **Mitigation Status Report** [Chapter A-16] is to be used for complex risks to provide the project manager with a better view of what is going on.
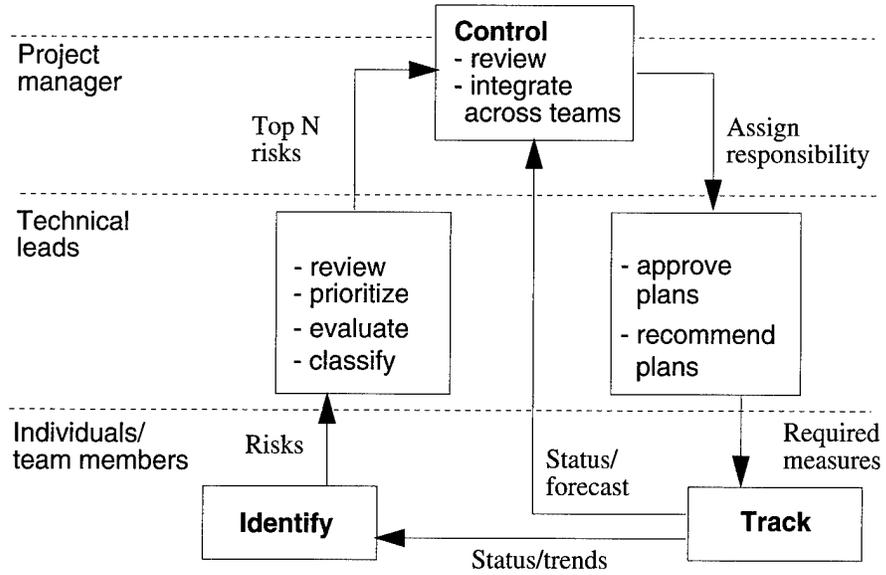
Final Recommendations

The final processes put in place for this project are summarized below, and have already been explained in detail in Part 3. Other recommendations were also made by the consultant. These were

- Use task plans for significant risks whose impact exceeds 5% of the total project budget.
- Increase the use of trends across projects to look for future areas of improvement for the company (e.g., testing schedules are always cropping up as critical risks—perhaps their scheduling methods need improvement).
- Use a higher level or more detailed level of attribute evaluation (based on [Air Force 88]) for the top N risks that exceed a specified range of cost impact to the project.
- Use **Mitigation Status Report** [Chapter A-16] for any risk with a complicated mitigation plan where the project manager wants special insight into progress.
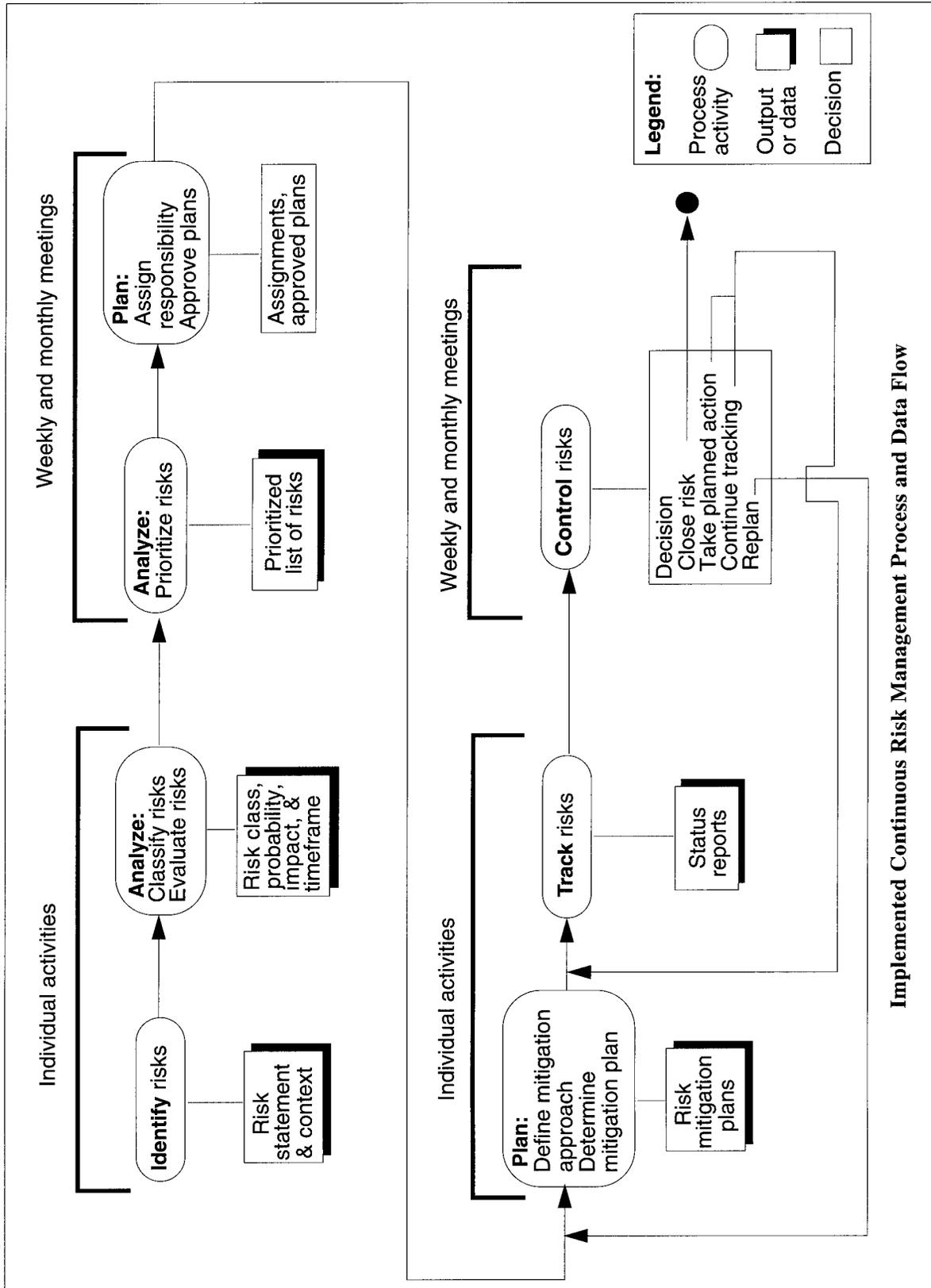
Final "Who Does What?"

The internal communication framework diagram on the next page shows the final allocation of responsibility for activities defined for this project.

```
Project                                    ┌─────────────┐
manager                                    │ Control     │
                                           │ - review    │
                                           │ - integrate │
                              Top N        │   across    │      Assign
                              risks        │   teams     │      responsibility
                                           └─────────────┘

Technical                    ┌──────────────┐           ┌──────────────┐
leads                        │ - review     │           │ - approve    │
                             │ - prioritize │           │   plans      │
                             │ - evaluate   │           │ - recommend  │
                             │ - classify   │           │   plans      │
                             └──────────────┘           └──────────────┘

Individuals/        Risks                      Status/        Required
team members                                   forecast       measures
                    ┌──────────┐                          ┌──────────┐
                    │ Identify │                          │  Track   │
                    └──────────┘      Status/trends       └──────────┘
```

Final Process and Data Flow

The diagram on the following page shows the final high level process and data flow developed for this project.

Legend:

Process activity

Output or data

Decision

Weekly and monthly meetings

Plan:
Assign
responsibility
Approve plans

Assignments,
approved plans

Analyze:
Prioritize risks

Prioritized
list of risks

Individual activities

Analyze:
Classify risks
Evaluate risks

Risk class,
probability,
impact, &
timeframe

Identify risks

Risk
statement
& context

Weekly and monthly meetings

Control risks

Decision
Close risk
Take planned action
Continue tracking
Replan

Individual activities

Track risks

Status
reports

Plan:
Define mitigation
approach
Determine
mitigation plan

Risk
mitigation
plans

Implemented Continuous Risk Management Process and Data Flow

Final Words:
It Takes Time
to Change

Installing a new technology or practice is never easy, and many improvement efforts fail. The ABC Project had many difficulties, but they persevered and helped to establish an effective risk management practice for RST, Inc. while improving their own project.

Success did not come instantly, there were barriers to overcome, errors in judgement made, and wrong decisions to correct.

While an external consultant was used initially, there is now a good base of experienced personnel in RST, Inc. who can act as internal consultants. The external consultant can be phased out as internal expertise solidifies or the external consultant can help on later improvements and new methods.

References

Cited in this chapter:

[Air Force 88]   Air Force Systems Command/Air Force Logistics Command Pamphlet 800-45. *Software Risk Abatement*, September 30, 1988.

Chapter 18

Summary
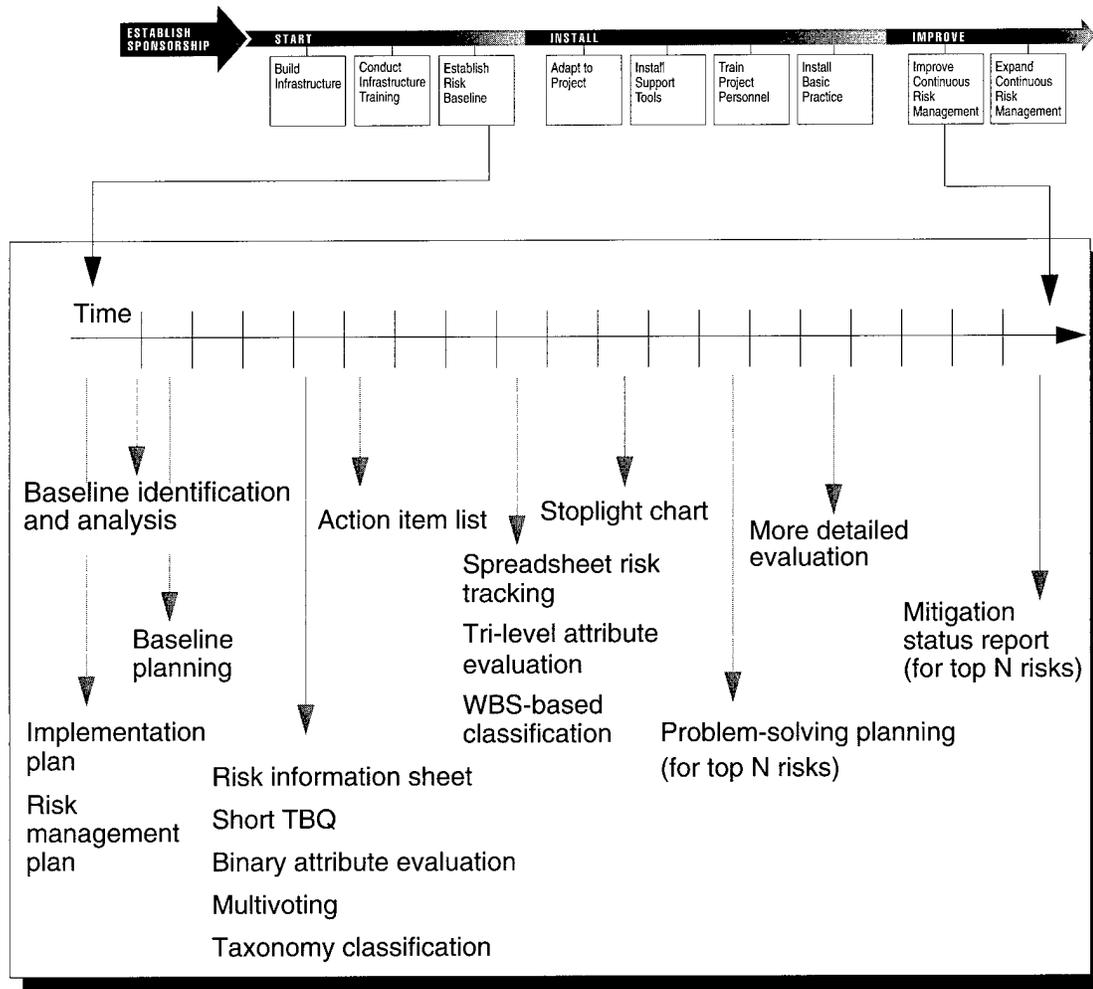
Section 1

The Application Roadmap Reprised

Why a Roadmap?

The roadmap (below) provides guidance to those who would implement Continuous Risk Management. Precise adherence to the order of events is not required as long as all of the activities are accomplished. In some cases, for example, *Adapt to Project* can occur first, before *Establish Risk Baseline*.

The roadmap is a tool, a guide, not a dictated standard.

Summarizing the Activities

The following is a summary of the necessary activities:

- *Establish Sponsorship*: Support, encourage, and reward successful improvement (required for success).
- *Build Infrastructure*: Identify all the critical roles for implementation and coaching and fill those roles.
- *Conduct Infrastructure Training*: Ensure infrastructure personnel are sufficiently trained and ready to perform their duties.
- *Establish Risk Baseline*: Find all the currently existing risks, analyze them, and build mitigation plans for the Top N.
- *Adapt to Project*: Adapt Continuous Risk Management to the project.
- *Install Support Tools*: Provide the tools needed to support the processes.
- *Train Project Personnel*: Train the project in the processes, methods, and tools.
- *Install a Basic Practice*: Begin simple until risk is instilled in the project culture.
- *Improve Continuous Risk Management*: Improve the processes, methods, and tools to meet the project's needs.
- *Expand Continuous Risk Management*: Add this practice to other projects in the organization.

Sample Timeline of Methods

The following diagram shows a possible timeline of methods and tools as they are introduced and used during this practice. This is not a specific recommendation, only an illustration of how different methods can be introduced.

Time

Baseline identification and analysis

Action item list   Stoplight chart

More detailed evaluation

Spreadsheet risk tracking

Baseline planning

Tri-level attribute evaluation

Mitigation status report (for top N risks)

WBS-based classification

Implementation plan

Problem-solving planning (for top N risks)

Risk information sheet

Risk management plan

Short TBQ

Binary attribute evaluation

Multivoting

Taxonomy classification

Tips for Applying Continuous Risk Management

The primary lessons learned from the efforts to apply risk management are these:

- Start simple.
- Learn to "think risk."
- Look slightly ahead first, and deal with those issues and risks.
- As time progresses, force yourself to look further and further ahead.
- Never throw out or ignore any information; scan it once in a while.
- Don't hesitate to abandon a method or tool after a fair trial and use something different.
- Always ask for feedback on how things are going and what works.
- Use outside facilitators until the project is comfortable with the practice and you are sure that open communication is firmly established.

Common Risks

There are risks that are common to any type of improvement endeavor, such as applying Continuous Risk Management [Radice 94]:

- insufficient sponsorship, especially senior managers
- resistance by middle managers (e.g., project managers)
- lack of motivation for improvement or change
- inadequate resources allocated to the effort
- inappropriate goals
- termination of activities before the practice is institutionalized
- lack of sustained focus on improvement

These are risks that need to be avoided or mitigated in order to be successful at implementing improvements such as Continuous Risk Management.

Section 2

Considerations for Organizations and New Projects

Organizations

Organizational improvement can be sponsored on a project level or on an organizational level. Part 4 dealt with applying Continuous Risk Management by starting with a project and using that success to motivate organization-level improvement. When an organization decides from the beginning to implement Continuous Risk Management across all projects, a variation on the application practice is used. Reaching a level of consistency and quality across all projects requires more effort to determine what the core set of common processes, methods, and tools are for the organization as well as what project-specific variations are permissible.

Commitment and Sponsorship

For organization-level change, sponsorship and commitment must come from the top managers and be reinforced downwards throughout the management chain. Process improvement groups and other project-independent consultants can be used as a common source of expertise and coaching to help establish and monitor risk management practice in each project.

Start

The activities in the *Start* phase are different and occur in a different order when implemented in organizations:
- Build infrastructure.
- Conduct infrastructure training.
- Adapt to project (preliminary adaptation of Continuous Risk Management to the organization).
- Install support tools.
- Select pilot projects and define project specific implementation plans.

Install

The *Install* activities should be the same within each pilot project:
- Establish risk baseline.
- Train project personnel.
- Install basic practice.

Improve

Within each pilot project, there is one *Improve* activity:
- Improve continuous processes, methods, and tools.

The consulting staff would monitor progress in each pilot until a good cross-section of pilots is successfully performing Continuous Risk Management. At that time, any refinements and improvement to the organization's practice standard are completed (the final adaptation of Continuous Risk Management). As with any project practice, a change procedure is put in place to manage future improvements and changes to the established standard.

Application Costs

The costs and required resources for applying Continuous Risk Management can be intimidating. When starting with an organization-wide application, these costs can be distributed across all projects. If only one project is initiating this application of Continuous Risk Management, the cost of the infrastructure members, training, and tools may require special funding. Sponsors should be aware of and commit to the need for resources before agreeing to encourage this improvement.

New Projects

The discussion on applying Continuous Risk Management has concentrated on implementing it within an existing project. New projects, however, are an excellent opportunity to get risk management started at the very beginning. There are several basic steps that can be taken:

- Conduct **Baseline Identification and Analysis** [Chapter A-4] and **Baseline Planning** [Chapter A-5] on the proposed project to identify major risks.
- Adapt Continuous Risk Management to the standard project management practice and document in a **Risk Management Plan** [Chapter A-28].
- Identify needed tools, training, and supporting infrastructure.
- Upon initiation of the project, begin routine risk management activities.

Section 3

References

Cited in this chapter:

[Radice 94]   Radice, Ron & Garcia, Suzie. *An Integrated Approach to Software Process Improvement (SPI)*. Tutorial presented at the Software Technology Conference, April 1994, Salt Lake City, Utah. For information about this tutorial, contact The Utah State University, Continuing Education/Conferences at (801) 797-0423.

For more information on technology transition, software risk management, and process improvement, see the following:

[Air Force 88]   Air Force Systems Command/Air Force Logistics Command Pamphlet 800-45. *Software Risk Abatement*, September 30, 1988.

[Fowler 93]   Fowler, Priscilla & Levine, Linda. *A Conceptual Framework for Software Technology Transition* (CMU/SEI-93-TR-31). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

[Fowler 90]   Fowler, Priscilla J.; Rifkin, Stan; & Card, David N. *Software Engineering Process Group Guide* (CMU/SEI-90-TR-24, ADA235784). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1990.

[Myers 92]   Myers, Charles R.; Maher, John H.; & Deimel, Betty L. *Managing Technological Change*. Course materials. Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1992. For information about this course, contact SEI Customer Relations at (412) 268-5800 or customer-relations@sei.cmu.edu.

[Paulk 93]   Paulk, Mark; Curtis, Bill; Chrissis, Mary Beth; & Weber, Charles V. *Capability Maturity Model for Software, Version 1.1* (CMU/SEI-93-TR-24, ADA263403). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

[Sisti 94]   Sisti, Frank J. & Joseph, Sujoe. *Software Risk Evaluation Method Version 1.0* (CMU/SEI-94-TR-19, ADA290697). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

Part 5
Summary and Conclusions

Introduction   This part summarizes the information provided in this guidebook, provides key considerations for success, provides conclusions, and discusses some future directions in Continuous Risk Management.
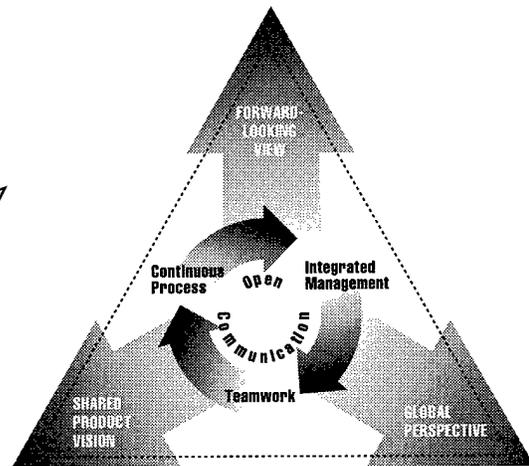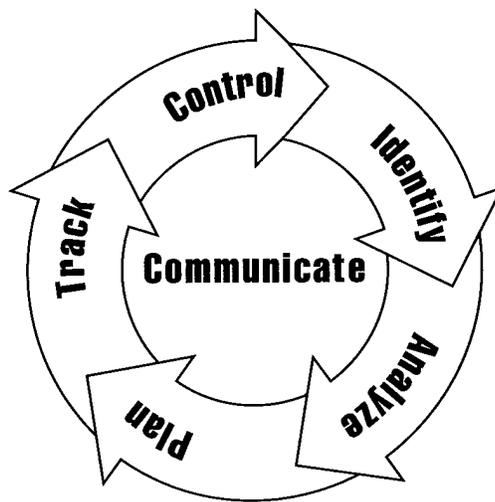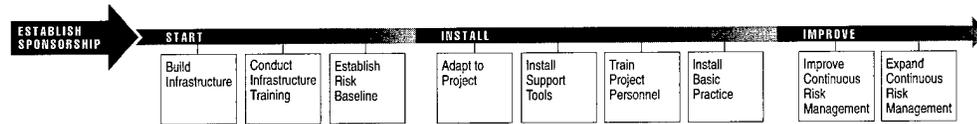
Chapter

Chapter 19

Summary

Section

Section 1

What Is Continuous Risk Management?

Description

Continuous Risk Management is a software engineering practice with processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making to
- assess continuously what can go wrong (risks)
- determine what risks are important to deal with
- implement strategies to deal with those risks

Continuous Risk Management Principles

Continuous Risk Management is built upon a set of principles (see following diagram) that, if followed, provide an effective approach to managing risk. The principles of Continuous Risk Management are the following:

- *Open communication* requires encouraging free-flowing information at and between all project levels, enabling formal, informal, and impromptu communication and bringing unique knowledge and insight to identifying and managing risk.
- *Forward-looking view* requires thinking toward tomorrow by identifying uncertainties, anticipating potential outcomes, and managing project resources and activities while anticipating uncertainties.
- *Shared product vision* requires arriving at a mutual product vision based upon common purpose, shared ownership, and collective commitment by focusing on results.
- *Global perspective* requires viewing software development within the context of the larger systems-level definition, design, and development, and recognizing both the potential value of opportunity and the potential impact of adverse effects.
- *Integrated management* requires making Continuous Risk Management an integral and vital part of project management by adapting Continuous Risk Management methods and tools to a project's infrastructure and culture.
- *Teamwork* requires working cooperatively to achieve a common goal, and pooling talent, skills, and knowledge.
- *Continuous process* requires sustaining constant vigilance while identifying and managing risks routinely throughout all phases of the project's life cycle.

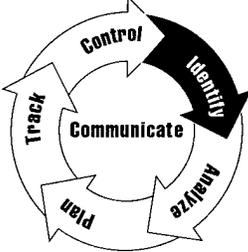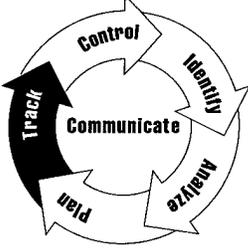The principles are shown in the following graphic.
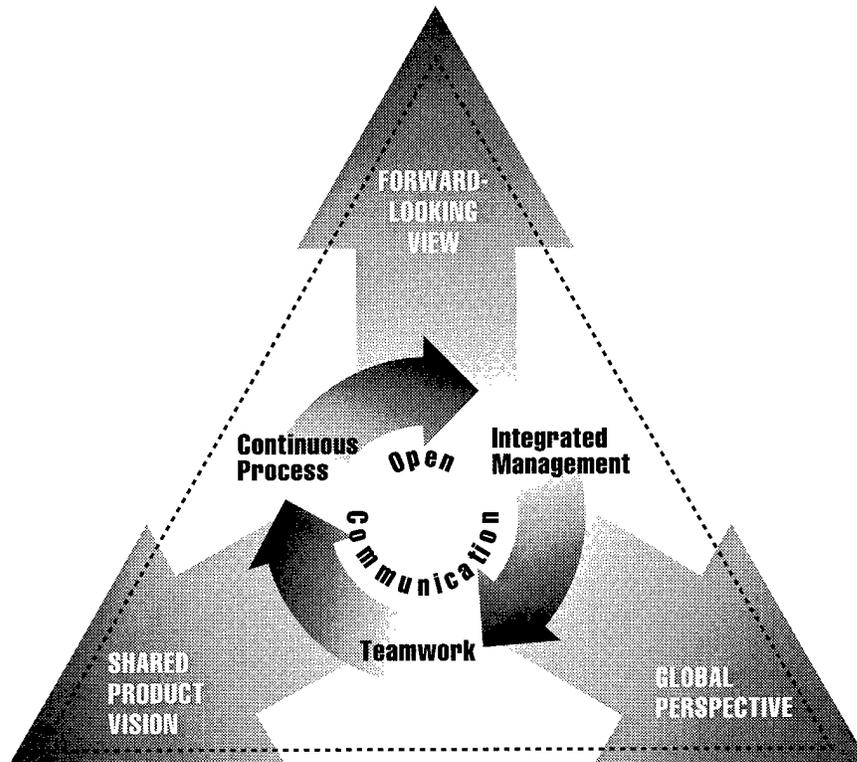
SEI Risk Management Paradigm

The SEI risk management paradigm is shown below. Each function has a set of activities backed by processes, methods, and tools that encourage and enhance communication and teamwork.
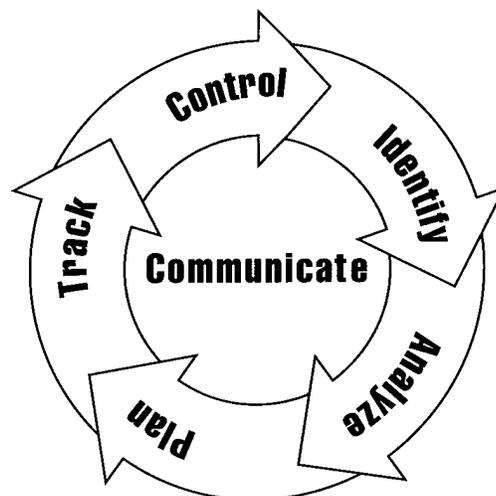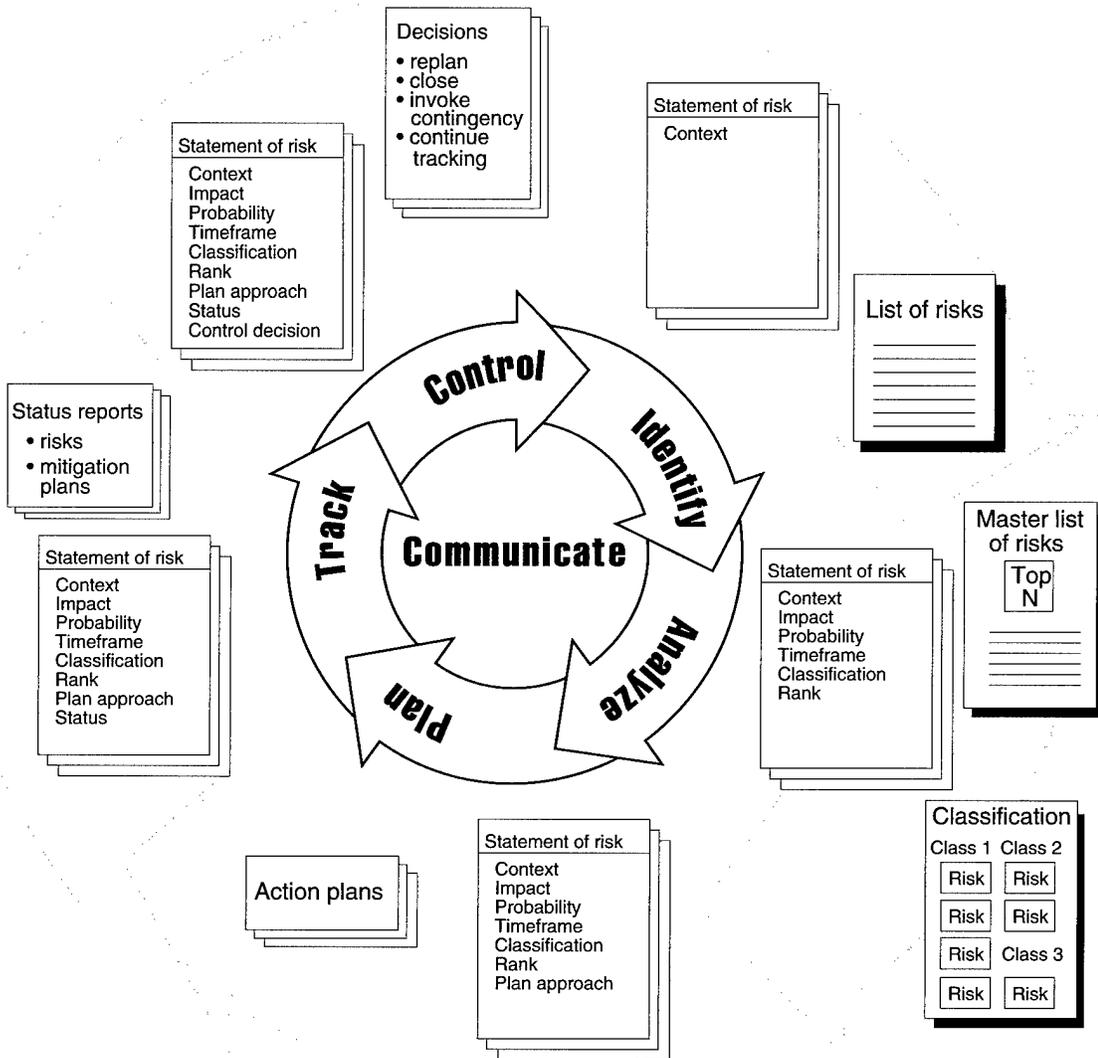
Continuous Risk Management Functions

The following table summarizes the Continuous Risk Management functions. A description of each function is provided and associated example methods and tools are listed. There are a variety of methods and tools that can be used to perform the different functions of Continuous Risk Management. Which specific method or tool is used is unimportant provided that the principles are upheld and the function input and output requirements are met.

Function	Description
Identify	Search for and locate risks before they become problems.
	Capture statements of risk and context.
	Example methods and tools: taxonomy-based questionnaire (TBQ), TBQ interviews, short TBQ, voluntary reporting, periodic risk reporting
Analyze	Transform risk data into decision-making information. Risk analysis is performed to determine what is important to the project and to set priorities.
	Evaluate impact probability, and timeframe, classify risks, and prioritize risks.
	Example methods and tools: tri-level attribute evaluation, taxonomy classification, multivoting, comparison risk ranking
Plan	Translate risk information into decisions and mitigating actions (both present and future) and implement those actions.
	Produce mitigation plans for mitigating individual or groups of risks.
	Example methods and tools: goal-question-measure, action item list, problem-solving planning, cause and effect analysis, brainstorming
Track	Monitor risk indicators and mitigation plans. Indicators and trends provide information to activate plans and contingencies. These are also reviewed periodically to measure progress and identify new risks.
	Acquire, compile, and report data on the risk and mitigation plan.
	Example methods and tools: spreadsheet risk tracking, mitigation status reports, stoplight charts

Function	Description
Control	Correct for deviations from the risk mitigation plans. Actions can lead to corrections in products or processes. Any action may lead to joint resolution. Changes to risks, risks that become problems, or faulty plans require adjustments in plans or actions. Analyze tracking data, decide on how to proceed, and execute decision. *Example methods and tools*: PERT charts, cost-benefit analysis, closing a risk
Communicate	Provide information and feedback internal and external to the project on the risk activities, current risks, and emerging risks. Communication occurs formally and informally. Communication is a key function in the Continuous Risk Management model that links to all the other functions. Therefore, each method identified previously is a vehicle for communication of risk.

Data Output Summary

The diagram on the next page summarizes the data output for each function of the SEI risk management paradigm.

Decisions
• replan
• close
• invoke
  contingency
• continue
  tracking

Statement of risk
Context

List of risks

Statement of risk
Context
Impact
Probability
Timeframe
Classification
Rank
Plan approach
Status
Control decision

Control

Identify

Track

Communicate

Status reports
• risks
• mitigation
  plans

Statement of risk
Context
Impact
Probability
Timeframe
Classification
Rank
Plan approach
Status

Plan

Analyze

Master list
of risks
Top
N

Statement of risk
Context
Impact
Probability
Timeframe
Classification
Rank

Classification
Class 1   Class 2
Risk   Risk
Risk   Risk
Risk   Class 3
Risk   Risk

Action plans

Statement of risk
Context
Impact
Probability
Timeframe
Classification
Rank
Plan approach

Data Output Summary

Section 2

Implementing Continuous Risk Management

**Key
Considerations**

To successfully implement Continuous Risk Management, a project must consider the following:

- *project organizational structure*: The project organizational structure provides information that will be fundamental in establishing a tailored risk management practice. It drives the internal and external communication as well as provides a structure for tailoring the processes and selecting appropriate methods and tools.
- *organization culture*: The organization's culture and recent history, particularly with respect to the application of quality and process improvements will affect the difficulty or ease of applying Continuous Risk Management in the project.
- *internal communication framework*: This framework helps to identify how the risk management activities may be associated with different project roles.
- *meeting structure*: The meeting structure indicates where much of the coordination and communication occurs.
- *tailoring the processes*: The project must take the conceptual view of the continuous functions of the risk management paradigm and show how these are implemented in the project. The result is tailored processes and data flows.
- *selecting methods and tools*: The project must select methods and tools to support the project's tailored risk management processes and integrate them with its current project management processes.
- *external communication*: Communication about risk must transcend the project boundary. Successful risk management requires some input from and visibility to stakeholders external to the project.

**Application
Roadmap**

Another way of looking at installation is with a "roadmap." An application roadmap for implementing Continuous Risk Management within a project is presented on the next page. There are three phases:

- *Start*: This phase focuses on establishing a commitment to proceed, building an infrastructure to support the implementation, training the project on the infrastructure, and establishing a critical mass of initial risks and mitigation plans.
- *Install*: This phase focuses on adapting the Continuous Risk Management processes to the project, identifying and installing support tools, training project personnel, and installing a basic risk management practice.
- *Improve*: This phase focuses on improving the processes, methods and tools as well as expanding Continuous Risk Management into other projects.
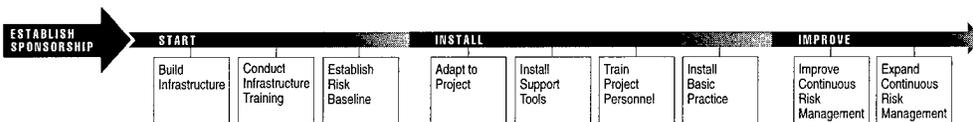
When to Start Continuous Risk Management

The best time to initiate Continuous Risk Management is as early in the project life-cycle as possible. The following table lists some opportune times to initiate or to start the Continuous Risk Management activities.

Opportunity	Description
Pre-contract activity	Include risk management provisions in the solicitation and statement of work.
Major project milestones (e.g., contract award or design reviews)	Prepare for a major project decision point, and the need to increase knowledge about risks for improved strategic planning.
Major project review	Prepare for a major review, such as design reviews, functional tests.
New manager	Use risk data information as an effective way to bring a new manager "up to speed" on the project.

Guidelines and Tips

Implementing a new technology or practice is never easy, and many improvement efforts fail. In working with many organizations who are piloting risk management efforts, the primary lessons the SEI Risk Program has learned from their efforts to install risk management are
- Start simple.
- Learn to "think risk."
- Look slightly ahead first, and deal with those issues and risks.
- As time progresses, force yourself to look further and further ahead.
- Never throw out or ignore any information; scan it once in a while.
- Don't hesitate to abandon a method after a fair trial and use something different.
- Always ask for feedback on how things are going and what works.
- Use outside facilitators until you're comfortable with the processes and are sure open communication is firmly established.

The key to installing Continuous Risk Management is in adhering to principles, performing the functions, and adapting the practice to suit your project.

Benefits of Successfully Implementing Continuous Risk Management

Soon, project personnel will feel comfortable performing risk management and you will see benefits to your project:
- *problems prevented before they occur*: Potential problems are identified and dealt with when it is easier and cheaper to do so—before they are problems and a crisis exists.
- *improved product quality*: A focus on the project's objective exists and personnel consciously look for things that may affect quality throughout product development.
- *better use of resources*: Early identification of potential problems provides input into management decisions regarding resource allocation.
- *teamwork*: Personnel at all levels of the project are involved and their attention focused on a shared product vision.

Chapter 20

Conclusions
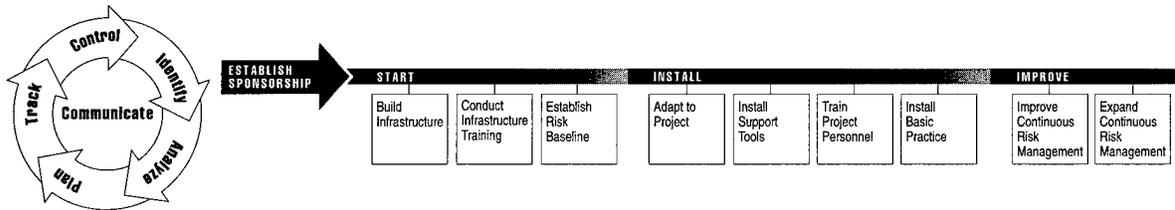
Section

Section 1

Conclusions

Guidebook Purpose

This guidebook is intended to teach you how to do Continuous Risk Management. To be successful, you'll need to tailor the processes, methods, and tools to suit your organization's project management processes.

Using this Guidebook

Take and adapt anything in this guidebook. This could be a little (e.g., one method) or a lot (e.g., implementation example). Different organizations will have different needs and uses for what is described here. Take whatever is needed to improve how you do Continuous Risk Management today.

Key Considerations

Effective Continuous Risk Management must
- fit your current project organization and culture—the project must own the practice
- satisfy the seven principles (open communication, integrated management, teamwork, continuous process, forward-looking view, global perspective, and shared product vision)
- be a flexible, not rigid practice
- be part of daily work (i.e., integrated into project management and daily routines)
- involve all project personnel

Reasons We Don't Do Risk Management

Remember the checklist of reasons project personnel use for not doing risk management which was introduced in Part 1? All of these reasons are barriers to risk management. Some of them are cultural barriers. All of them need to be overcome. Here's a sample list of answers to address the concerns inherent in the reasons.

❑ I don't have the time. There's too much regular project work to do.

Answer: If you don't take the time now, you'll take the time later (and usually more time) to fix problems which could have been prevented.

❑ It's not rewarded. Nobody wants to hear about what we can't do.

Answer: Sponsors and management must be prepared to reward the behavior they want to see.

❑ It's a bureaucratic nightmare. The processes are too complicated and time consuming.

Answer: Continuous Risk Management is successful when it is tailored to the project management processes. Start simple and improve the processes over time.

❑ I don't want to look stupid, especially in front of upper management.

Answer: Sponsors and management should educate the project about what is expected. Use your process improvement group to lay the groundwork.

❑ We already know our risks. We did an assessment at the beginning of the project. Once is enough!

Answer: Has anything changed since you identified the risks? If so, then the risks are not the same. You probably no longer know what all the risks to the project are. How useful is out of date information?

❏ This is just another management initiative. I'll wait to see if they're serious before I put any effort into it. Why waste time and energy?

Answer: This is a valid point but if no one else improves, is that a valid reason why you shouldn't? Don't you want to be better than your competition?

❏ They shoot the messenger. If I had a solution I wouldn't need to bring it up in the first place.

Answer: Sponsors and management need to encourage a risk-aware culture. Work with project personnel to identify potential solutions and choose a solution.

❏ Identifying risks means you need to solve them. We already have enough to do.

Answer: Again, if you don't take the time now, you'll take the time later (and usually more time) to fix problems which could have been prevented.

❏ _____(Fill in your own)

Answer: You already manage risks every day—when you drive your car, plan travel, budget for college expenses, use preventative health care. Apply the same philosophy to your job and the project you work on.

Section 2

Future Directions

Future Guidebook Versions

The SEI Risk Program will continue to test the processes, methods, and tools with new clients as well as expand our work to include more on metrics, cost models, and benchmarking for best practices. Future guidebook versions will address the results of these endeavors.

Continuous Risk Management Training

This guidebook can be augmented with training to master specific skills, as described in the Continuous Risk Management application roadmap ("Train Project Personnel" activity in the install phase) in Part 4. The SEI is planning a companion training course addressing the contents of this guidebook.

Software Risk Evaluation

The SEI Software Risk Evaluation (SRE) [Sisti 94] is a collection of methods that establishes a baseline set of risks, as described in the start phase in the Continuous Risk Management application roadmap. The SRE structures many of the methods and tools described in this guidebook into a concentrated timeframe to produce a risk baseline and mitigation strategies. It also includes the use of external expertise to assist in the classification, prioritization, and development of mitigation strategies.

Team Risk Management Guidebook

Team Risk Management [Gluch 94b, Higuera 94] extends the concept of Continuous Risk Management to customer-supplier relationships (e.g., government-contractor teams). A companion guidebook is planned to address the specific concerns customers and suppliers have addressing risk through a joint risk management practice.

Providing Feedback

The SEI Risk Program welcomes feedback on any part of this guidebook as well as ideas for new methods or tools. Please send any comments to SEI Customer Relations at this address:

Customer Relations
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Phone: (412) 268-5800
Internet: customer-relations@sei.cmu.edu

Risk Program Activities

To find out about other SEI Risk Program activities, and, eventually, the status of future guidebook versions, see the SEI Web page:

http://www.sei.cmu.edu/

Section 3

References

Cited in this chapter:

[Gluch 94b]   Gluch, David P.; Dorofee, Audrey J.; Murphy, Richard L.; Walker, Julie A.; & Williams, Ray C. *An Introduction to Team Risk Management Version 1.0* (CMU/SEI-94-SR-001). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

[Higuera 94]   Higuera, Ronald P.; Dorofee, Audrey J.; Walker, Julie A.; & Williams, Ray C. *Team Risk Management: A New Model for Customer-Supplier Relationships* (CMU/SEI-94-SR-05, ADA 283987). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

[Sisti 94]   Sisti, Frank J. & Joseph, Sujoe. *Software Risk Evaluation Method Version 1.0* (CMU/SEI-94-TR-19, ADA290697). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

References

[Air Force 95]   Department of the Air Force, Software Technology Support Center. *Guidelines for Successful Acquisition and Management of Software Intensive Systems: Weapon Systems, Command and Control Systems, Management Information Systems* Volume 1, Version 1.1. Salt Lake City, Utah: Department of the Air Force, Software Technology Support Center, 1995.

[Air Force 88]   Air Force Systems Command/Air Force Logistics Command Pamphlet 800-45. *Software Risk Abatement*, September 30, 1988.

[Arrow 88]   Arrow, Kenneth J. "Behavior Under Uncertainty and its Implications for Policy," 497-507. *Decision Making: Descriptive, Normative, and Prescriptive Interactions*. Cambridge: Cambridge University Press, 1988.

[Basili 84]   Basili, Victor R. & Weiss, David M. "A Methodology for Collecting Valid Software Engineering Data." *IEEE Transactions on Software Engineering SE-10*, 6 (November 1984): 728-738.

[Baumert 92]   Baumert, John H. & McWhinney, Mark S. *Software Measures and the Capability Maturity Model* (CMU/SEI-92-TR-25). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1992.

[Bennatan 92]   Bennatan, E. M. *On Time, Within Budget - Software Project Management Practices and Techniques*. McGraw-Hill International (UK) Limited, 1992.

[Boehm 89]   Boehm, Barry. *IEEE Tutorial on Software Risk Management*. New York: IEEE Computer Society Press, 1989.

[Boehm 81]   Boehm, Barry. *Software Engineering Economics*. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1981.

[Brassard 94]   Brassard, Michael & Ritter, Diane. *The Memory Jogger™ II:A Pocket Guide of Tools for Continuous Improvement & Effective Planning*. Methuen, Ma.: GOAL/QPC, 1994.

[Brassard 89]   Brassard, Michael. *The Memory Jogger +™: featuring the seven management and planning tools*. Methuen, Ma.: GOAL/QPC, 1989.

[Carr 93]   Carr, Marvin; Konda, Suresh; Monarch, Ira; Ulrich, Carol; & Walker, Clay. *Taxonomy-Based Risk Identification* (CMU/SEI-93-TR-6, ADA266992). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

[Charette 89]   Charette, Robert N. *Software Engineering Risk Analysis and Management*. New York: McGraw-Hill, 1989.

[Clark 95]   Clark, Bill. "Technical Performance Measurement in the Risk Management of Systems," Presented at the Fourth SEI Conference on Software Risk, Monterey, CA, November 6-8, 1995. For information about how to obtain copies of this presentation, contact SEI customer relations at (412) 268-5800 or customer-relations@sei.cmu.edu.

[Covello 93]   Covello, V.T.; Fischhoff, B.; Kasperson, R. E.; & Morgan, M. G. "Comments on the 'Mental Model' Meets the Planning Process." *Risk Analysis 13*, 5 (October 1993): 493-494.

[Evans 83]   Evans, M. W.; Piazza, P.; & Dolkas, J. B. *Principles of Productive Software Management*. New York: John Wiley and Sons, 1983.

[FitzGerald 90a]   FitzGerald, Jerry. "Risk Ranking Contingency Plan Alternatives." *Information Executive 3*, 4 (Fall 1990): 61-63.

[FitzGerald 90b]   FitzGerald, Jerry; & FitzGerald, Andra F. Ch. 5, "A Methodology for Conducting a Risk Assessment," 59-72. *Redesigning Controls into Computerized Systems,* 2nd ed. Redwood City, CA: Jerry FitzGerald & Associates, 1990.

[Fowler 93]   Fowler, Priscilla & Levine, Linda. *A Conceptual Framework for Software Technology Transition* (CMU/SEI-93-TR-31). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

[Fowler 90]   Fowler, Priscilla J.; Rifkin, Stan; & Card, David N. *Software Engineering Process Group Guide* (CMU/SEI-90-TR-24, ADA 235784). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1990.

[Gluch 94a]   Gluch, David P. *A Construct for Describing Software Development Risk* (CMU/SEI-94-TR-14, ADA284922). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

[Gluch 94b]   Gluch, David P.; Dorofee, Audrey J.; Murphy, Richard L.; Walker, Julie A.; & Williams, Ray C. *An Introduction to Team Risk Management Version 1.0* (CMU/SEI-94-SR-001). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

[Grady 92]   Grady, Robert B. *Practical Software Metrics for Project Management and Process Improvement.* Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1992.

[Grady 87]   Grady, Robert B. & Caswell, Deborah L. *Software Metrics: Establishing a Company-Wide Program,* Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1987.

[Hays 88]   Hays, William L. *Statistics.* New York: Holt, Rinehart and Winston, Inc., 1988.

[Higuera 94]   Higuera, Ronald P.; Dorofee, Audrey J.; Walker, Julie A.; & Williams, Ray C. *Team Risk Management: A New Model for Customer-Supplier Relationships* (CMU/SEI-94-SR-05, ADA 283987). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

[Higuera 93]   Higuera, Ronald P. & Gluch, David P. "Risk Management and Quality in Software Development." *Proceedings of the Eleventh Annual Pacific Northwest Software Quality Conference.* Portland, Oregon, October 18-20, 1993. Portland, Oregon: Pacific Northwest Software Quality Conference, 1993.

[Juran 89]   Juran, J. M. *Juran on Leadership for Quality.* New York: The Free Press, 1989.

[Kepner 81]   Kepner, Charles H. & Tregoe, Benjamin B. *The New Rational Manager.* Kepner-Tregoe, Inc. Princeton, NJ: Princeton Research Press, 1981.

[Kirkpatrick 92]   Kirkpatrick, Robert J.; Walker, Julie A.; & Firth, Robert. "Software Development Risk Management: An SEI Appraisal." Software Engineering Institute Technical Review '92 (CMU/SEI-92-REV). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1992.

[Kloman 90]   Kloman, H.F. "Risk Management Agonists." *Risk Analysis 10*, 2 (1990): 201-205.

[Lowrance 76]   Lowrance, William W. *Of Acceptable Risk.* Los Altos, Ca.: William Kaufmann, 1976.

[Lumsdaine 90]   Lumsdaine, Edward & Lumsdaine, Monika. *Creative Problem Solving.* New York: McGraw-Hill, 1990.

[Mayrhauser 90]   Mayrhauser, Anneliese von. *Software Engineering: Methods and Management*. San Diego Ca.: Academic Press, Inc., 1990.

[Meredith 89]   Meredith, Jack R. & Mantel, Samuel J. Jr. *Project Management: A Managerial Approach*, 2nd ed. New York: John Wiley and Sons, 1989.

[Moran 90]   Moran, John W.; Talbot, Richard P.; & Benson, Russell M. *A Guide to Graphical Problem-Solving Processes*. Milwaukee Wi.: ASQC Quality Press, 1990.

[Myers 92]   Myers, Charles R.; Maher, John H.; & Deimel, Betty L. *Managing Technological Change*. Course materials. Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1992. For information about this course, contact SEI Customer Relations at (412) 268-5800 or customer-relations@sei.cmu.edu.

[NRC 89]   Committee on Risk Perception and Communication, Commission on Behavioral and Social Sciences Education, National Research Council. *Improving Risk Communication*. Washington, D.C.: National Academy Press, 1989.

[Osborn 53]   Osborn, Alexander. *Applied Imagination; Principles of Creative Thinking*. New York: Scribner, 1953.

[Paulk 93]   Paulk, Mark; Curtis, Bill; Chrissis, Mary Beth; & Weber, Charles V. *Capability Maturity Model for Software, Version 1.1* (CMU/SEI-93-TR-24, ADA263403). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

[Pfleeger 91]   Pfleeger, Shari Lawrence. *Software Engineering: The Production of Quality Software*, 2nd ed. New York: MacMillan Publishing Co., 1991.

[Pressman 92]   Pressman, Roger S. *Software Engineering: A Practitioner's Approach*, 3rd ed. New York: McGraw-Hill, Inc., 1992.

[Pulford 96]   Pulford, Kevin; Kuntzmann-Combelles, Annie; & Shirlaw, Stephen. *A Quantitative Approach to Software Management: The ami Handbook*. Wokingham, England: Addison-Wesley Publishing Company, 1996.

[Radice 94]   Radice, Ron & Garcia, Suzie. *An Integrated Approach to Software Process Improvement (SPI)*. Tutorial presented at the Software Technology Conference, April 1994, Salt Lake City, Utah. For information about this tutorial, contact The Utah State University, Continuing Education/Conferences at (801) 797-0423.

[Radice 88]   Radice, Ron A. & Phillips, Richard W. Chapter 6, "Planning The Project," 183-184. *Software Engineering: An Industrial Approach*, Volume 1. Englewood Cliffs, N.J.: Prentice-Hall, 1988.

[Rosenau 92]   Rosenau, Milton D. *Successful Project Management: A Step-by Step Approach With Practical Examples*. New York: Van Nostrand Reinhold, 1992.

[Rowe 88]   Rowe, William D. *An Anatomy of Risk*. Malabar, Fla.: Robert E. Krieger, 1988.

[Scholtes 88]   Scholtes, Peter R. *The Team Handbook: How to Use Teams to Improve Quality*. Madison, Wi.: Joiner Associates, Inc., 1988.

[SEI 92]   Software Engineering Institute. "The SEI Approach to Managing Software Technical Risks." *Bridge* (October 1992): 19-21.

[Shere 88]   Shere, Kenneth D. *Software Engineering and Management*. Englewood Cliffs, N.J.: Prentice-Hall, 1988.

[Sisti 94]   Sisti, Frank J. & Joseph, Sujoe. *Software Risk Evaluation Method Version 1.0* (CMU/SEI-94-TR-19, ADA290697). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

[Thayer 88]   Thayer, Richard H. *Software Engineering Project Management Tutorial*. Washington D.C.: Computer Society Press of the Institute of Electrical and Electronics Engineers, Inc., 1988.

[Umbaugh 89]   Umbaugh, Robert E. & Gitomer, Jerry. "Project Scheduling and Control," 37-48. *Handbook of Systems Management: Development and Support*. Boston, Ma.: Auerbach Publishers, 1989.

[Van Scoy 92]   Van Scoy, Roger L. *Software Development Risk: Opportunity, Not Problem*. (CMU/SEI-92-TR-30, ADA 258743). Pittsburgh, Pa.: Software Engineering Institute, 1992.

[Webster's 81]   *Webster's Third New International Dictionary*. Springfield, Ma.: Merriam-Webster, 1981.

[Xerox 92]   Xerox Corporation and Carnegie Mellon University. *The University Challenge: Problem-Solving Process User Manual*. Stamford, Ct.: Xerox Corporation, 1992.

Glossary

accept   A *mitigation approach*[1] that essentially does nothing with the risk. It is handled as a problem if it occurs. No risk management resources are expended dealing with accepted risks. See *acceptance rationale*.

acceptance rationale   A type of *action plan* that documents the reason or rationale for accepting a risk (doing nothing with it). This is documented for historical reasons.

accountability   Defines who must ultimately answer for the success or failure of managing a risk.

action item list   A simple type of *mitigation plan*, this is a simple list of actions, *responsibility*, and due dates for completing the actions associated with a mitigation strategy.

action plan   The course of action chosen for dealing with a risk. This can be a *research plan* (for risks that need to be researched), *acceptance rationale* (for risks that are accepted), *tracking requirements* (for risks that will be watched), or a *mitigation plan* (for risks that will be mitigated).

Analyze   One of the six functions of the SEI risk management paradigm. The Analyze function is a process in which risks are examined in further detail to determine the extent of the risks, how they relate to each other, and which ones are the most important to deal with. Analyzing risks has three basic activities:

- evaluating the attributes of risks
- classifying risks
- prioritizing (ranking) risks

application roadmap   A "roadmap" that directs the implementation (or application) of *Continuous Risk Management* in a project, and, eventually, an organization. It identifies the key activities required for successful implementation organized into three phases: Start, Install, and Improve.

authority   The right and the ability to assign resources for mitigating a risk.

Communicate   One of the six functions of the SEI risk management paradigm. The Communicate function is a process in which risk information is conveyed between all levels of a project team. Risk communication deals with the ideas of probability and negative consequences. It is present in all of the other functions of the SEI risk management paradigm and is essential for the management of risks within an organization. Communication must both fit within an organization's culture and expose the risks that are present in an organization's projects.

---

1. Where a definition includes a term defined elsewhere in this glossary, that term is *italicized*.

condition   The key circumstances, situations, etc., that are causing concern, doubt, anxiety, or uncertainty. In a *risk statement*, the condition phrase is the phrase at the beginning of the statement.

consequence   The possible negative outcomes of the current conditions that are creating uncertainty. In a *risk statement*, the consequence phrase is the phrase at the end of the statement.

context   Context provides additional detail regarding the events, circumstances, and interrelationships within the project that may affect the risk. This description is more detailed than can be captured in the basic statement of risk.

continuous process   A sustaining principle of *Continuous Risk Management*, continuous process requires

- sustaining constant vigilance
- identifying and managing risks routinely throughout all phases of the project's life cycle

Continuous Risk Management   Continuous Risk Management is a *software engineering practice* with processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making to

- assess continuously what could go wrong (risks)
- determine which risks are important to deal with
- implement strategies to deal with those risks

Control   One of the six functions of the SEI risk management paradigm. The Control function is a process that takes the tracking status reports for the watched and mitigated project risks and decides what to do with them based on the reported data. The person who has *accountability* for a risk normally makes the control decision for that risk. The general process of controlling risks includes

- analyzing the status reports
- deciding how to proceed
- executing the decisions

delegate   To assign *responsibility* for a risk to someone else within the team or project. The person to whom a risk is delegated is usually at a lower level in the organization. See also *transfer* and *keep*.

forward-looking view   A defining principle of *Continuous Risk Management*, forward-looking view requires

- thinking toward tomorrow, identifying uncertainties, anticipating potential outcomes
- managing project resources and activities while anticipating uncertainties

global perspective   A defining principle of *Continuous Risk Management*, global perspective requires

- viewing software development within the context of the larger systems-level definition, design, and development
- recognizing both the potential value of opportunity and the potential impact of adverse effects

Identify   One of the six functions of the SEI risk management paradigm. The Identify function is a process of transforming uncertainties and issues about the project into distinct (tangible) risks that can be described and measured. Identifying risks involves two activities:

- capturing a statement of risk
- capturing the *context* of a risk

impact   The loss or effect on the project if the risk occurs. Impact is one of the three attributes of a risk.

implementation plan   This plan defines how *Continuous Risk Management* will be implemented within a project. It describes how the transition will occur, roles and responsibilities, a schedule for implementing specific processes and methods, costs and schedules for acquiring and training personnel on new tools, etc.

indicator   A representation of measurement data that provides insight into a process or improvement activity. Indicators can be used to show status and are also called status indicators. Indicators may use one or more measures, and they can give a more complex measure of the risk and *mitigation plan*.

infrastructure costs Those costs associated with implementing risk management activities and supporting risk management processes, methods, and tools within the organization. These costs may be spread out across multiple projects. See also *mitigation costs* and *risk management costs*.

integrated management   A sustaining principle of *Continuous Risk Management*, integrated management requires

- making Continuous Risk Management an integral and vital part of project management
- adapting Continuous Risk Management methods and tools to a project's infrastructure and culture

keep   To retain *responsibility* for a risk. See also *delegate* and *transfer*.

measure (metric)   A standard way of measuring some attribute of the risk management process. Risk and *mitigation plan* measures can be qualitative or quantitative. Measure is synonymous with metric.

mitigate   A *mitigation approach* that deals with a risk by developing strategies and actions for reducing (or eliminating) the *impact, probability*, or both, of the risk to some acceptable level. It may also involve shifting the *timeframe* when action must be taken. See *mitigation plan*.

mitigation approach   The approach taken to deal with a risk. This can be to *accept* it, *research* it, *watch* it, or *mitigate* it.

mitigation costs   Those costs directly associated with mitigating specific risks to the project. This is the cost of carrying out the *mitigation plan*. See *infrastructure costs* and *risk management costs*.

mitigation plan   An *action plan* for risks that are to be mitigated. It documents the strategies, actions, goals, schedule dates, *tracking requirements*, and all other supporting information needed to carry out the mitigation strategy. See also *action item list* and *task plan*.

open communication   The core principle of *Continuous Risk Management*, open communication requires

- encouraging free-flowing information at and between all project levels
- enabling formal, informal, and impromptu communication
- using consensus-based processes that value the individual voice (bringing unique knowledge and insight to identifying and managing risk)

Plan   One of the six functions of the SEI risk management paradigm. The Plan function is a process for determining what, if anything, should be done with a risk. It produces an *action plan* for individual or sets of related risks. Planning answers the questions

- Is it my risk? (*responsibility*)
- What can I do? (approach)
- How much and what should I do? (scope and actions)

probability   The likelihood the risk will occur. Probability is one of the three attributes of a risk.

research   A *mitigation approach* that involves investigating the risk itself to increase the level of understanding until a decision about what to do with the risk can be reached. This is a preliminary approach used to make sure an informed decision can be made to *accept*, *watch*, or *mitigate* a risk.

research plan   An *action plan* for risks that needs to be researched. It documents a plan and schedule for investigating the risks, evaluating the results, and reporting the conclusions.

responsibility   The quality or state of being assigned the task of developing and implementing a risk *action plan*.

risk   The possibility of suffering loss. In a development project, the loss describes the *impact* to the project, which could be in the form of diminished quality of the end product, increased costs, delayed completion, or failure.

risk baseline   A "snapshot" of all currently known risks to a project, used to begin the process of implementing *Continuous Risk Management* within that project.

risk management costs   The costs associated with performing risk management activities—e.g., identifying risks, building status reports, and developing mitigation plans. This should not be confused with *mitigation costs* or *infrastructure costs*.

risk management plan   A formal plan or documentation of the risk management practice (processes, methods, and tools) to be used for a specific project. This directs and manages the activities used to perform risk management within that project.

risk statement (also known as statement of risk)   For a risk to be understandable, it must be expressed clearly. Such a statement must include

- a description of the current conditions that may lead to the loss
- a description of the loss or consequence.

shared product vision   A defining principle of *Continuous Risk Management*, shared product vision requires

- arriving at a mutual product vision based upon common purpose, shared ownership, and collective commitment
- focusing on results

software engineering practice   All of the processes, methods, and tools required to fully implement and perform a particular software engineering technology, such as *Continuous Risk Management.*

software engineering process group (SEPG)   The Software Engineering Process Group is the focal point for process improvement. Composed of line practitioners who have varied skills, the group is at the center of the collaborative effort of everyone in the organization who is involved in software process improvement.

task plan   A complex type of *mitigation plan* that should be similar to a project's standard task plan. It is used for complex risks or sets of risks or complex, expensive mitigation plans that require extensive details relevant to scheduling, budgets, actions, contingency plans, task interrelationships and dependencies, etc.

teamwork   A sustaining principle of *Continuous Risk Management*, teamwork requires

- working cooperatively to achieve a common goal
- pooling talent, skills, and knowledge

timeframe   The period when action is required to *mitigate* the risk. Timeframe is one of the three attributes of a risk.

Track   One of the six functions of the SEI risk management paradigm. The Track function is a process in which risk data are monitored by the person(s) responsible for tracking watched and mitigated risks. Tracking risks includes three activities:

- acquiring *tracking data*
- compiling tracking data
- reporting tracking data

tracking data   The *measure, indicators*, and *triggers* used to monitor risks and mitigation plans.

tracking requirements   An *action plan* for watched risks. These are the indicators, triggers, and thresholds used to monitor the risks, as well as the requirements for documenting and reporting status.

transfer   To allocate *authority, responsibility,* and *accountability* for a risk to another person or organization. This is considered a lateral or upward transition of responsibility—e.g., to a customer or another team in the organization.

trigger   Thresholds for *indicators* that specify when an action, such as implementing a contingency plan, may need to be taken. Triggers are generally used to

- provide warning of an impending critical event
- indicate the need to implement a contingency plan to preempt a problem
- request immediate attention for a risk

watch   A *mitigation approach* that monitors a risk and its attributes for significant change. Watched risks may later be mitigated or closed without any further action, depending upon how it changes as time progresses. See *tracking requirements*.

Appendix A

Methods and Tools
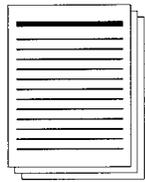
Risk Management Plan

A Risk Management Plan documents how risks will be managed on a project: the process, activities, milestones, and responsibilities associated with risk management. It is a subset of the project plan and is written before the project begins.

Control
- Cause and Effect Analysis
- Closing a Risk
- Cost-Benefit Analysis
- List Reduction
- Mitigation Status Report
- Multivoting
- PERT Charts
- Problem-Solving Planning
- Risk Information Sheet
- Spreadsheet Risk Tracking
- Stoplight Chart

Identify
- Baseline Identification and Analysis
- Brainstorming
- Periodic Risk Reporting
- Project Profile Questions
- Risk Form
- Risk Information Sheet
- Short TBQ
- Taxonomy-Based Questionnaire (TBQ)
- TBQ Interviews
- Voluntary Risk Reporting

Track
- Bar Graph
- Mitigation Status Report
- Risk Information Sheet
- Spreadsheet Risk Tracking
- Stoplight Chart
- Time Correlation Chart
- Time Graph

Control / Identify / Analyze / Plan / Track / Communicate

Plan
- Action Item List
- Baseline Planning
- Planning Decision Flowchart
- Planning Worksheet
- Problem-Solving Planning
  - Affinity Grouping
  - Brainstorming
  - Cause and Effect Analysis
  - Cost-Benefit Analysis
  - Gantt Charts
  - Goal-Question-Measure
  - Interrelationship Digraph
  - List Reduction
  - Multivoting
  - PERT Charts
  - Work Breakdown Structure
- Risk Information Sheet

Analyze
- Affinity Grouping
- Bar Graph
- Baseline Identification and Analysis
- Binary Attribute Evaluation
- Comparison Risk Ranking
- Multivoting
- Pareto Top N
- Potential Top N
- Risk Form
- Risk Information Sheet
- Taxonomy Classification
- Top 5
- Tri-level Attribute Evaluation

Introduction

This appendix contains descriptions of the methods and tools used to implement Continuous Risk Management; these methods and tools are referenced throughout the body of the guidebook. Methods provide systematic approaches to performing the Continuous Risk Management processes and include procedures and guidelines and tips. Tools provide templates and forms along with an example. Tools described with methods are either tools that are specific to the method or are examples of more general tools described elsewhere in the appendix.

Each section of this appendix describes either a method or a tool. These sections are organized as shown in the graphic below.

Method
- Description
- When to Use
- Procedure
- Tools (if applicable)
- Guidelines and Tips

Tool
- Description
- How to Use
- Example
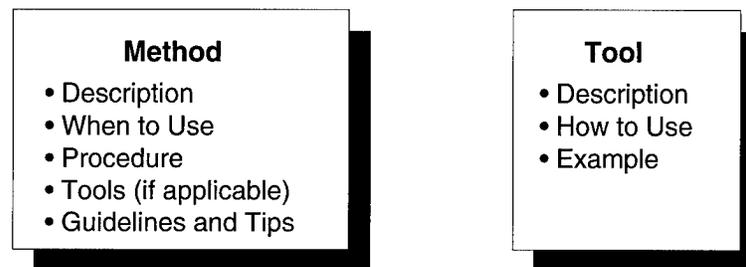
Note: The word "facilitator" is commonly used to indicate who performs different activities or leads a group in applying some methods. If it is not practical to have an independent facilitator, one of the group can lead the activities and participate. However, the leader must be careful never to dominate the process or the group members. Facilitation skills are generally required for anyone who is a leader.

Chapter

Chapter

Chapter A-1

Action Item List

Description

Action item lists are the simplest means of documenting and tracking risk mitigation actions. They are not as extensive as task plans, but address key factors, such as

- action description
- responsible personnel
- mitigation goals or success factors
- due date
- closing status or results
- closing date
- (optional) intermediate status, comments, etc.

While action item lists do not generally have sufficient detail to support complex mitigation strategies, they are sufficient for simple actions, and for getting started with risk management. The **Planning Worksheet** [Chapter A-22] is a good supporting tool to use in conjunction with an action item list to document causes of the risk, alternative actions, and related information.

How to Use

Action item lists are most often used to track the actions that are assigned to members of a group or team; however, the lists can also be used by individuals to track their own actions and status.

Use of an action item list is simple. As actions are identified and assigned, they are added to the list and usually given a distinct identifier. Actions are closed when the action is complete and the results are satisfactory. Groups generally use consensus to achieve item closure. Data on closed action items are retained for historical purposes and also in case the action needs to be revisited at some future time.

**Example
Action Item
List**

There are many templates for action items lists; the form on the following page is an example of one that can be used for risk-related actions.

Risk Action Item List

ID	Risk Statement	Mitigation Goal/Success Measures	Action Description	Assigned To:	Due Date	Current Status
23	We're not sure what the emergency procedures are; we might do the wrong things	Defined, documented, viable procedure / everyone knows procedure or knows where to find it.	Document current emergency back-up procedures Distribute to all personnel	S. Smith	3/15/96 4/1/96	3/1/96-documented; pending approval
34	Several key people have long commutes; if bad weather occurs, they might not make it in and the schedule could suffer	Bad weather is no longer a justifiable excuse for missing schedules / operational modems at all key personnel homes; server supports remote access; personnel trained in using modems and access procedure	Purchase 5 more modems for remote dial-in Distribute and test modems Document dial-in procedure and train key personnel	G. Samms	4/1/96 4/15/96 4/20/96	3/1/96-purchase order submitted
41	We're not all trained on the tools and we can't all be gone at the same time for a class; we're likely to keep losing time trying to figure out the tools.	Everyone gets trained as soon as possible / 75% reduction in help-desk calls by 4/15/94; survey indicates 80% personnel comfortable with the tools	Buy 10 sets of self-instruction manuals Lead weekly brown bag, cross-training lunches	G. Samms	3/1/96 start 3/15/96	3/1/96-ordered; shipment late - expected in next week

Chapter A-2

Affinity Grouping[1]

---

1. In *The Memory Jogger Plus +*™ Affinity Grouping is discussed under "Affinity Diagrams" [Brassard 89].
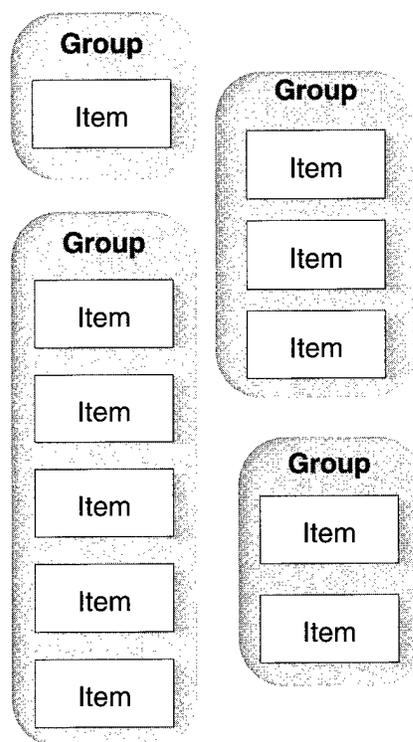
Section 1

Affinity Grouping Description

Introduction

The affinity grouping method groups items (e.g., risks) that are naturally related and then identifies the one concept that ties each grouping together [Brassard 89]. Affinity grouping organizes large amounts of data into groupings based on the natural relationship between each item, and defines the groups of items.

Diagram

The following diagram shows the inputs and outputs for affinity grouping.
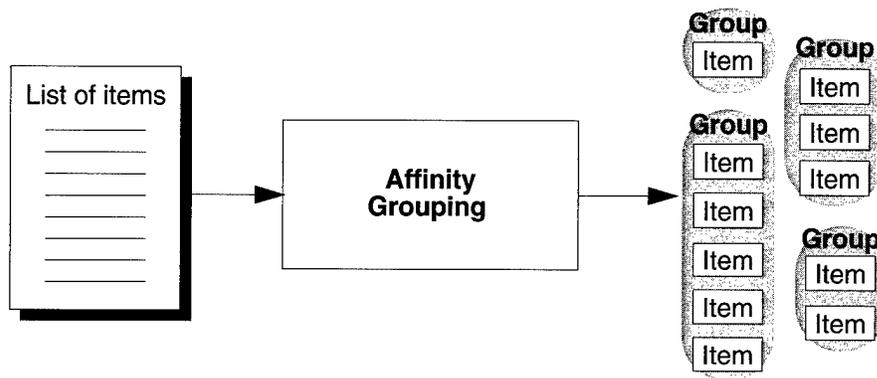
Personnel Requirements

Affinity grouping may be done by an individual or a group. If performed by a group of three or more, one person should be the facilitator and recorder (but he or she could still participate or contribute).

Section 2

When to Use

When to Use

Use this method

- to classify risks when you do not have a predefined structure
- when breakthrough thinking is required [Brassard 89]
- when broad issues/themes need to be identified [Brassard 89]
- when you have a large list of items to make sense out of

Constraints

Avoid using this method for things that are simple or require a quick solution [Brassard 89].

Benefits

This method

- provides a way to efficiently sort through large amounts of information [Brassard 89]
- allows truly new patterns of information to rise to the surface [Brassard 89]
- requires active participation by all participants in the process [Brassard 89]
- helps to identify duplicate risks

Section 3

Conducting an Affinity Grouping

Procedure

This table describes the procedure for conducting an affinity grouping. This procedure is a subset of the steps described in the Affinity Diagram chapter of *The Memory Jogger Plus* +™ [Brassard 89].

Step	Action
1	**Review items for understanding**. Facilitator ensures all participants understand the items on the list.
2	**Record items on cards**. Facilitator records each item on a separate card. Print legibly and large enough so that the cards can be read from a distance of four to five feet away.
3	**Display cards**. Facilitator shuffles the cards and spreads them out randomly. Allow enough space in front of the work area to allow five to six people to easily see and move the cards.
4	**Arrange cards into related groupings**. All participants look for two cards that seem related in some way and place those cards to one side. They also look for other cards that are either related to each other or to the original two cards that were set aside. Participants repeat this process until all the cards have been placed in 7±2 groupings.
5	**Create header cards for groupings**. Participants look for a card in each grouping that captures the central idea that ties all of the cards together. If no card exists, they create one. Place the header card above its group.

Section 4

Affinity Grouping Tools

**Sample
Affinity
Diagram**

Below is a generic sample of an affinity diagram [Brassard 89] illustrating the results of affinity grouping session. It provides a visual summary of all groups and items.
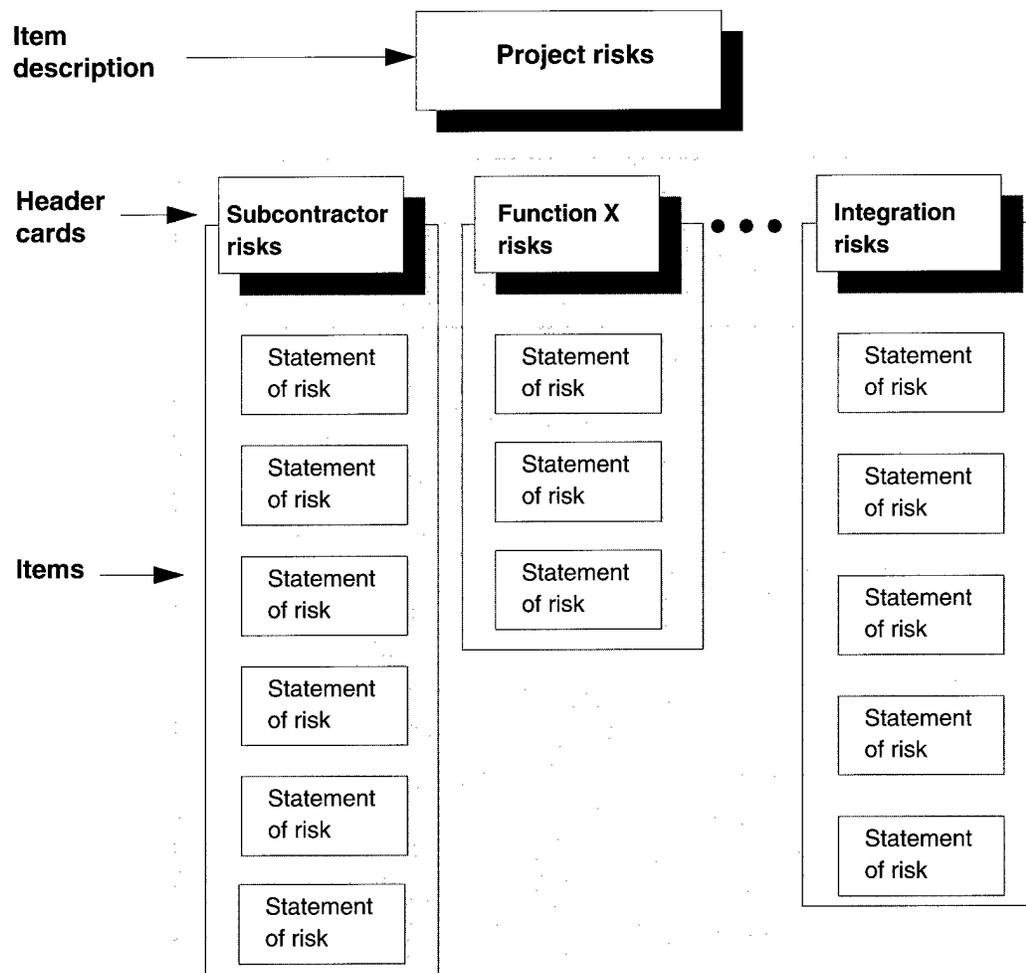
Section 5

Guidelines and Tips

**General
Guidelines and
Tips**

The following tips and guidelines were adapted from the notes described in the affinity diagram chapter of *The Memory Jogger Plus +*™ [Brassard 89, pp. 17-40].

- Record items on a medium that is easy to move—3M's Post-it™ note paper or 3x5 note cards work well.
- Have participants move cards at will, without talking. It encourages thinking "outside the box" and discourages arguing over the specific words used.
- Encourage participants to react to what they see instead of agonizing over the "right" placement. The objective is speed.
- If a participant doesn't like where a card is, he or she should move it. It will all eventually settle into consensus.
- Do not force cards into groupings in which they do not belong. Create a new category. A single card may form its own grouping.
- Avoid jargon when wording the header cards. The header cards should be clear enough that a person outside the session could look at just the header cards and understand the essence and detail of the items. The header card should be more than a one-word title.
- Teams can "produce and organize more than 100 ideas or issues in 30-35 minutes" [Brassard 89, p.17].

**Affinity
Subgroups**

Where there may be several items in an affinity group, there may also be two or more sub-groups which can be identified.

References

Cited in this chapter:

[Brassard 89]

Brassard, Michael. Ch. 1, "Affinity Diagram," 17-40. *The Memory Jogger Plus +*™*:featuring the seven management and planning tools.* Methuen, Ma.: GOAL/QPC, 1989.

For more information on affinity grouping, see the following:

[Brassard 94]

Brassard, Michael & Ritter, Diane. *The Memory Jogger* ™ *II:A Pocket Guide of Tools for Continuous Improvement and Effective Planning.* Methuen, Ma.: GOAL/QPC, 1994.

Chapter A-3

Bar Graph

Description

Bar graphs compare a collection of data across multiple categories by graphically presenting the data using bars, the lengths of which are proportional to the measures of the data. For example, in risk management, bar graphs can be used to graphically represent categories of risks and the number of risks in each category.

How to Use

This is a convenient method for displaying large amounts of data that are difficult to interpret when they are in tabular form. The underlying distribution of the data is illustrated by using this technique.

For example, as risks are analyzed, they are grouped into classes of related risks. These data are displayed graphically in a bar graph for risk tracking and control. The graphs are used to identify trends in the number of risks in individual categories or classes.

Example

A technical lead examined the following bar graph, and noticed that there were a large number of testing-related risks on the project. As coding progresses, testing issues normally surface; however, software coding for this project had not begun. Analysis of the testing-related risks showed that the test plans were inadequate. The mitigation plan for the risks called for project personnel to receive more training in the area of software testing. The personnel received the training, and the risks were successfully mitigated.
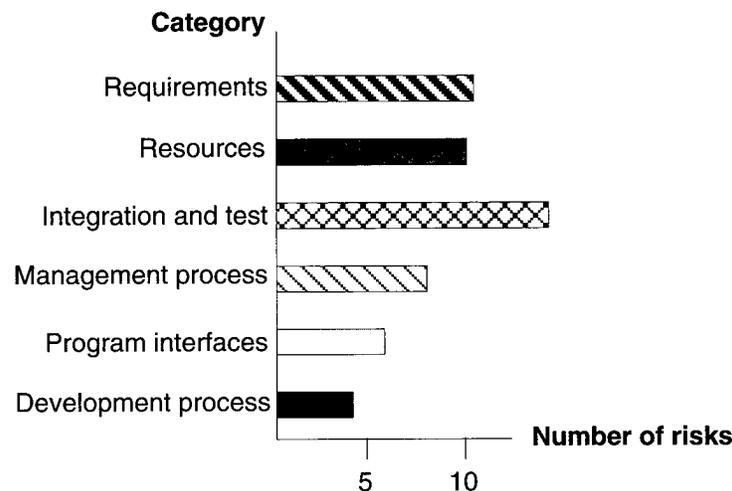
References

For more information on bar graphs, see the following:

[Brassard 89]   Brassard, Michael. *The Memory Jogger +*™*: featuring the seven management and planning tools*. Methuen, Ma.: GOAL/QPC, 1989.

[Hays 88]   Hays, William L. *Statistics*. New York: Holt, Rinehart and Winston, Inc., 1988.

[Moran 90]   Moran, John W.; Talbot, Richard P.; & Benson, Russell M. *A Guide to Graphical Problem-Solving Processes*. Milwaukee Wi.: ASQC Quality Press, 1990.

Chapter A-4

Baseline Identification and Analysis
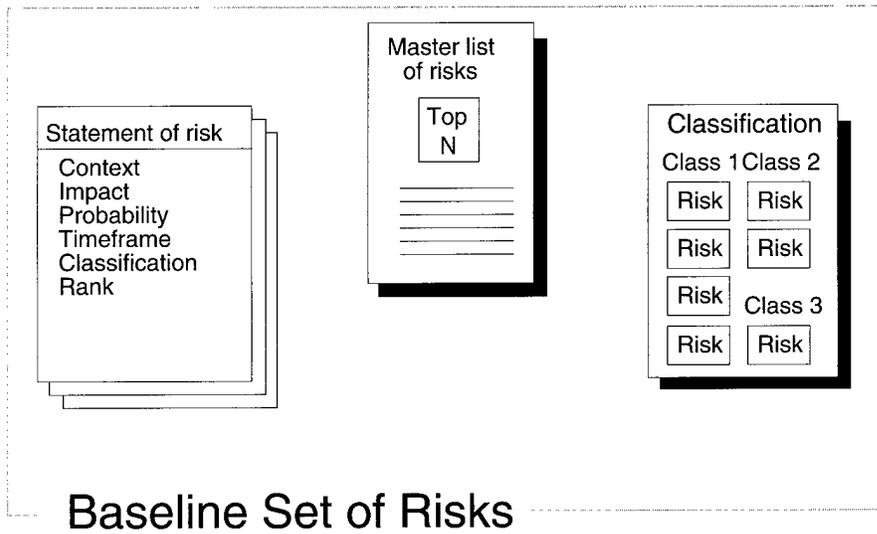
Statement of risk

Context
Impact
Probability
Timeframe
Classification
Rank

**Master list
of risks**

Top
N

Classification

Class 1 Class 2

Risk Risk

Risk Risk

Risk Class 3

Risk Risk

Baseline Set of Risks

Section 1

Baseline Identification and Analysis Description

Introduction

Baseline identification and analysis is a process for establishing a baseline set of risks early in a project. It produces a "snapshot" of all the risks that exist at that particular point in time. It consists of a concentrated, coordinated sequence of methods and tools to identify and analyze all the currently known risks to the project. The selection of methods and tools used in this process is driven by the project's needs and how well project personnel can accomplish the purpose of each activity using those methods. Typically, baseline identification and analysis is followed by **Baseline Planning** [Chapter A-5], in which mitigation plans are developed for the top N risks or risk areas.

Diagram

This diagram shows the inputs and outputs for baseline identification and analysis.
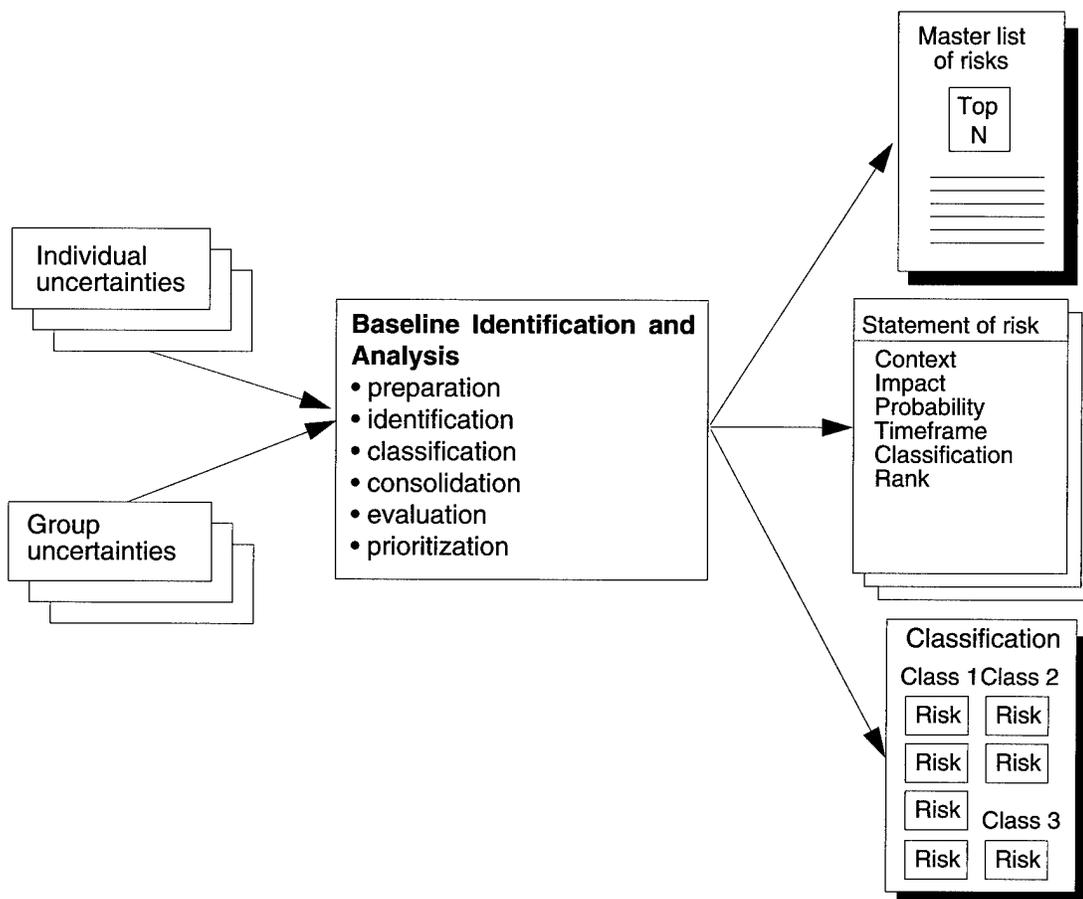
Personnel Requirements

Baseline identification and analysis is expected to be done by a group with a facilitator (whether from the project or eternally supplied) who will lead the group sessions.

Section 2

When to Use

When to Use

Use this method

- early in a project's life cycle to establish a baseline of currently-existing risks—e.g., during requirements definition (design and code phases are also acceptable) or during any major cycle of an interactive system development model
- before submission of a project proposal to identify major risks the proposal should address or to decide if the proposal should even be submitted

Note: This can also be used thereafter to periodically re-establish the baseline as major project milestones are met (e.g., during system requirements or system design reviews). This would provide the project manager with a periodic "big picture" overview of where the project stands in terms of probable success. If done, it is recommended that the baseline be re-established semi-annually (or at major project milestones), as it does take a considerable amount of time to accomplish.

Constraints

The methods and tools selected to implement this process come with their own constraints and benefits. Weigh these carefully when making the decision of which ones to use.

Benefits

This method

- provides a critical mass of risks with which to get started in risk management
- provides a "snapshot" of all the currently known risks in the project and their relative importance, allowing effective allocation of resources for mitigation
- if used more than once, provides a periodic checkpoint of the overall state and probable success of the project

Section 3

Conducting Baseline Identification and Analysis

Overall Procedure

This table describes the activities or steps to be followed.

Note: The order of some of these steps can be changed to suit the project. Classification and consolidation can be done after evaluation. Be aware of the inputs and outputs of the methods when you change the order.

Step	Action
1	**Prepare: select methods, participants, and schedule**. Select the appropriate methods for each activity in baseline identification and analysis (see Section 4). Select personnel to participate in each activity, considering their experience, availability, and the requirements for the selected method. Build a schedule for participants, facilitator(s), and facilities and notify everyone of their responsibilities.
2	**Identify**. Generate risk statements and context. The focus is on quantity and quality of risk statements and on breadth and depth of coverage. The purpose of this step is to quickly identify all the known risks to the program.
3	**Classify**. Group risks into related sets. This provides for easier evaluation and management, and supports the effective allocation of resources. Chose the structure and basis for classification carefully as it should be used for the duration of the project.
4	**Evaluate**. Evaluate the probability, impact, and timeframe for each risk. An overall evaluation for a set of risks can also be done.
5	**Consolidate**. Within each set or class of risks, eliminate duplicate, combine similar risks, and describe a common "theme" for each set. This provides a high-level view of the project's risks and supports later Track [Chapter 7] and Control [Chapter 8] functions by allowing some risks to be tracked as sets. *Note*: Risks are duplicates if they essentially refer to the same thing. The wording does not have to be identical but the intent of the risks must be the same. Consider both the risk statement and the context when looking for duplicates.
6	**Select and prioritize the top N**. Using the results of evaluation, select the top N risks to the program (the most important risks), and prioritize them relative to each other.
7	**(Optional) Prepare and give results briefing**. Prepare a briefing on the results of the baseline identification and analysis for the project. At a minimum, include • a list of all risks and risk sets and their evaluation attributes • the top N risks and their relative priority • next steps

What Kind of Schedule?

The schedule for baseline identification and analysis depends on the methods selected. For example, **Taxonomy-Based Questionnaire Interviews** [Chapter A-33] take about three hours for each peer group interviewed. If **Voluntary Risk Reporting** [Chapter A-39] and the **Risk Form** [Chapter A-26] are used to solicit risks, then a period of time, e.g., a week, might be set aside for people to submit risks. Additional time periods must be set aside for the other activities of classification, evaluation, consolidation, and prioritization.

Who Does These Activities?

In general, project personnel participate in the activities, although many of the methods require at least one facilitator, and some, such as **Taxonomy-Based Questionnaire Interviews** [Chapter A-33], may require several facilitators (i.e., a baseline team). Another consideration is using specific project personnel for specific activities. A suggested allocation of activities to project roles is provided in the table below.

Activity	Project Roles
Prepare (select methods, participants and set schedule)	Project manager, facilitator, SEPG member (preferably not from the project), technical leads
Identify	All project personnel or a cross-section
Classify	Technical leads, project manager, any of the participants in identification if group methods are used
Evaluate	Whoever identifies the risks. The project manager and technical leads may also want to review and revise evaluations, but if they choose to do so, they should note what changes were made and why.
Consolidate	Technical leads
Prioritize	Project manager and technical leads. Project personnel can also participate through such methods as top 5.
Give results briefing	Project manager should give the briefing to project personnel, although the facilitator may also assist.

Documenting Results

It is important to document the results of the baseline identification and analysis. Undocumented or uncollected information is too easily lost. If a database is being used, all data should be entered into the database, particularly the context for the risks. Otherwise paper-based repositories are necessary. All of this information then goes to the baseline planning sessions and to the rest of the Continuous Risk Management activities. An optional step is to brief the project, and perhaps senior management in the organization on the results of the baseline identification and analysis.

Section 4

Considerations for Selecting Methods and Tools

Description

This appendix contains a wide variety of methods and tools. Selecting from these methods and tools to support baseline identification and analysis is not difficult, but it must be done with some considerations for the project. This section shows what methods can be used for each of the activities as well as some of the considerations that should be taken into account.

What Considerations?

There are many considerations for selecting methods to use during baseline identification and analysis. These include
- facilitator requirements
- availability of trained facilitators
- time and resource requirements
- compatibility between inputs and outputs of selected methods
- scope and coverage of the methods
- familiarity of project personnel with the methods (e.g., many of these methods are based on standard quality improvement methods)
- project schedules and milestones

Note: In the long term, an organization should be willing to try several methods and determine which combination will work best within their culture and environment before settling on a standard set of methods.

Methods Summary

Any number of methods and tools can be used to accomplish a baseline identification and analysis. A summary of the possible methods and tools and combinations of methods and tools that could be used and some considerations for selections are presented in the tables below. See the specific method chapters for additional information that should be considered.

Note: Preparation and consolidation have no specific methods or tools and are not included below.

All Activities

This table describes the methods and tools that can be used to support most of the activities in baseline identification and analysis (does not support preparation and consolidation).

Methods and Tools	Considerations
Risk Information Sheet [Chapter A-27]	Simple, easy to use form; can be electronic or paper based

Identification

This table describes the methods and tools for identification of risks.

Methods and Tools	Considerations
Brainstorming [Chapter A-7]—idea generation technique	Unstructured, unpredictable scope of coverage Easy to use (little training required)
Voluntary Risk Reporting [Chapter A-39] with Risk Form [Chapter A-26] and Short Taxonomy-Based Questionnaire [Chapter A-29]—personnel submit all known risks using the risk form as they think of them over some specified period of time	Unpredictable time duration, no indicator of completion Better scope of coverage, easy to use, little or no impact on personnel schedule, does not require a facilitator
Periodic Risk Reporting [Chapter A-19] with Short Taxonomy-Based Questionnaire [Chapter A-29] or Risk Form [Chapter A-26]—required meeting using the risk form to report all known risks.	Impact to personnel schedules, may take more time than a group interview to get all of the risks Better scope of coverage, easy to use, may not require a facilitator
Taxonomy-Based Questionnaire Interviews [Chapter A-33]—peer group interviews using the taxonomy-based questionnaire	Impact to personnel schedule, requires at least one trained facilitator/interviewer Best scope of coverage
Project Profile Questions [Chapter A-25] to tailor the taxonomy (if needed)	Easy to use, shortens the questionnaire by eliminating unneeded questions

Classification

This table describes the methods and tools for classification of risks.

Method or Tool	Considerations
Affinity Grouping [Chapter A-2]—group risks together that "look like they belong." No specific structure used.	Unpredictable results, classes are not likely to be repeatable across projects Easy to use, may not require facilitator
Taxonomy Classification [Chapter A-34]—uses taxonomy as structure for classes	Requires facilitator or trained leader familiar with the taxonomy Predictable, repeatable structure and basis for any project using this method

Evaluation

This table describes the methods and tools for evaluating risks.

Method or Tool	Considerations
Binary Attribute Evaluation [Chapter A-6]—yes or no	May not provide enough distinction between risks Easy to use and fast
Tri-level Attribute Evaluation [Chapter A-38]—high, medium, and low	Reasonable level of distinction between risks Easy to use

Prioritization

This table describes the methods and tools for prioritizing of risks.

Method or Tool	Considerations
List Reduction [Chapter A-15]—use as a preliminary step to shorten a long list	Does not yield a priority—draws a line between important and not important risks Easy to use
Multivoting [Chapter A-17]—determines relative priority among risks	Requires facilitator or trained personnel Standard quality method that most personnel are familiar with
Pareto Top N [Chapter A-18]	Should be used with tri-level attribute evaluation Does not provide explicit priority other than that established by attribute values Easy to use Requires only one person
Potential Top N [Chapter A-23]—use as a preliminary step to shorten a long list	Should be used with top 5 Does not yield a priority Easy to use
Top 5 [Chapter A-37]—gets input from a wide variety of personnel who identified risks	Should be used with binary attribute evaluation Likely to include personal bias Allows for individual voice and expertise

Software Risk Evaluation (SRE)

The SEI Software Risk Evaluation (SRE) [Sisti 94] is a collection of methods that establishes a baseline set of risks. The SRE structures many of the methods and tools identified above into a concentrated timeframe to produce a risk baseline and mitigation strategies. It also includes the use of external expertise to assist in the classification, prioritization, and development of mitigation strategies.

Section 5

Guidelines and Tips

Schedule

It helps to set a preliminary schedule after selecting methods to see what impact that has on personnel selections. Several iterations may be needed to arrive at the optimal mix of methods and personnel.

When multiple days are needed, it is best to use consecutive days of the week, unless it is being performed at geographically dispersed sites. Too much elapsed time distorts the baseline as circumstances and situations change between the first risk identified and the last.

Method Selection

If the selected methods do not appear to be having the desired effect, try a different method on the next baseline or re-baseline effort.

Computer Supports

Computer support for collecting and processing data is extremely useful in avoiding loss of data. It also prevents a loss of time later while waiting for someone to transcribe all the data into a data base or on forms.

A non-technical note-taker with a lap-top computer can be used for recording information. Some editing and refinement of notes is performed afterwards.

Duplicate Risks

Care must be taken not to merge risks that seem similar, but are actually different in the project's eyes. Classifying risks will group similar risks.

Consolidation

When consolidating several risks, make sure the summary statement accurately reflects all the risks. If a single summary statement cannot be made, consider making more than one consolidated set of risks.

Don't lose or throw away the individual risk information. It may be needed later if circumstances change and one of the risks becomes more important.

Baseline Planning

Don't forget the next step—planning. Identifying the "problem" without identifying a "solution" has a tendency to leave the issue unresolved. If you fail to do something with the baseline set of risks, you have wasted nearly all your efforts.

How Do You Know You Have All the Risks?

There is no guarantee that any specific set of methods will yield every existing risk. There are usually some small number of risks that simply cannot be foreseen. The point is to manage all that known risks and minimize the number that could not be foreseen.

How Many Risks is Enough?

Taxonomy-based questionnaire interviews tend to yield between 15-30 risks from each peer group. Four peer groups average about 100-120 risks. Extremely large, diverse projects with large numbers of peer groups have been known to produce over 500 risks during a baseline session.

The best clue to when you have enough is the degree of repetition. If the selected method is no longer yielding any new risks, and shows no promise of yielding new risks, it is time to stop identification and proceed to the next step.

Example: You decide to use the taxonomy-based questionnaire interviews but also wanted to interview everyone. So you partition the software engineers into 7 peer groups with a variety of backgrounds, experience, and seniority in each group. The first group identifies 27 risks, the second group adds 12 new ones, the third group adds 2 new ones, and the fourth adds no new ones at all. At this point, the peer group interviews could be stopped and the current list of risks handed out to the remaining software engineers along with the short taxonomy-based questionnaire. They could submit risk forms for any new risks they can identify.

References

Cited in this chapter:

[Sisti 94]   Sisti, Frank J. & Joseph, Sujoe. *Software Risk Evaluation Method Version 1.0* (CMU/SEI-94-TR-19, ADA290697). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

Chapter A-5

Baseline Planning

Baseline Mitigation Plans
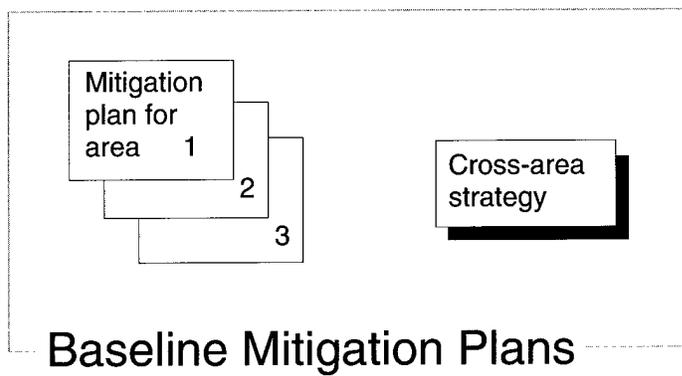
Section 1

Baseline Planning Description

Introduction   The baseline planning method develops integrated mitigation plans for multiple sets of related risks (also referred to as a risk areas or mitigation areas) resulting from **Baseline Identification and Analysis** [Chapter A-4]. Baseline planning is best accomplished as a series of group planning sessions with a follow-on integration session to deal with the sets of risks. Not all baseline risks are actually dealt with; the priority order of sets and individual risks will drive how much planning is done at this time. Other risks and sets of risks may be put on hold until a later time or, as described in **Plan** [Chapter 6], may be accepted or watched.

Note: **Problem-Solving Planning** [Chapter A-24] deals with a single risk or a single set of risks and focuses on developing a detailed, complete task plan for mitigation. The primary focus of baseline planning is on integrating strategies across sets.

Diagram   The following diagram shows the inputs and outputs for baseline planning.
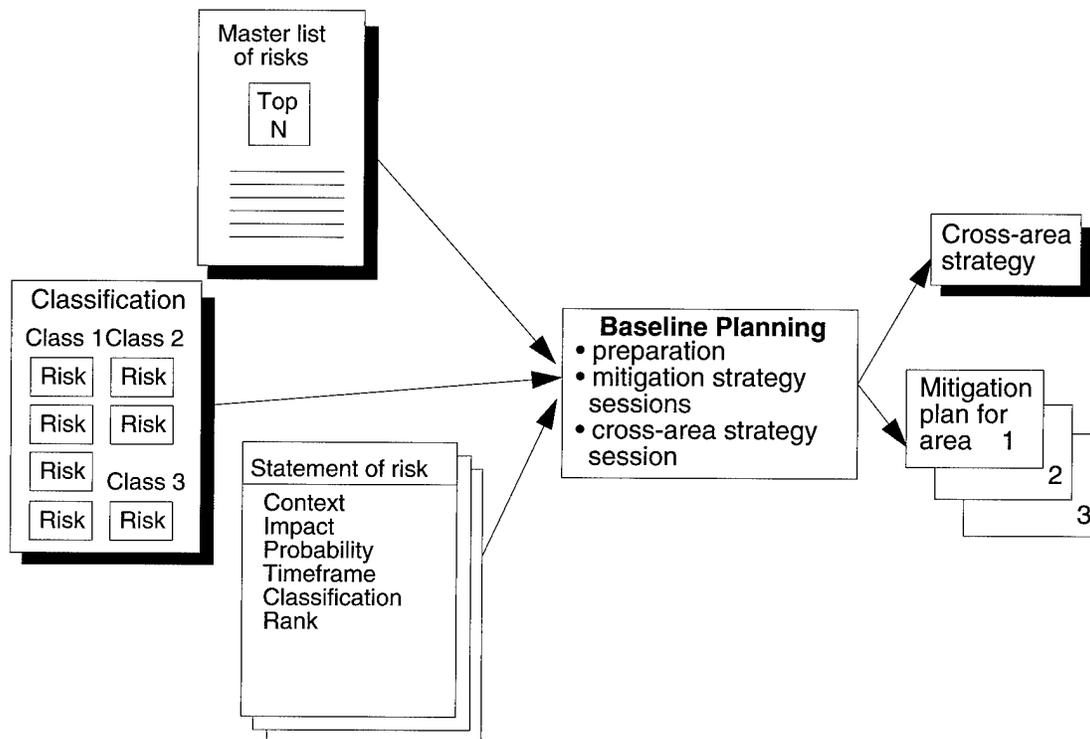
Personnel Requirements   Baseline planning is expected to be done by a group with a facilitator (whether from the project or eternally supplied) who will lead the group sessions.

Section 2

When to Use

When to Use

This method is used shortly after a **Baseline Identification and Analysis** [Chapter A-4], but can also be used at any time to deal with multiple sets of risks. Any method that is used to establish a baseline set of risks and analyze them can be followed by this method. It is important, however, to build baseline mitigation plans as soon as possible after establishing the baseline.

Constraints

This method
- should not be used for minor or less important sets of risks—the resources required for this activity are likely to be higher than the potential impact of a minor risk
- should not be used for a relatively simple set of risks where the solution is obvious

Specific mitigation plans may require additional effort (usually by an individual as opposed to the group) to make the plan implementable (e.g., exact resource requirements and accurate budgets).

Benefits

This method
- supports an integrated, team effort at building complex, integrated risk mitigation plans
- forces a concentrated effort at building mitigation plans for the important sets of risks in a risk baseline in a short time frame. This is necessary to avoid making plans for risks that have changed faster than plans can be built

Section 3

Conducting Baseline Planning

Preparation

The facilitator meets with the project manager to discuss the baseline planning sessions and to determine which sets of risks or mitigation areas to deal with, who should attend, and the schedule for the sessions. The project manager should specify his or her mitigation goals for these areas to be used later as a checkpoint for the mitigation strategies. The project manager's goals should reflect his or her high level view—project success, satisfied customers, controlled budget and schedule.

Mitigation Strategy Session Procedure

This table describes the overall procedure for conducting a mitigation strategy session. One or more sessions are held to deal with the selected risk sets or mitigation areas. Parallel or serial sessions may be used if time and required personnel permit. The length of the session depends upon the skill level of the project personnel (e.g., are they familiar with problem-solving skills, quality methods and tools, etc.) and the complexity of the risk area, but should be between one-half and one full day per mitigation area. Multiple facilitators may be required for parallel sessions.

Note: Like problem-solving planning, the assumption here is that these are risks for which a task plan is required for mitigation. In other words, these are not sets of risks which can be accepted, watched, or dealt with by only watching them.

Step	Action
1	**Explain process**. The facilitator explains the process, reviews the mitigation area and sets expectations for the mitigation strategy session's results.
2	**Analyze mitigation area**. Identify recent changes, root causes, consequences and interrelationships, and any other information that will complete understanding of the risk area.
3	**Set mitigation goals and constraints**. Determine what goals and constraints exist for mitigating this risk area. The project manager's mitigation goals should also be considered at this point.
4	**Identify high-level mitigation strategies**. Expand, decompose, or modify the suggestions as needed. Check back against the causes and consequences to make sure the important ones are being addressed. Reduce the list to the desired set.
5	**Determine actions to implement the strategies**. Given the selected strategies • expand them into a detailed mitigation plan with a list of prioritized actions • identify sequences and dependencies • estimate cost and personnel effort • identify indicators for evaluating progress • estimate a schedule for the actions • where possible, link the schedule and actions back to project milestones and events *Note*: Eliminate any actions that are too costly but make sure there are no dependencies on the eliminated action.

Step	Action
6	**Validate coverage.** Make sure all critical or top N risks and the mitigation goals are addressed by the strategies.
7	**Review, refine, and document.** Review all of the material and make any necessary adjustments to schedule, resources, actions, etc. Identify any other steps that are needed to make this an implementable plan (e.g., assign responsibility for actions, get approval, etc.). Document the results.
8	**Repeat steps 1 - 7.** Repeat these steps for each selected mitigation area until complete.

Cross-Area Strategy Session Procedure

The following table describes the overall procedure for conducting a cross-area strategy session.

Step	Action
1	**Review recommended strategies.** Look across the recommended strategies, actions, schedules, etc. to see if there are any dependencies, conflicts, or potentials for synergistic integration. Review the strategies, actions, schedules, dependencies, costs, and required resources.
2	**Resolve conflicts.** Resolve any conflicts between actions, schedules, or resources.
3	**Prioritize strategies and actions.** Prioritize mitigation strategies and actions as needed to meet resource and schedule constraints.
4	**Document overall plan.** Document the overall plan for the mitigation areas including the prioritized list of strategies and actions, dependencies and sequencing, changes made to each sessions results, and unresolved conflicts that need further attention.

Who Does These Activities?

A facilitator leads all group sessions. Project personnel participate in the sessions according to their areas of expertise (e.g., which risks are they familiar with, what knowledge or background do they have that would help with mitigation planning). A suggested allocation of activities to project roles is provided in the table below.

Activity	Project Roles
Preparation (selecting mitigation areas and participants, and setting schedule)	Project leader and facilitator
Mitigation strategy sessions	A facilitator leads each session. A group of project personnel (which can include the project manager) participates in each session. Outside experts for specific domains may also be used.

Activity	Project Roles
Cross-area strategy sessions	A facilitator leads each session. A group of project personnel (which can include the project manager) participates in this session. A cross selection of personnel from each of the mitigation strategy session groups is recommended.

Section 4

Considerations for Selecting Methods and Tools

Description

As with **Problem-Solving Planning** [Chapter A-24], there are a variety of methods and tools that can be used for each of these activities. Unlike baseline risk identification and analysis, the decision on which tools to use does not have to be made in advance of the session or be consistent for all sessions. Each set of risks and each set of participants may require different methods and tools to be effective. The key here is to be flexible—and this flexibility is generally best achieved through the use of trained facilitators who can adapt to changing needs during the session.

Methods and Tools

The table below lists the possible methods and tools that can be used for each activity in baseline planning as well as some criteria for which ones to use.

Activity	Method or Tool	Considerations
Preparation	Interrelationship Digraph [Chapter A-14]	Shows dependencies between risk areas, determine which areas to tackle first
Mitigation planning sessions	Brainstorming [Chapter A-7]	Generates list of root causes Generates list of possible strategies Generates list of actions
	Cause and Effect Analysis [Chapter A-8]	Determines consequences and causes of the risks' interrelationships
	Cost-Benefit Analysis [Chapter A-11]	Shows differences between strategies and actions
	Gantt Chart [Chapter A-12]	Documents schedule of actions
	Goal-Question-Measure [Chapter A-13]	Establishes indicators to evaluate progress and success
	Interrelationship Digraph [Chapter A-14]	Determines risks, consequences, and causal interrelationships
	List Reduction [Chapter A-15]	Reduces list of possible strategies or actions
	Multivoting [Chapter A-17]	Ranks causes in terms of their contribution to the risk area Ranks alternative strategies Ranks possible actions
	PERT Chart [Chapter A-20]	Documents sequence and dependencies of actions
Cross-area strategy session	Cost-Benefit Analysis [Chapter A-11]	Chooses between strategies and actions
	Interrelationship Digraph [Chapter A-14]	Shows how the mitigation plans relate to each other

Software Risk Evaluation (SRE)

The SEI Software Risk Evaluation (SRE) [Sisti 94] is a collection of methods that establishes a baseline set of risks. The SRE structures many of the methods and tools identified above into a concentrated timeframe to produce a risk baseline and mitigation strategies. It also includes the use of external expertise to assist in the classification, prioritization, and development of mitigation strategies.

Section 5

Guidelines and Tips

General

Without baseline planning to help the project on to the next steps, baseline identification and analysis may not be effective. Identifying the "problem" without identifying a "solution" has a tendency to leave the issue unresolved.

Participants

Keep the sessions small, about six people, but include those with the required knowledge and experience.

Participants who know general quality and problem-solving methods are usually quicker and more adept at this activity.

The sessions require having the right people there—project personnel with the skills, background, experience, and knowledge necessary for developing effective plans.

**Success
Measures**

Measures of success and progress must be identified to judge when the mitigation is complete. Without these, it is too easy for the plan to go off-course and become ineffective without anyone realizing it.

**Cross-Area
Strategy
Session**

The cross-area strategy session may not be necessary if the same personnel participate in all of the sessions or if the risk areas are so disjoint as to have no overlap in strategies and actions.

Management can use the results to modify the project plan. Mitigation plans for the top N risks or risk areas determined by baseline identification and analysis will generally be significant enough to impact the project plan.

Tool Support

Computers (word processors, spreadsheets, databases, etc.) should be used as much as possible to cut down on the paperwork and data transcription process.

Scheduling

Risks are not static—it is vital that baseline planning occur as soon as possible after the **Baseline Risk Identification and Analysis** [Chapter A-4]. Significant delays may require re-evaluation and prioritization of risks due to changes in circumstances and situations. Finally, delay means the project is less likely to be able to take effective mitigation action.

References

Cited in this chapter:

[Sisti 94]

Sisti, Frank J. & Joseph, Sujoe. *Software Risk Evaluation Method Version 1.0* (CMU/SEI-94-TR-19, ADA290697). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

Chapter A-6

Binary Attribute Evaluation

Evaluation Form			
Risk	**Significant Impact**	**Likely to Occur**	**Near-term Timeframe**
Statement of risk A	✓		✓
Statement of risk B	✓	✓	
Statement of risk C		✓	
• •			

Section 1

Binary Attribute Evaluation Description

Introduction

Binary attribute evaluation is a simple method used to evaluate the impact, probability, and timeframe of a risk, providing a basic level of qualitative analysis for risks. The attribute values for each risk are determined based on specific definitions and answers to related questions. Risk attribute values are

- *impact*: significant or insignificant
- *probability*: likely to occur or not likely to occur
- *timeframe*: near-term or far-term.

Diagram

The following diagram shows the input and output of the binary attribute evaluation method.
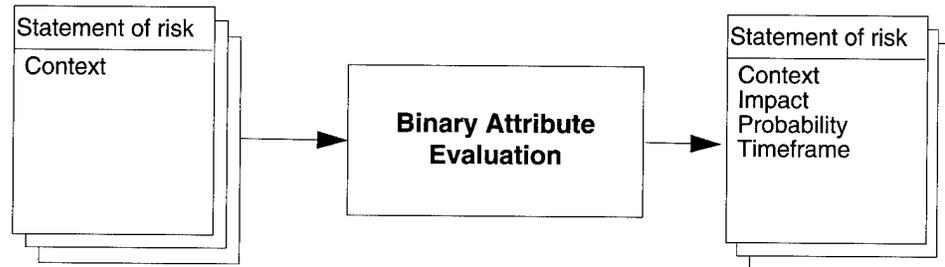
Personnel Requirements

Binary attribute evaluation can be completed by an individual or a group. If performed by a group of three or more, one person should be the facilitator and recorder (but he or she could still participate or contribute).

Section 2

When to Use

When to Use

Use this method
- as a first step in analysis
- when you need to discriminate among a large number of risks such as during **Baseline Identification and Analysis** [Chapter A-4].
- following the use of **Taxonomy-Based Questionnaire Interviews** [Chapter A-33].

Constraints

This method is not quantitative. It uses a qualitative binary approach. Many risks can have the same evaluation yet the degree of each attribute may be different. It cannot distinguish between risks when this occurs.

Example: Risk A and Risk B may both be evaluated as having a significant impact, likely to occur, and in the near-term timeframe. However, for Risk A the impact is a schedule delay of 2 months and for Risk B the impact is that the system will fail integration and test.

Benefits

This method
- is simple. All steps are straightforward.
- does not require resource-intensive activities. The method works with the knowledge the participants possess.
- is quick. Evaluation can be accomplished in a single session.

Section 3

Conducting a Binary Attribute Evaluation

**Attribute
Definitions
and Criteria
Questions**

A risk is *significant* if the impact will seriously disrupt the process, degrade the product, or threaten project success.

A risk is *likely to occur* if it is more probable than not.

A risk is *near-term* if action is required soon.

Note: Attribute values are determined by asking a set of criteria questions for each attribute as seen in the procedure table below.

**Individual vs.
Group**

The following two tables provide procedures for conducting binary attribute evaluation as an individual and with a group. The group procedure will include the procedure for individuals for those steps which are conducted by the individual.

**Individual
Evaluation
Procedure**

The following table describes how an individual evaluates each risk.

Step	Action
1	**Review risks for understanding**. Ensure you understand the statement of risk and context for each risk.
2	**Review attribute definition and questions**. Ensure you understand the definitions for • significant impact • likely to occur • near-term timeframe
3	**Evaluate the impact of the risk**. Mark the impact of the risk *significant* if the answer to any of the following criteria questions is yes. • Will any user see the impact of this risk in terms of performance? function? quality? • Will the project/company see the impact of this risks in terms of budget? schedule?
4	**Evaluate the likelihood of the risk**. Mark the likelihood of the risk *likely to occur* if the answer to any of the following criteria questions is yes. • Have you seen this occur in similar circumstances? • Are there conditions or circumstances which make this risk more likely to occur than not?
5	**Evaluate the timeframe of the risk**. Mark the timeframe of the risk *near-term* if the answer to any of the following criteria questions is yes. • Will the project be impacted soon? • Does this require a long lead-time solution? • Must the project act soon?
6	**Repeat Steps 3-5 for each remaining risk**.

Group Evaluation Procedure

This table describes the procedure for a facilitator(s) conducting a binary attribute evaluation with a group. When this method is used with a group, the results need to be merged to reach a single value for each attribute (extreme evaluation).

Step	Action
1	**Explain individual evaluation procedure**. The facilitator describes to participants how they should evaluate the risks.
2	**Conduct individual evaluation**. Each participant individually evaluates each risk (see individual evaluation procedure).
3	**Select extreme evaluation**. Each participant will have selected one of eight possible combinations for the attribute values. Select the participant evaluation that is the most extreme (see extreme evaluation table).
4	**Record extreme evaluation**. The facilitator records/documents the extreme evaluation with statement of risk and context information.

Note: Participants are not involved in Steps 3-4 and therefore may leave after the completion of Step 2.

Extreme Evaluation

The order of the attributes is important. The attribute values act like a series of filters in evaluating risks. Risks evaluated as significant are considered more important than those that are insignificant. Risks that are significant and likely are more important than those that are insignificant or significant and unlikely, etc. The following table illustrates the possible evaluation values. They are listed in order from most extreme (top) to least extreme (bottom).

Significant?	Likely to Occur?	Near-term?	Evaluation Values
Yes	Yes	Yes	Significant, likely, near-term
		No	Significant, likely, far-term
	No	Yes	Significant, unlikely, near-term
		No	Significant, unlikely, far-term
No	Yes	Yes	Insignificant, likely, near-term
		No	Insignificant, likely, far-term
	No	Yes	Insignificant, unlikely, near-term
		No	Insignificant, unlikely, far-term

Example: Three participants evaluated a risk as follows:
- participant 1: significant, unlikely, near-term
- participant 2: insignificant, likely, near-term
- participant 3: significant, unlikely, far-term

Using extreme evaluation, participant 1's evaluation would be selected and the risk would be recorded as significant, unlikely, and near-term.

Note: The rationale behind using the extreme value is to preserve the individual voice—the person who might have unique knowledge about a risk.

Section 4

Binary Attribute Evaluation Tools

Sample Form   Below is a sample of an evaluation form each participant would fill out.

Evaluation Form

Risk	Significant Impact	Likely to Occur	Near-term Timeframe
Statement of risk A	✓		✓
Statement of risk B	✓	✓	
Statement of risk C		✓	
• •			

Key:

✓	Attribute value is yes

	Attribute value is no

Example: Risk A is evaluated as having a significant impact, not likely to occur and in the near-term timeframe. Risk B is evaluated as having significant impact, likely to occur, and in the far-term timeframe. Risk C is evaluated as having an insignificant impact, likely to occur, and in the far-term timeframe.

Using Binary Numbers To Select Extreme Evaluation

If the three attributes of evaluation (impact, probability and timeframe) are considered as a binary number, selecting extreme evaluation can be simplified.

2^2	2^1	2^0

Significant (impact)   **Likely (probability)**   **Near-term (timeframe)**
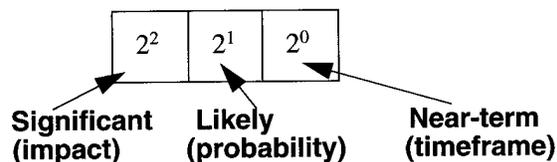
In the extreme evaluation worksheet, let the presence of a check mark for "impact" = 2^2, for "probability" = 2^1, and for "timeframe" = 2^0.

Binary Numbers Example

A risk that is evaluated by a participant as
- significant impact (2^2)
- not probable (0^1)
- near-term timeframe (2^0),

The binary number = 101, or, in decimal, $2^2 + 0 + 2^0 = 4 + 0 + 1 = 5$.

If another participant evaluated the same risk as
- significant impact (2^2)
- probable (2^1)
- far-term timeframe (0^0),

The binary number = 110, or, in decimal, $2^2 + 2^1 + 0^0 = 4 + 2 + 0 = 6$.

The extreme evaluation, assigned by one of the participants, is easily selected as "6," which is interpreted as "*significant* impact, *likely* probability, and *far-term* timeframe."

Section 5

Guidelines and Tips

General

As a first attempt at analysis, binary attribute evaluation works well, especially on a large number of risks. It requires few resources and helps to highlight which risks need a more detailed level of analysis.

Experience with the **Baseline Identification and Analysis** [Chapter A-4] shows that 30 minutes is sufficient for an individual to evaluate a set of 20-25 risks.

Providing participants with a one-page handout containing the attribute definitions and questions helps them to remember the definitions as they evaluate each risk.

Refining Criteria Questions

The results will be more useful if the project refines the criteria questions with questions that make sense to the project. The more specific the criteria are, the easier it will be for participants to evaluate the risks.

Automated Support

For group applications, having a computer application available which automatically selects the extreme evaluation saves times. A simple spreadsheet can save time and reduce error.

Chapter A-7

Brainstorming[1]

**List
of
ideas**

1. Brainstorming was pioneered by Alex Osborn [Osborn 53].

Section 1

Brainstorming Description

Introduction

Brainstorming is a group method for generating ideas, which can be input to other methods for grouping, prioritizing, or evaluating. Participants verbally identify ideas as they think of them, thus providing the opportunities for participants to build upon or spring off each others' ideas. Criticism or evaluation of ideas is not performed at this time. Classic or verbal brainstorming is described here, although other variations are summarized.

Diagram

The following diagram shows the input and output for brainstorming.

```
Creative      →    Brainstorming    →    List of
 energy                                   ideas
```
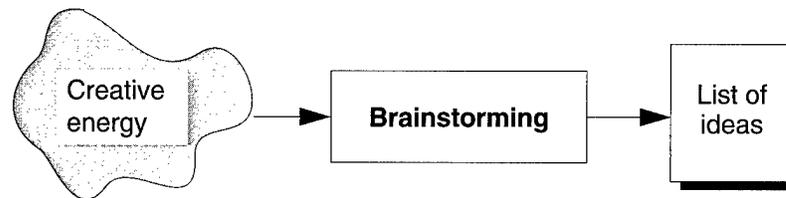
Personnel Requirements

Brainstorming can be done by an individual or a group. If performed by a group of three or more, one person should be the facilitator and recorder (but he or she could still participate or contribute).

Section 2

When to Use

When to Use

Use brainstorming whenever there is a need to produce a list of ideas or alternatives. It can be used during planning to generate a list of mitigation strategies, possible causes for the risk, or areas of impact of the risk.

It is also used during risk identification, in a structured manner, to identify risks (See **Taxonomy-Based Questionnaire Interviews** [Chapter A-33] for discussion of that particular type of brainstorming).

Constraints

This method
- is best used within a small group (i.e., fewer than nine people [Lumsdaine 90])
- requires a skilled facilitator to deal with conflict and negative emotions that may surface and must be controlled; dominating personalities that could take over; shy people who need to be encouraged to contribute; sidetracking into unproductive issues and topics

Benefits

This method
- does not require training of the participants
- is an enjoyable exercise
- generates a lot of ideas in a short amount of time

Section 3

Conducting a Brainstorming Session

Procedure

This table describes the process for conducting a brainstorming session with a group and a facilitator. Individual application generally follows the same basic steps but all steps are performed by the same person.

Step	Action
1	**Discuss issue or risk**. Facilitator presents issue or risk for which ideas are to be generated and ensures it is understood by all.
2	**Explain process**. Facilitator explains brainstorming process and reiterates the rules: • Do not judge or criticize the ideas of the speaker. • Encourage wild ideas or thinking outside the box. • Build on the ideas of others (if done by a group). • Go for quantity of ideas. • Have fun!
3	**Generate ideas**. Ideas are generated by the participants using one of the following variations [Xerox 92]: • unstructured: Call out ideas spontaneously. • round-robin: Each participant takes a turn, in order, to state an idea.
4	**Record ideas**. Facilitator writes the ideas on some visual medium in sight of all participants (flip-chart, dry-erase board, viewgraphs, sticky-notes, etc.).
5	**Review list**. All participants review the list for clarity and understanding. Revise any words as needed.

Note: Grouping, prioritizing, and otherwise dealing with the resulting list of ideas can be done with any number of analysis methods such as **Affinity Grouping** [Chapter A-2] or **Multivoting** [Chapter A-17].

**Unstructured
vs. Round-
Robin**

The following table summarizes the advantages and disadvantages of the two variations
(step 3 in the above procedure) for submitting ideas.

Variation	Advantage	Disadvantage
Unstructured	Spontaneous Creative Easier to build on other's ideas	Dominating personalities take over. Too many simultaneous talkers can lead to lost ideas.
Round-Robin	Difficult for one person to dominate Yields a more focused discussion Everyone encouraged to participate	Hard to wait for a turn Loss of energy possible Reluctance to let go of one's turn Not as easy to build on others' ideas

**Other
Variations**

There are many variations to the classic verbal style of brainstorming. One source of variations is Lumsdaine's *Creative Problem Solving* [Lumsdaine 90], from which the following table is summarized.

Variation	Advantages	Disadvantages
Written variations, also called brainwriting: written idea generation instead of verbal	Can be used with larger groups (>9 people) Controls dominators and sidetracking Lets shy people contribute Reduces pressure to conform	Does not allow for direct verbal interaction Produces fewer ideas
Interactive (combines classic and written techniques): alternate periods of silent idea writing with verbal sharing	Large quantity of higher-quality ideas Can be used in larger groups (>9)	Can be very complex and difficult to facilitate
Force-fitting techniques: methods to stimulate creativity that may require temporary departure from problem at hand	Encourages idea generation Good to use when group gets "stuck"	May add to time required for effort

Section 4

Guidelines and Tips

Timing

Keep the session short (15-45 minutes), but allow time for everyone to contribute their ideas.

**Deciding
When to Stop**

There are three possible rules to follow:

- Stop if more than 30-60 seconds pass without any contributions (good for short sessions).
- Set a time limit (30-45 minutes) and stick to it unless the ideas are still flowing freely, in which case add 5 more minutes at a time.
- Set a number of "passes" for round-robin contributions then switch to a specified time period for open contributions.

Note: using a fixed time-frame may require intervention to stimulate creativity when participants run down.

References

Cited in this chapter:

[Lumsdaine 90]

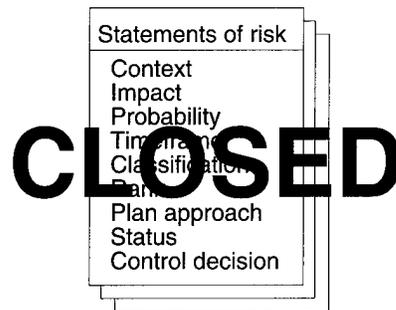Lumsdaine, Edward & Lumsdaine, Monika. *Creative Problem Solving*. New York: McGraw-Hill, 1990.

[Osborn 53]

Osborn, Alexander. *Applied Imagination; Principles of Creative Thinking*. New York: Scribner, 1953.

[Xerox 92]

Xerox Corporation and Carnegie Mellon University. *The University Challenge: Problem-Solving Process User Manual*. Stamford, Ct.: Xerox Corporation, 1992.

For more information on brainstorming, see the following:

[Scholtes 88]

Scholtes, Peter R. *The Team Handbook: How to Use Teams to Improve Quality*. Madison, Wi.: Joiner Associates, 1988.

Chapter A-8

Cause and Effect Analysis[1]

Section

1. Cause and effect analysis is derived from the work of Dr. Kaoru Ishikawa (president of Musashi Institute of Technology in Tokyo, previously Professor of Engineering at the Science University of Tokyo), who developed the Ishikawa (or fishbone) diagrams described in this chapter.
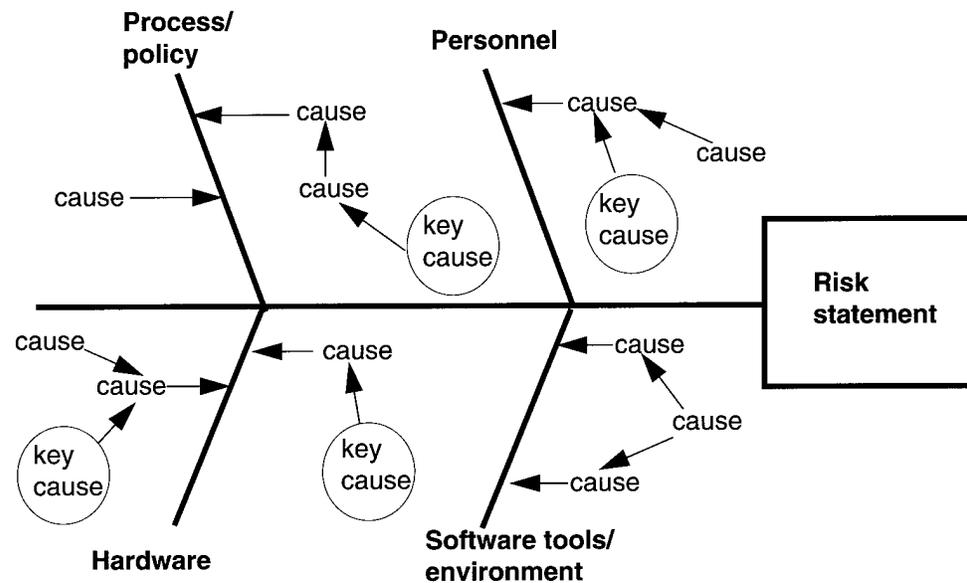
Section 1

Cause and Effect Analysis Description

Introduction   Cause and effect analysis is a method for diagramming the relationships and interrelationships between a risk and the many factors that can cause it. It can also be used for a related set of risks to determine the collective set of causal factors.

Diagram   The following diagram shows the inputs and outputs for cause and effect diagrams.
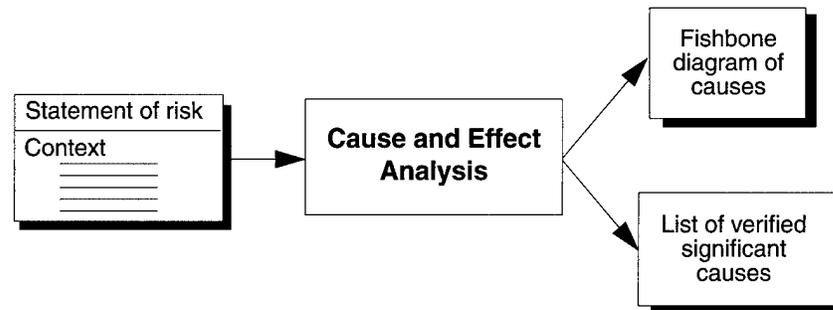
Personnel Requirements   Cause and effect analysis can be done by an individual or a group. If performed by a group of three or more, one person should be the facilitator and recorder (but he or she could still participate or contribute).

Section 2

When to Use

When to Use

Cause and effect analysis can be used
- to identify and verify the factors which are causing a risk or set of risks.
- to identify the required factors for a successful mitigation strategy.

Constraints

Since this method uses brainstorming to help identify the factors populating the diagram, the same constraints that apply for brainstorming are also a factor here.

This method
- should be used with a small group (e.g., less than nine people [Lumsdaine 90])
- requires a leader with good facilitation skills to deal with conflict and negative emotions that may surface and must be controlled; dominating personalities that could take over; shy people who need to be encouraged to contribute; sidetracking into unproductive issues and topics

Benefits

This method
- documents the knowledge of a group of people relative to what's causing the risk or the factors needed for a successful mitigation strategy
- is an easily-understood graphic that is more meaningful than a simple list
- can easily be done by an individual as well as a group

Section 3

Performing Cause and Effect Analysis

Procedure

The table below describes the process for conducting a cause and effect analysis session with a group. Individual application generally follows the same basic steps, but all steps are performed by the same person.

Step	Action
1	**Discuss item for analysis**. Facilitator presents risk or mitigation strategy for which causes are to be identified, and ensures that all participants understand it.
2	**Explain process**. Facilitator explains cause and effect process.
3	**Construct fishbone structure**. Facilitator diagrams the basic fishbone structure with the risk or strategy at the right end of the board or paper and the main factors on the major "ribs." Major factors can include the following [Xerox 92], [Scholtes 88]:[a] • people • equipment or instruments • environment • material • methods, process, procedures • management
4	**Add cause factors to fishbone structure**. On each of the major ribs or factors, the facilitator writes the factors the participants consider to be causes. Brainstorming or other data collection methods can be used to identify these.
5	**Identify the most significant causes (or combinations)**. Determine which of the causes or combinations of causes are the most significant contributors to the risks and mark them with circles (e.g., discuss and vote). Collect additional information to verify that causal relationship, if necessary.

a. See also Hertz, Paul. *Manual for Training in the Deming Method*. Paul Hertz Group, Inc., 1988.

Section 4

Cause and Effect Analysis Tools

Fishbone Diagram

Fishbone diagrams can be drawn on dry-erase boards, flip charts, overheads, or be computer generated. The basic structure is simple: a "head" (risk being analyzed) and the "ribs" or major factors, usually four with an optional "tail."

Sample Fishbone

This sample fishbone shows a risk and the causes that are leading to the risk. Significant causes are circled.
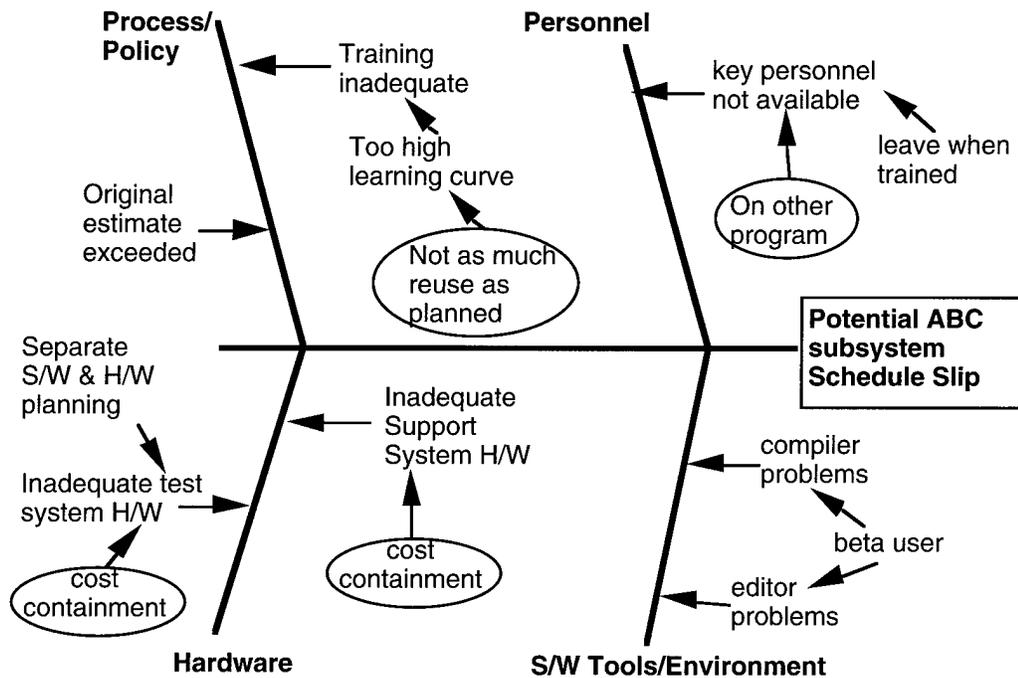
Section 5

Guidelines and Tips

Other Uses

Less disciplined use of the method (related ideas and issues can be added to the diagram as well as causes) can support structured discussion of the risk or strategy.

Joint Causes

Mark any causes which may be under the jurisdiction of another organization. Joint mitigation of the risk may then be required.

References

Cited in this chapter:

[Lumsdaine 90]

Lumsdaine, Edward & Lumsdaine, Monika. *Creative Problem Solving.* New York: McGraw-Hill, 1990.

[Scholtes 88]

Scholtes, Peter R. *The Team Handbook: How to Use Teams to Improve Quality.* Madison, Wi.: Joiner Associates, Inc., 1988.

[Xerox 92]

Xerox Corporation and Carnegie Mellon University. *The University Challenge: Problem-Solving Process User Manual.* Stamford, Ct.: Xerox Corporation, 1992.

Chapter A-9

Closing a Risk

Statements of risk

Context
Impact
Probability
Time frame
Classification
Plan
Plan approach
Status
Control decision

CLOSED

Section 1

Description of Closing a Risk

Introduction

Closing a risk is a procedure for formally documenting information about a risk that has been successfully mitigated, has been accepted, or has become a problem.

Diagram

The following diagram shows the inputs and outputs for closing a risk.
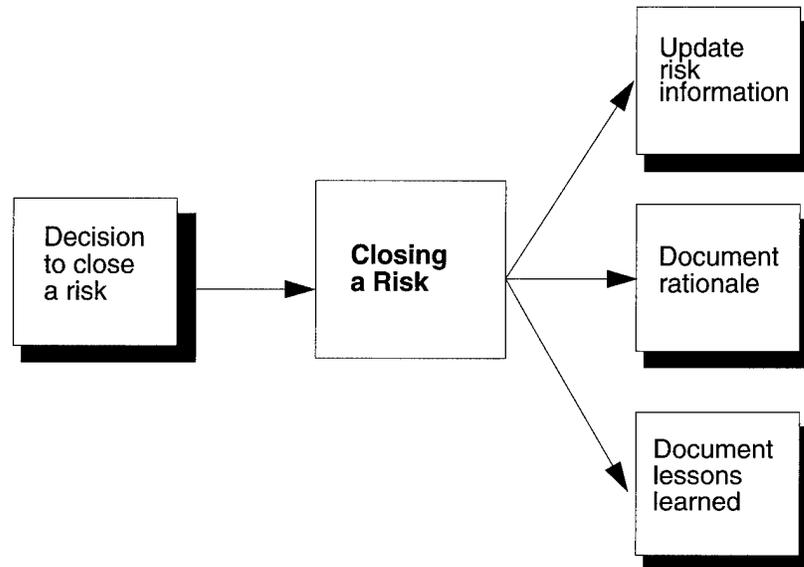
Personnel Requirements

Closing a risk requires actions by the person who is responsible for tracking the risk. The need to close a risk is triggered by achieving a set of exit or closure criteria defined by project personnel during the **Plan** function [Chapter 6] of the risk management paradigm. The decision to close a risk is made during the **Control** function [Chapter 8] of the paradigm. Closing a risk can require approval from a predefined level of project management (e.g., project manager, team leader, etc.) if appropriate.

Section 2

When to Use

When to Use

Use this method

- when the probability, impact, or risk exposure are either near zero or below an acceptable threshold as defined in the mitigation goal. The risk is considered to have been successfully mitigated and is accepted.
- when conditions have changed such that the risk is no longer relevant to the project
- when a risk becomes a problem and must be tracked as such

Constraints

Setting thresholds for qualitative measure data can be difficult and may result in a risk being closed prematurely.

It can be difficult to gain consensus from project personnel on whether to close a risk.

Benefits

The project will develop a database of lessons learned that will help project personnel mitigate future risks. Project personnel will have data about which mitigation strategies worked and which didn't.

Risk relationships and dependencies that were not obvious will be kept in the project database for future reference.

Relevant analysis data, especially the cost and benefits of the mitigation plan, will be kept in the project database.

The project will have an historical record of all risk management actions that were taken.

Section 3

Closing a Risk

Procedure

The following table describes how to close a risk.

Step	Action
1	**Determine risk status**. Project personnel determine the status of a risk during the Control function [Chapter 8]. This can be done formally or informally and usually requires consensus among the project personnel (e.g., during a project meeting). Closing a risk is executed by the person responsible for the risk. Those risks marked for closure are addressed by the following steps. *Note*: If the risk being closed is a part of a set of risks, then an informed decision either to close the set or to close selected risks within the set must be made.
2	**Update risk information**. Information related to the closing of a risk is added either to the Risk Information Sheet [Chapter A-27] or to another appropriate risk documentation tool which is chosen by project personnel.
3	**Obtain proper approval**. Project personnel must follow the designated procedure for obtaining appropriate approval for closing a risk (e.g., signature from team leader, project manager, etc.). Risks that were transferred or delegated need approval from all affected parties before they can be closed.
4	**Document the lessons learned and rationale**. The lessons learned from watching or mitigating the risk or set of risks and the rationale for closing the risk or set should be captured upon closure. This information may be relevant to the present project or to other projects within the organization.

Note: If a closed risk resurfaces at a future time, there should be a project procedure in place indicating how to handle the situation. Either the old risk should be reopened or a new risk that references the old one should be opened. Important information and trends can be lost if the linkages are not maintained.

**Consider-
ations for
Closing a Risk**

The following questions can be used to help guide project personnel in determining whether to close a risk:

- Is the probability either near zero or below an acceptable threshold? If the answer is yes, then the risk can be accepted and closed.

- Is the impact either near zero or below an acceptable threshold? If the answer is yes, then the risk can be accepted and closed.

- Is the risk exposure either near zero or below an acceptable threshold? If the answer is yes, then the risk can be accepted and closed.

- Have conditions changed such that the risk can be accepted (i.e., the project is now willing to live with the problem if it should occur)? If the answer is yes, then the risk can be closed.

- Have the mitigation goals been met? If the answer is yes, then the risk can be closed.

- Has the risk become a problem? If the answer is yes, then the risk can be closed and then tracked as a problem.[1]

**Documen-
tation of
Lessons
Learned**

The following list contains examples of the types of lessons learned that should be retained in an organization's database:

- failed mitigation plans and the reasons for their failure. Keeping this information can prevent costly repetitions of mistakes in other projects.

- risk relationships and dependencies that were not obvious. This list will include risks that were not identified early in the process, but which surfaced later.

- successful mitigation plans and why they were successful. Keeping this information can make successful mitigation strategies available to other projects within an organization.

- relevant analysis data, especially the cost and benefits of the mitigation plan

---

1. With the close relationship between risks and problems, risk tracking systems and problem tracking systems can be combined. Problems are risks with probabilities of 100%.

Section 4

Tools for Closing a Risk

**Risk
Information
Sheet**

The decision to close a risk and the required approval are documented on the chosen form or in the chosen database by project personnel. The example in this section employs a **Risk Information Sheet** [Chapter A-27] to document information about closing a risk.

**Sample Risk
Information
Sheet**

The following is an example of a completed risk information sheet. This particular example is from **Life-Cycle of a Risk** [Chapter 12] which describes a scenario for a typical risk.

ID ABC104	Risk Information Sheet	Identified: __2/14/ 96

Priority 5	**Statement** The estimated schedule and resources for integration
Probability High	& test at the test facility may be inaccurate; delays in testing &
Impact High	insufficient testing time could lead to a defective product.

	Origin Smith	**Class** Program constraint: Resources	**Assigned To:** ____Jones
Timeframe Near			

Context
The estimates used for System ABC were based on those used for the LMN Project,
which, at the time, appeared to be good estimates. However, the lessons learned from
that project included one about inadequate time and resources at the test facility.
Project LMN's delivered system is similar to System ABC and we're going to be
using the same test facility.

Mitigation Strategy
1. Jones to review/revise unit & integration testing estimates based
   on LMN & 2 successful projects. Due 4/15.
2. Assign Green to get current status & projected completion dates for test facility
   upgrades. Due 3/11.
3. Jones check with QA & CM about how well things are going in their areas. Due 5/1.
4. Jones revise and resubmit test facility schedules based on above actions. Due 6/20.

Contingency Plan and Trigger

Request a delay in scheduling from the
customer equal to 1/2 the % slip seen by
LMN Project (assuming 50% slip due to
CM/QA problems we don't have)

If we can't get accurate
estimates OR the revised
schedule is rejected

Status	**Status Date**
• Software Z purchase delayed indefinitely. Webster to try and free up paperwork (due 4/15/96)	3/12/96
• I&T estimate revisions are sound, but means delay in testing start (2 months) and 2X integration time. Special meeting called (due 4/24) to review project impacts. Software Z paperwork still locked up. Jones to look for work-around (due 4/27)	4/20/96
• Personnel adjustments and overtime = no schedule slip. Completion sequence changed. Jones to review test facility request to see if this affects it. (due 5/27). Software Z available elsewhere. Trying to transfer licensing (due 5/27). CM and QA check out fine.	5/5/96
• System Z installed, tested, and approved for use. Revised facility request approved.	6/30/96
• Risk closed - integration and testing successfully completed. Risk no longer exists.	9/12/96

Approval A. Jones Mr. Webster/PM	**Closing Date** 9 / 12/ 96	**Closing Rationale** All testing completed successfully; probability = 0.

Sample Lessons Learned

The following is an example of the lessons learned for the risk which is documented on the risk information sheet shown on the previous page. This particular example is from **Life-Cycle of a Risk** [Chapter 12], which describes a scenario for a typical risk.

Lesson Type	Lesson
Unit and integration testing (UIT) estimation	The old UIT method has been used for a long time, but now appears to be outdated. We have documented a new method (see corporate post 1034) and it seems to have an increased accuracy (45% improvement) based on our experience and the judgement of Wiley and Stone, our site experts.
Test facility schedule communication	There was no formal mechanism for communicating test facility upgrade schedules that we know about. This is a hole in the site management procedure that the site manager has corrected, as of this date. It does prove, however, that making assumptions about other managers' schedules without verifying those assumptions is unwise.
Budget impacts on tool purchases	When corporate headquarters shut down the budget on tool purchases and Software Z could not be purchased, word was not communicated to all site and project managers. This gap in policy has been corrected, but it highlights the need for all managers to verify all interdependencies and communicate issues to other project managers. It would have been helpful if the test facility manager had known which other project managers were dependent upon purchasing Software Z.
Return on mitigation investment	We estimate our savings from mitigating this risk as at least 10% of our project budget—$250,000. This is based on our estimation that the delay in integration testing would have been 3 months and the customer would have had to accept a less than desired product. This customer dissatisfaction is an incalculable cost - they do a lot of work with us and might have felt it necessary to look elsewhere. Three pending contracts might have been affected (total $14.3 million).

Section 5

Guidelines and Tips

General

If there is disagreement as to whether a risk should be closed and if a consensus cannot be reached, it is best to leave it open.

Success Criteria

Determining whether a risk meets the success criteria and can be closed usually requires either formal or informal discussion to reach a consensus.

Premature Closing

A risk should not be closed just because an action was taken. Project personnel must determine if the success criteria to close the risk have been met. There is a tendency to close risks early. It is better to leave risks open rather than to close them prematurely.

Classification

Using the same risk classification scheme across multiple projects helps to construct a consistent database of lessons learned.

Chapter A-10

Comparison Risk Ranking[1]

Ranked risks

1 _____
2 _____
3 _____
4 _____
5 _____
•
•
•

Section

1. Comparison Risk Ranking (CRR) was developed by Jerry FitzGerald [FitzGerald 90a] [FitzGerald 90b] as part of an approach to designing controls into computerized systems.

Section 1

Comparison Risk Ranking Description

Introduction

Comparison risk ranking (CRR) is a method in which risks are ranked by comparing the risks, two at a time, to an established criterion or set of criteria (stated in the form of a question). Each risk is compared to every other risk. Each participant in the process casts a vote in each comparison.

Note: There are other, similar methods for conducting paired comparisons [Xerox 92]. This chapter outlines the SEI experience in conducting the CRR method.

Diagram

The following diagram shows input and output for comparison risk ranking.
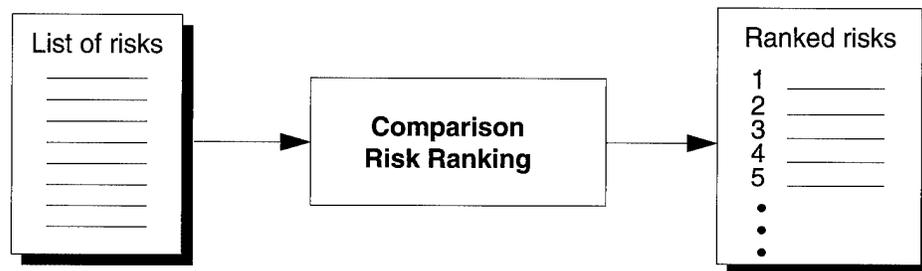
Personnel Requirements

Comparison risk ranking can be done by an individual or a group. If performed by a group of three or more, one person should be the facilitator and recorder (but he or she could still participate or contribute).

Section 2

When to Use

When to Use   CRR can be used when you have a small number of risks (<20) to rank.

CRR can be used when the desired result is an ordered ranking of the risks and there is no need for degree of preference.

Example: Risk A is more important than Risk B. Note that we do not know how much more important Risk A is than Risk B.

Constraints   Conducting a CRR session can become a time-consuming process. The number of comparisons required grows quickly as the number of risks to be ranked increases.

Benefits   The method
- allows decision makers to simplify the prioritization process by focusing on two risks at a time
- allows decision makers to give a preference for the relative degree of loss, urgency, and type of impact without being forced to come up with exact numbers
- provides participants with a structured environment for face-to-face communication about every pair of risks

Section 3

Conducting a Comparison Risk Ranking Session

Procedure

The table below describes the procedure for conducting a comparison risk ranking session.

Step	Action
1	**Explain process and groundrules**. The facilitator explains this process and the following groundrules: • Respect confidentiality, non-attribution. • Talk about issues, not persons or agencies. • Discuss risks, don't solve the problem (for now). • Build or clarify, do not criticize. • Let all participants take part. • Keep to the schedule. • Have fun and get it done.
2	**Select comparison criteria and develop comparison question**. Selecting the comparison criteria depends on what's important to the project: cost? performance? schedule? training? etc. The participants must decide what criteria are appropriate to use for ranking based on what's important to the project. *Examples*: • Which risk has a more significant impact? • Which risk is more likely to occur? • Which risk has a greater impact on performance?
3	**Conduct comparison and record votes for each pair of risks**. The participants perform the pairwise comparisons: • comparing the risks • voting *Note*: There are three implementation variations: • individual comparison and individual voting • group comparison and individual voting • group comparison and group consensus voting
4	**Calculate resultant ranking**. The facilitator calculates by • totalling pairwise comparison votes for each risk • sorting risks by total votes from highest to lowest
5	**Review ranking with participants**. Reviewing the results allows the participants to react to and discuss the resultant ranking.

Section 4

Comparison Risk Ranking Tools

**Sample
Comparison
Risk Ranking
Form**

Below is a sample of a comparison risk ranking form [FitzGerald 90b] used to capture pairwise comparison information.

Comparison Risk Ranking Form

Comparison question → Which risk is more important to the project?

Risk a	Risk a		
Risk b		Risk b	
Risk c			Risk c

Pairwise comparison cell

List of risks to rank
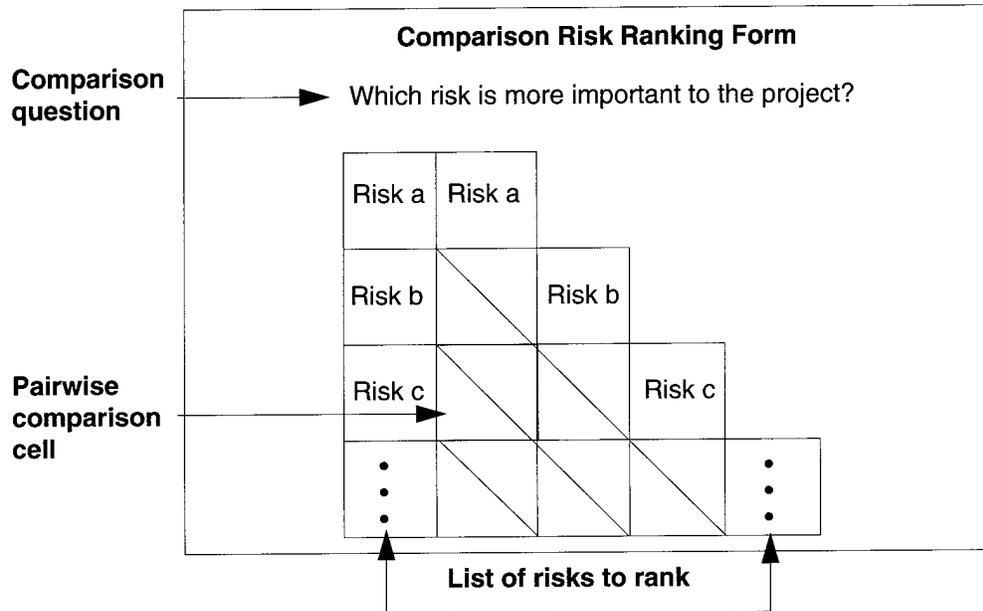
Filling in the Cells

The following table illustrates how to fill out the comparison cells in the form by an individual or with group consensus voting.

If...	Then...
Risk a is more important than Risk c	Risk a / Risk c: 1 / 0
Risk c is more important than Risk a	Risk a / Risk c: 0 / 1
Risk a and Risk c are equally important	Risk a / Risk c: 0.5 / 0.5

Note: When individual voting is used, each individual makes the comparison and the results are summed and recorded in the cell.
Individual Voting Example:

Participant 1:

Risk a

Risk c | 1 / 0

Participant 2:

Risk a

Risk c | 1 / 0

Participant 3:

Risk a

Risk c | 0.5 / 0.5

Comparison result entered into cell

Risk a

Risk c | 2.5 / 0.5
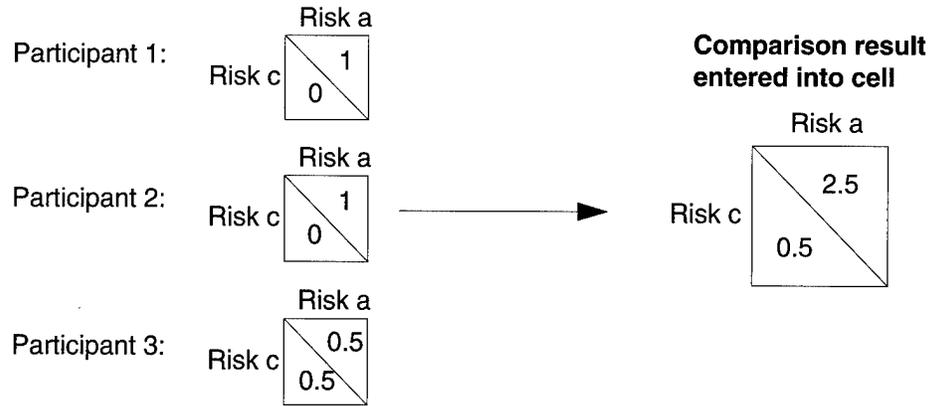
Calculating the Ranking

The comparison risk ranking form provides an easy and succinct way to capture and total the votes.

Add the upper right hand cell numbers of the column risk to the bottom left hand cell numbers of the corresponding row risk.

Group consensus voting example: Which risk is more important to the project?

Total

2	Risk a	Risk a		
3	Risk b	(0) / 1	Risk b	
0.5	Risk c	(1) / 0	1 / 0	Risk c
0.5	Risk d	(1) / 0	1 / 0	0.5 / 0.5	Risk d

◯ Total for Risk a = 0 + 1 + 1 = 2

▢ Total for Risk b = 1 + 1 + 1 = 3
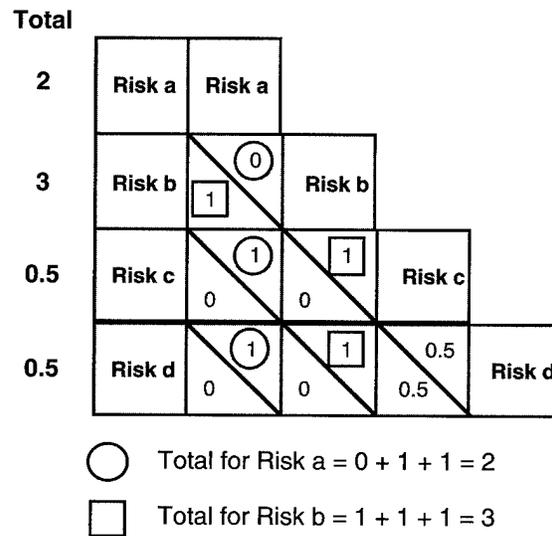
From the example we see that based on the number of votes the ranking of risks is
1. Risk b
2. Risk a
3. Risk c and Risk d (tie)

Section 5

Guidelines and Tips

Number of Risks and Timing

Keep the number of risks to be ranked under 20. More than that will markedly increase the amount of time required. For 20 risks, limit the application time to 3 hours including breaks. Most groups will be ready to quit after three hours.

For n risks the number of comparisons required is n(n-1)/2.

Example:

# Risks	Comparisons Required	Average Time
5	10	15 min
10	45	30 min
15	105	60 min

The first comparisons will generally take longer since people are adjusting to the process and discussing risks for the first time, but eventually they reach a point where they can handle 4-5 comparisons per minute.

Number of Participants

Keep the number of participants between one and six. This will provide a good range of perspectives about the risks without greatly increasing the time required for the application.

Defining Comparison Criteria

Be as specific as possible when defining the comparison criteria. Well defined criteria will make comparing risks easier for the participants. It may also speed up the process.

Automated Support

Having a computer application available which captures the individual comparisons and automatically generates the ranking is helpful. A simple spreadsheet can save time and reduce the possibility of error.

References

Cited in this chapter:

[FitzGerald 90a]   FitzGerald, Jerry. "Risk Ranking Contingency Plan Alternatives." *Information Executive 3*, 4 (Fall 1990): 61-63.

[FitzGerald 90b]   FitzGerald, Jerry & FitzGerald, Ardra F. Chapter 5, "A Methodology for Conducting a Risk Assessment," 59-72. *Designing Controls into Computerized Systems*, 2nd ed. Redwood City, Ca.: Jerry FitzGerald & Associates, 1990.

[Xerox 92]   Xerox Corporation and Carnegie Mellon University. *The University Challenge: Problem-Solving Process User Manual*. Stamford, Ct.: Xerox Corporation, 1992.

Chapter A-11

Cost-Benefit Analysis[1]

Costs

Benefits

Projections

Section

1. The method described here is a simple one from the Xerox Problem Solving manual [Xerox 92].

Section 1

# Cost-Benefit Analysis[1] Description

Introduction

Cost-benefit analysis, as described here, is a simple method for comparing estimates of total costs and benefits of a mitigation strategy as a means of analysis and decision support during risk planning. This is not a method to calculate precise costs or benefits; it is done to support a decision between two or more alternative strategies.

Note: This type of analysis is commonly used by project managers and planners. Boehm's Constructive Cost Model (COCOMO) is a classic reference [Boehm 81] for software cost estimation. Almost any reference for project management will deal with cost estimation methods.

Diagram

The following diagram shows the inputs and outputs for cost-benefit analysis.
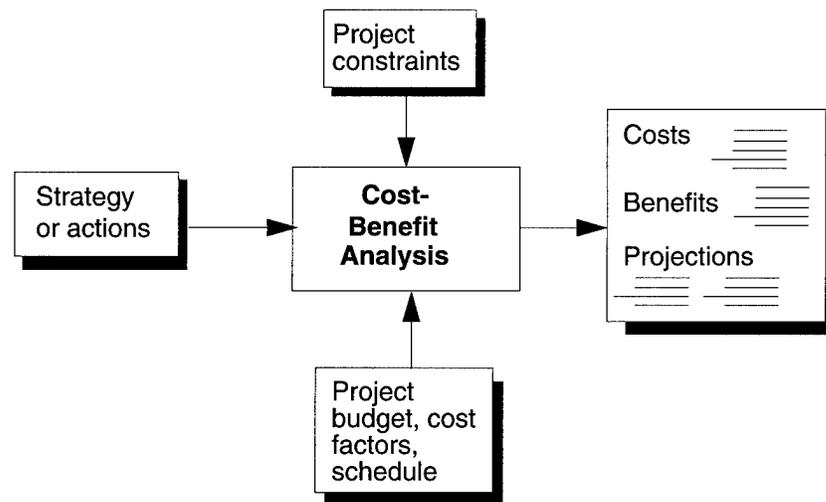
Personnel Requirements

Cost-benefit analysis can be done by an individual or a group. If performed by a group of three or more, one person should be the facilitator and recorder (but he or she could still participate or contribute). All participants (with the possible exception of a facilitator who is not contributing), should be familiar with the organization's accepted cost estimation practices.

---

1. There are multiple methods used to actually generate cost estimates (and estimates for benefits). Many of these are specific to the project or organization. Users of this cost-benefit analysis method may need to supplement it with more precise cost estimation methods to derive the degree of accuracy required for budgeting purposes.

Section 2

When to Use

When to Use Use this method when there is a need to evaluate and decide among strategies or a set of actions based upon the cost and benefits to the project.

Constraints Cost-benefit analysis relies on the existence of accepted cost estimating practices (e.g., COCOMO [Boehm 81], corporate overhead costs per employee hour, standard equipment costs, etc.). If the participants are not familiar with the way the organization does costing, the estimates derived may not have the desired degree of validity. In that case, identifying the types of costs and benefits (e.g., personnel, workstations, software tools, etc.) may be of some use until costing expertise is available.

Benefits This method
- provides decision makers with a quantitative perspective of the alternatives
- helps decision makers understand the scope of the alternatives
- may not require a lot of time (depending on the degree of accuracy desired)

Section 3

Performing Cost-Benefit Analysis

Procedure

The table below describes the process for conducting a cost-benefit analysis session with a group. Individual application generally follows the same basic steps but all steps are performed by the same person.

Step	Action
1	**Explain strategy or set of actions**. The facilitator presents a strategy or set of actions for which costs and benefits are to be generated, and ensures they are understood by all participants.
2	**Explain process**. The facilitator explains the cost-benefit analysis process.
3	**Estimate cost factors**. Participants identify and estimate the cost factors (all aspects of the strategy that will result in costs). Estimates can be on a summary or periodic (e.g., cost per month, year, etc.) basis. Changing costs should be charted across the relevant time span. Identify any intangible cost that cannot be estimated, but will have an impact on the decision.
4	**Estimate benefit factors**. Participants identify and estimate the benefit factors. Assumptions on the benefits of the strategy may need to be made; if so, document them. Estimates can be on a summary or periodic (e.g., benefits per month, year, etc.) basis. Changing benefits should be charted across the relevant time span. Identify any intangible benefit that cannot be estimated but will have an impact on the decision.
5	**Review the cost and benefit estimates**. Participants review the cost and benefit estimates for completeness and accuracy. Revise any estimates as needed. Use the data to support comparison between strategies or to support decisions.

Types of Costs

Costs should include everything that is needed to fully implement the strategy. They should also include the costs or impacts to the project from the strategy. Costs can include

- personnel time
- personnel salaries and benefits
- capital equipment costs
- office supplies/equipment
- support tools: software and documentation
- training costs
- delays in system delivery/completion
- changes in project plan—milestones and schedule, contents of milestones, process changes (management or development), resource allocation, personnel changes
- penalties or loss of contract awards
- delivered system changes—requirements, design, interfaces

Types of Benefits

Benefits from a strategy are primarily the reduction in risk to the project or to the organization. There are also intangible benefits to consider. For example, the cost to train personnel on project A to reduce a risk may be also recouped in later projects as more skilled personnel are now available. Benefits from a strategy can include

- reduced probability or impact from the risk
- reduced long-term development costs
- increased personnel efficiency
- improved morale
- reduced schedules
- keeping the contract (not losing it)
- satisfied customer—which can lead to other contracts
- more informed customer or supplier (and more cooperative)
- improved support systems
- more effective management and development processes
- improved allocation of resources
- more realistic requirements
- improved system operations

Section 4

Cost-Benefit Analysis Tools

Analysis Results

The results of a cost-benefit analysis can have many forms, the most likely being some form of spreadsheet. Spreadsheets provide a suitable framework for combining the results of the analyses of many strategies into a comparison table that can be used to support decision making.

Strategy Example

This is a simplistic example of a strategy's cost and benefits being analyzed.

Strategy
Replace old workstations at the rate of 3 per month.
Provide training to 33 employees (11 per month).
The 25% expected improvement in performance will allow us to meet requirements for performance and deliver required system.

Costs and Benefits Example

This is an example of the type of results you might expect to see from a cost-benefit analysis for the strategy example above. The following tables show the basic costs and benefits for this strategy.

Type of Cost	Cost	Totals
9 Workstations	$4000 per machine	$12,000/month for 3 months
Training	$4000/month	$4000/month for 3 months
Time lost due to training	$200/employee—11 employees trained per month	$2200/month for 3 months

Type of Benefit	Benefit	Totals
Typical increase in performance by 25%	$200 per trained employee per month saved	$6600/month after all employees trained

Twelve-Month Projection Example

The table below provides a twelve month projection of the costs and benefits for the strategy.

12 -Month Projection		
Month	**Cost**	**Benefit**
1	$18200	0
2	$18200	$2200
3	$18200	$4400
4		$6600
5		$6600
6		$6600
7		$6600
8		$6600
9		$6600
10		$6600
11		$6600
12		$6600
Total	**$54, 600**	**$66,000**

In this case, the costs appear to approach the benefit, which may cause the decision maker to look for less expensive alternatives. If one were to consider the cost of losing the contract or the benefit to the company on follow-on projects, the margin of benefit over cost increases. If there is a high or suspected high degree of uncertainty in the estimation methods used to derive costs and benefits, a wide margin of benefit over cost might be required in order make a decision.

Section 5

Guidelines and Tips

Think Broadly

Costs and benefits come in many forms; consider *all* possibilities.

Many little costs (or benefits) can swiftly add up.

Remember there may be more benefit to the organization than to the project.

Strategy and Action Descriptions

The description of the strategy or actions must be detailed enough to enable known cost estimating techniques (those used by the organization) to be used with an acceptable degree of accuracy.

Example: The strategy "improve employee morale" by itself is too vague. With a measurable goal, such as "reduce employee turnover by 50%," a more detailed set of actions and estimations can be made, such as
- Give everyone a 2% raise.
- Eliminate weekend work.

Consider Intangible Benefits

Benefits can often be intangible, but nonetheless, they may have considerable effect on the bottom line.

Example: Improvements in employee morale can be hard to measure, but the negative impact of unhappy employees can be severe.

Ranges and Probabilities

A range of numbers as opposed to a single number can also be very useful for looking at costs and benefits; in this case, determine, if possible, the probability curve for the range.

Example: A range of $2000 - $10,000 can have multiple interpretations. The $2000 extreme may be more likely than the $10,000, or vice versa.

References

Cited in this chapter:

[Boehm 81]

Boehm, Barry. *Software Engineering Economics*. Englewood Cliffs, N.J.: Prentice-Hall, Inc. 1981.

[Xerox 92]

Xerox Corporation and Carnegie Mellon University. *The University Challenge: Problem-Solving Process User Manual*. Stamford, Ct.: Xerox Corporation, 1992.

For more information on cost-benefit analysis, see the following:

[Arrow 88]

Arrow, Kenneth J. "Behavior Under Uncertainty and its Implications for Policy," 497-507. *Decision Making: Descriptive, Normative, and Prescriptive Interactions*. Cambridge: Cambridge University Press, 1988.

Chapter A-12

Gantt Charts

Description

Gantt charts are common management tools for diagramming schedules, events, activity durations, and responsibilities and can be used for complex risk mitigation strategies and their actions.

How to Use

Gantt charts can be used to document and track the actions generated as part of mitigation planning. The Gantt chart should include [Xerox 92]
- what will be done
- who is responsible
- when tasks will start and end
- assumptions (include contingency plans if assumptions are not met and any other contingency actions or triggers associated with the mitigation effort).

If the mitigation is complex enough to require a Gantt chart, integration with project plans should be considered. Schedule slips and changes resulting from the control phase can be documented on the Gantt chart.

Example Background

This example looks at a sample risk statement and shows the mitigation goals for the mitigating actions as well as the key issues revolving around the risk.

Risk Statement
• The translation effort looks like it will slip; if it does, the whole test schedule will be in jeopardy.
Mitigation Goals
• Modify the schedule with possible completion date further out.
• Do not increase cost.
• Identify a drop-dead date and include a buffer.
• Get to IV & V with "quality" product (i.e., will satisfy requirements).
Key Issues
• software and firmware maturity
• test lab time
• system performance requirements
• repair priority
• spares

**Example
Gantt Chart**

This Gantt chart shows the mitigating actions that were developed to deal with the key issues and mitigate the risk while achieving the mitigation goals.

Task	Assigned To:	Week Ending							
		1/6	1/13	1/20	1/27	2/3	2/10	2/17	2/24
Produce aggressive test strategy for firmware-software (evaluate interface and performance).	Technical manager	▭							
Develop test case and scenarios for areas of concern.	Technical manager			▭					
Develop summary stress test.	Technical manager						▭		
Clarify lab tasking and control.	Customer lab manager						▭		
Establish priority for spares.	Project managers (customer and supplier), customer lab manager	▭							
Develop realistic serial-parallel schedule.	Technical manager, customer lab manager								▭

Assumptions:

• produces favorable outcome within costs
• does not affect critical design review schedule
• includes complete final component testing to support Independent Validation and Verification and integrated system testing

Contingency Actions and Triggers:

• If costs are projected to exceed desired limit, project managers will revisit mitigation goals.

• If the critical design review schedule is expected to be affected, project managers will meet to discuss alternative options.

• If final component testing cannot be included, project managers will revisit mitigation goals; replanning may be necessary.

References

Cited in this chapter.

[Xerox 92]   Xerox Corporation and Carnegie Mellon University. *The University Challenge: Problem-Solving Process User Manual.* Stamford, Ct.: Xerox Corporation, 1992.

Gantt charts are explained in most project management books and training classes. For more information on Gantt charts, see the following:

[Bennatan 92]   Bennatan, E. M. *On Time, Within Budget - Software Project Management Practices and Techniques.* McGraw-Hill International (UK) Limited, 1992.

[Mayrhauser 90]   Mayrhauser, Anneliese von. *Software Engineering: Methods and Management.* San Diego Ca.: Academic Press, Inc. 1990.

[Meredith 89]   Meredith, Jack R. & Mantel, Samuel J. Jr. *Project Management: A Managerial Approach*, 2nd ed. New York: John Wiley and Sons, 1989.

[Pfleeger 91]   Pfleeger, Shari Lawrence. *Software Engineering: The Production of Quality Software*, 2nd ed. New York: MacMillan Publishing Co., 1991.

[Pressman 92]   Pressman, Roger S. *Software Engineering: A Practitioner's Approach*, 3rd ed. New York: MacGraw-Hill, Inc., 1992.

[Shere 88]   Shere, Kenneth D. *Software Engineering and Management.* Englewood Cliffs, N.J.: Prentice-Hall, 1988.

[Thayer 88]   Thayer, Richard H. *Software Engineering Project Management Tutorial.* Washington D.C.: Computer Society Press of the Institute of Electrical and Electronics Engineers, Inc., 1988.

[Umbaugh 89]   Umbaugh, Robert E. & Gitomer, Jerry. "Project Scheduling and Control," 37-48. *Handbook of Systems Management: Development and Support.* Boston, Ma.: Auerbach Publishers, 1989.

Chapter A-13

Goal-Question-Measure[1]

Goal 1   Goal 2

Question 1   Question 2   Question 3   Question 4

Measure 1   Measure 2   Measure 3   Measure 4   Measure 5

Section

1. The term "measure," as used here, is synonymous with "metric." The original method as developed by Basili and Weiss [Basili 84] is called "Goal-Question-Metric."
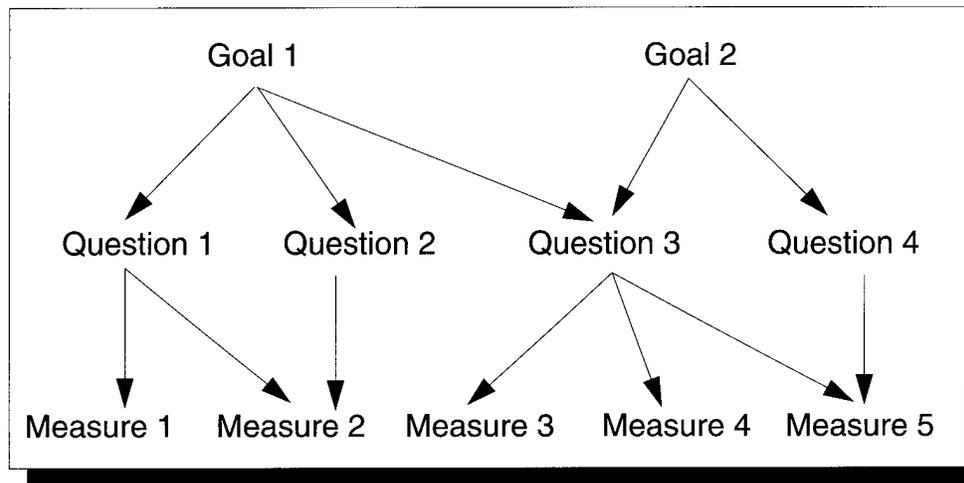
Section 1

Goal-Question-Measure Description

Introduction

Goal-question-measure (G-Q-M) is a variation of the method proposed by Basili and Weiss for collecting valid software engineering data [Basili 84]. It is adapted to help risk mitigation planners determine what indicators to use to track the progress of a mitigation strategy and the changes in the status of a risk. During the **Plan** function [Chapter 6] of the risk management paradigm, project personnel decide what goals are needed to measure the risk or mitigation plan status as well as what needs to be done with the data once it is gathered. They then build a list of questions that will help them to choose the appropriate risk indicators.

Note: The method described in this chapter is a subset of the goal-question-metric method proposed by Basili and Weiss. Goal-question-measure employs the parts of goal-question-metric that apply directly to risk management.

Diagram

The following diagram shows the inputs and outputs of the goal-question-measure method.
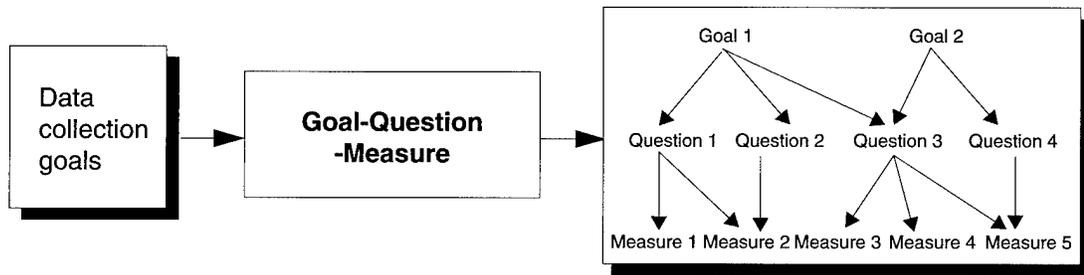
Personnel Requirements

Goal-question-measure can be done by an individual or a group. If performed by a group of three or more, one person should be the facilitator and recorder (but he or she could still participate or contribute). All participants should be familiar with the method.

Section 2

When to Use

When to Use

Use this method during risk planning to build a set of questions to identify indicators that will be used to track and control the risk or mitigation plan status.

Constraints

This method
- requires a clear understanding of the risk mitigation goal
- requires personnel with the appropriate experience and knowledge to identify goals that are neither too broad nor too narrow
- requires personnel with the appropriate experience and knowledge to construct and ask the correct set of questions needed to identify indicators

Benefits

This method
- is flexible and can be adapted to any type of organization and measurement objective
- provides a process to define measurement data that can be used to monitor the risk or mitigation plan status

Section 3

Applying Goal-Question-Measure

Procedure

The table below describes the procedure for goal-question-measure. The steps may be iterative.

Step	Action
1	**Establish data collection goals.** The data collection goal defines the desired outcome of the data collection effort. In many cases, the data collection goal is the same as the mitigation goal. If the mitigation goal is too broad, it can be broken into more specific sub-goals.
2	**Develop questions.** For each data collection goal, a list of questions of interest is developed. The questions define data parameters and categorizations that permit analysis of the data. They are used to determine the quantities that need to be measured and the aspects of the goals that can be measured.
3	**Establish indicators.** For each question, the measures that relate to the questions are identified. After examining the list of measures, project personnel choose the indicators for which data will be collected. Indicators can be one of the measures identified or can be a combination of two or more of the measures.

G-Q-M and Risk Planning

Indicators that are used to track risks and mitigation plans are identified during the **Plan** function of the risk management paradigm. The goal-question-measure method is one way to identify a number of measures related to the mitigation goal. From these measures, indicators that will be used to track risks and mitigation plans are identified.

Indicator Guidelines

The table below describes some guidelines to use when choosing indicators for tracking risks and mitigation strategies.

Guideline	Explanation
Anticipatory	Indicators should be effective predictors of future events and possibilities.
Concise and relevant	Indicators should concisely describe the important elements of the risk and associated mitigation strategies.
Economical	Indicators should be defined to minimize the resources (person-hours, computing capacity, etc.) required for collection and reporting.

Section 4

Goal-Question-Measure Example

Description

The goal-question-measure example in this section is derived from part of an example documented in *A Quantitative Approach to Software Management* [Pulford 96].

Mitigation Goal

On a given project, the mitigation goal for a particular set of risks is to reduce the number of defects introduced during the software process. Project personnel decide to use the goal-question-measure method to identify indicators for monitoring the set of risks.

Questions Related to the Mitigation Goal

Project personnel identified the following areas of software development which are related to the mitigation goal of reducing defects: products and processes. For each area, they identified specific components of interest, which are listed in the second column of the table below. From the components, project members then derived a set of questions that were used to determine the appropriate measures for the mitigation goal. The questions are listed in the third column in the table below.

Area	Component	Question
Products	Requirements specification	Q1: What is the quality of the requirements specification?
	Design specification	Q2: What is the quality of the design specification?
	Code	Q3: What is the quality of the code?
	Test plan	Q4: What is the quality of the unit test plan?
Processes	Requirements analysis	Q5: How effective is requirements analysis at detecting errors?
	Design and code	Q6: How effective is the design and code process at detecting errors?
	Unit test	Q7: How effective is the unit test at detecting errors?

Measures Derived from the Questions

Project members determined that the set of questions could be directly used to generate measures. The following table shows the set of measures derived from the questions.

Question	Indicators Derived from the Questions
Q1	M1: Customer queries that can be traced to a problem in the requirements specification
Q2	M2: Customer queries that can be traced to a problem in the design specification
Q3	M3: Customer queries that can be traced to a problem in the code
Q4	M4: Customer queries that can be traced to a problem in the test plan

Question	Indicators Derived from the Questions
Q5	M5: The number of errors detected during requirements analysis
Q6	M6: The number of errors detected during the design and code review process
Q7	M7: The number of errors detected during unit testing

Indicators for the Mitigation Goal

In general, once measures are established, project personnel must choose indicators that will be used to provide insight into the mitigation goal. The indicators can be one of the measures or can be a combination of two or more of the measures. In this example, measures M5, M6, and M7 were chosen as status indicators for the mitigation goal. They can be used during development to monitor the software development process. Measures M1, M2, M3, and M4 would be collected after the product is shipped. The risk will either have been successfully mitigated or will have become a problem by the time these data can be collected. They can be useful for refining the software process on future projects within the organization but are not useful as risk indicators in this example.

Section 5

Guidelines and Tips

Defining Goals

Be clear about the goals for the data collection. Unclear goals will not provide the answers being sought.

Goals are not well defined if questions of interest are not or cannot be defined.

References

Cited in this chapter:

[Basili 84]

Basili, Victor R. & Weiss, David M. "A Methodology for Collecting Valid Software Engineering Data." *IEEE Transactions on Software Engineering SE-10*, 6 (November 1984): 728-738.

[Pulford 96]

Pulford, Kevin; Kuntzmann-Combelles, Annie; & Shirlaw, Stephen. *A Quantitative Approach to Software Management: The ami Handbook*. Wokingham, England: Addison-Wesley Publishing Company, 1996.

For more information on goal-question-measure, see the following:

[Grady 92]

Grady, Robert B. *Practical Software Metrics for Project Management and Process Improvement*. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1992.

Chapter A-14

Interrelationship Digraph
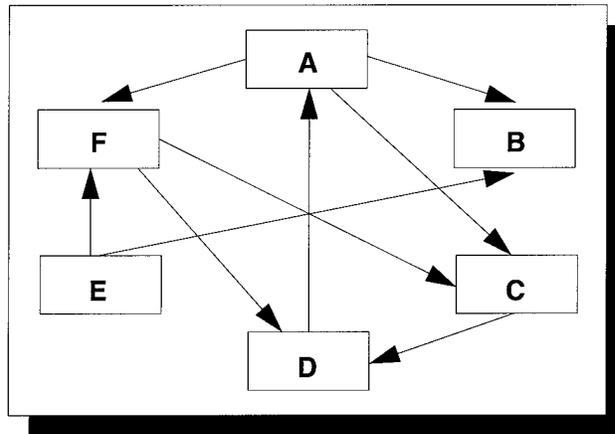
Section

Section 1

Interrelationship Digraph Description

Introduction

The interrelationship digraph method is used to identify the cause and effect relationships among a set of items [Brassard 94]. For Continuous Risk Management this method is commonly used during risk planning. During planning these items could be

- risk/mitigation areas: the risks or set of risks being mitigated
- strategies: strategies selected for a set of mitigation areas
- activities: activities outlined in an mitigation plan for a particular mitigation area

Diagram

The following diagram shows the input and output of the interrelationship digraph method.
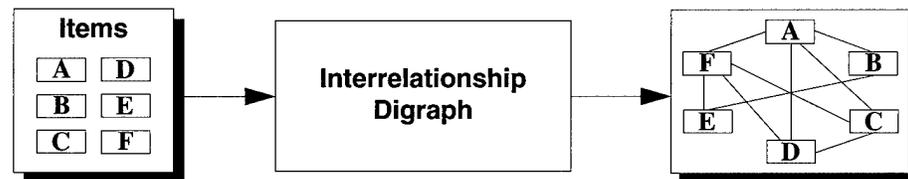
Personnel Requirements

The interrelationship digraph method can be done by an individual or a group. If performed by a group of three or more, one person should be the facilitator and recorder (but he or she could still participate or contribute).

Section 2

When to Use

When to Use

Use this method

- to identify the cause and effect relationship, root causes, etc., among a set of items
- to increase the understanding of a set of risks: to find cycles of dependencies or root causes and to identify critical risks in a set (which ones must be mitigated)
- to determine the interrelationships and dependencies among a set of actions or strategies in support of the **Problem-Solving Planning** method [Chapter A-24]
- to determine which risk areas to deal with first during a **Baseline Planning** session [Chapter A-5]

Constraints

The result will only be as good as the knowledge the participants bring. It is important to select the "right" participants. Participants need to be familiar with the items. They should have "intimate knowledge of the subject under discussion" [Brassard 94, p. 77].

Benefits

This method encourages participants to "think in multiple directions rather than linearly" [Brassard 94, p. 76]—that is, it allows participants to think beyond the obvious when trying to identify interrelationships.

Discussions about relationships between items uncover the participants' assumptions and identify sources of disagreements [Brassard 94].

Section 3

Constructing an Interrelationship Digraph

Procedure

The following table describes how to construct an interrelationship digraph. This procedure is a based on steps described in the interrelationship digraph chapters of *The Memory Jogger Plus +*™ [Brassard 89] and *The Memory Jogger* ™ *II* [Brassard 94].

Step	Action
1	**Review the items.** Review the items on the list for understanding.
2	**Define the issue/problem statement.** Define a statement which summarizes the problem or issue surrounding the items. *Example:* Strategies independently selected for mitigating a set of risks.
3	**Record items on cards.** Record each item on a separate card. Print legibly and large enough so that the cards can be read from a distance of four to five feet away.
4	**Display the cards.** Arrange the cards so that there is ample room to draw arrows between cards.
5	**Draw relationship arrows between cards.** Look at each pair of items and determine, by consensus, if there is an interrelationship. Does Item X cause or influence Item Y? If yes, draw an arrow Item X to Item Y. *Note:* A variation of this step is to apply a weighting factor to the arrow based on the strength of the interrelationship.
6	**Review and revise, as necessary.** After comparing all items, review the relationships and make any necessary changes.
7	**Tally arrow information.** Count and record the number of incoming and outgoing arrows for each item. If a weighting factor was used, calculate the total weight for each item.
8	**Select key items.** Use the tallied arrow information, experience, and judgment to reach consensus on the key items to be worked on.

Dual Arrow Directions

When looking at a pair of items, it's possible that each has a causal or influential effect on the other. In those cases, avoid using two-headed arrows. Pick the stronger of the relationship [Brassard 89].

Weighting Strength of Relationship

To distinguish the relative strength of a relationship, a weighting factor may be applied to the arrow. Relationship strength can be
• significant = 9
• medium = 3
• weak = 1 [Brassard 94, p. 81]

Total Weight for an Item

If a weighting factor is used, a total weight can be tallied for an item by summing the individual relationship weights associated with each incoming and outgoing arrow. This can point to items that have the "strongest effect on the greatest number of issues" [Brassard 94, p. 81].

Total Weight Example

The example below illustrates how weights would be applied to the interrelationship digraph.

Key:

Significant = 9
Medium = 3
Weak = 1
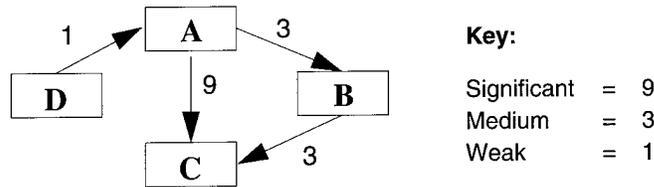
Items	Number of Outgoing Arrows	Number of Incoming Arrows	Total Weight
A	2	1	13
B	1	1	6
C	0	2	12
D	1	0	1

Large Number of Outgoing Arrows

A large number of outgoing arrows indicates that this item has a causal or influential effect on a number of other items. This could suggest that this is a root cause or an item that must be dealt with first. This item can be thought as a "Cause/Driver" [Brassard 94, p. 79].

Large Number of Incoming Arrows

A large number of incoming arrows indicates that this item is affected or influenced by a number of other items. This item can be thought of as a "Result/Rider" [Brassard 94, p. 80].

Section 4

Interrelationship Digraph Tools

Matrix Format

Below is a sample of a matrix format [Brassard 94, p. 81] for capturing the interrelationships among a set of six items.

	A	B	C	D	E	F	No. of Causes/ Drivers ⇑	No. of Results/ Riders ⇐	Total Weight
A	•								
B		•							
C			•						
D				•					
E					•				
F						•			

Filling in the Matrix

The following table illustrates how to fill out the matrix cells in the form by an individual or by group consensus.

If...	Then...
Item A has a causal or influential effect on Item B	Item B Item A ⇑
Item B has a causal or influential effect on Item A	Item B Item A ⇐
There is no causal or influential relationship between Item A and Item B	Item B Item A −

Note: If a a weighting factor was used, it would be added to the cell. For example, if Item A was noted as having a significant effect (value=9) on Item B the matrix cell would indicate the following:

Item B
Item A 9 ⇑

Matrix Example

A project baselined its risks and classified the risks into six areas for mitigation. Project management is trying to determine the dependencies among the areas and, given scarce resources, which areas should be mitigated first.

Key:
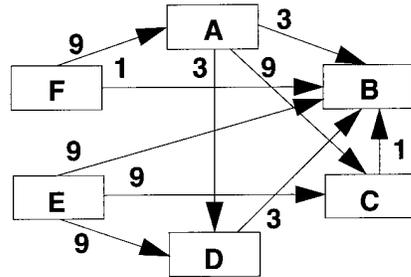
Significant = 9
Medium   = 3
Weak   = 1

Item	Risk Area
A	Requirements
B	Testing
C	Systems engineering
D	Configuration management
E	Staffing

	A	B	C	D	E	F	Cause/ Driver ⇑	Result/ Rider ⇐	Total Weight
A	•	3 ⇑	9 ⇑	3 ⇑	-	9 ⇐	3	1	24
B	3 ⇐	•	1 ⇐	3 ⇐	9 ⇐	1 ⇐	0	5	17
C	9 ⇐	1 ⇑	•	-	9 ⇐	-	1	2	19
D	3 ⇐	3 ⇑	-	•	9 ⇐	-	1	2	15
E	-	9 ⇑	9 ⇑	9 ⇑	•	-	3	0	27
F	9 ⇑	1 ⇑	-	-	-	•	2	0	10

351

**Matrix
Analysis**

From the matrix we see that both requirements and staffing have the most number of out-going arrows, indicating that they affect a number of other risk areas, and are thus considered key items. Testing has the most number of incoming arrows and no outgoing arrows indicating that it is influenced by other risk areas but does not itself affect other risk areas. Staffing has been weighted the most, with requirements as a close second. Based on this information and the project's experience, mitigation plans will first be implemented for the requirements and staffing risk areas.

Section 5

Guidelines and Tips

General

The following tips and guidelines were adapted from *The Memory Jogger Plus* +™ [Brassard 89]:

- Record items on a medium that is easy to move—3M's Post-it™ note paper or 3x5 note cards work well.
- Lay out the cards allowing ample room to draw lines between cards.
- Use 10-20 items for maximum effectiveness; use a minimum of 5 items.
- Walk through the cards in a structured manner to ensure that all comparisons are made.
- Limit the number of participants to 6.

Supporting Information

When used as part of risk planning, it is important to keep the big picture and the context of what is intended. For example, when dealing with risk areas, it is important to understand the risks underneath each area and their context before making relationship determinations. Also knowing that there are only resources to mitigate one area versus all risk areas may influence which area is chosen.

Card vs. Matrix Approach

Use both approaches in parallel. Have someone record the information on the matrix as the relationships are drawn among the cards.

- When working with a group, it seems best to begin by putting the items on 3x5 cards and displaying them on a wall surface. This visual representation helps you think about relationships between items. (*Note*: weights can be shown with different colors or thickness of the lines.)
- When looking for key items, the matrix approach seems best for organizing the data and showing how the information compares between items.

Selecting Key Items

The arrow and weight information provides a good summary of the relationships among the items but it should only be used as input into selecting the key items. Use the team's knowledge of the items and experience to make the selection, even if the numbers don't reflect the decision. Don't let the numbers dictate the decision. Use the team's best judgment [Brassard 89].

References

Cited in this chapter:

[Brassard 94]   Brassard, Michael & Ritter, Diane. *The Memory Jogger ™ II:A Pocket Guide of Tools for Continuous Improvement & Effective Planning*. Methuen, Ma.: GOAL/QPC, 1994.

[Brassard 89]   Brassard, Michael. *The Memory Jogger +™ : featuring the seven management and planning tools*. Methuen, Ma.: GOAL/QPC, 1989.

For more information on interrelationship digraphs, see the following:

[Moran 90]   Moran, John W.; Talbot, Richard P.; & Benson, Russell M. *A Guide to Graphical Problem-Solving Processes*. Milwaukee, Wi.: ASQC Quality Press, 1990.

Chapter A-15

List Reduction[1]

Smaller list of items

1. Xerox Corporation and Carnegie Mellon University, *The University Challenge: Problem-Solving Process User Manual*, Xerox Corporation, Stamford, Connecticut, 1992.

Section 1

List Reduction Description

Introduction

List reduction is a method for dealing with a large number of risks, strategies, or other ideas, and is especially useful for dealing with the results of a **Brainstorming** [Chapter A-7] session. The intent is to clarify the options to enable understanding by all members of the group and reduce the list to a manageable number.

Diagram

This diagram illustrates the input and output of a list reduction activity.

```
┌──────────┐          ┌──────────────────┐          ┌──────────┐
│ Large    │          │                  │          │ Smaller  │
│ list of  │ ───────▶ │  List reduction  │ ───────▶ │ list of  │
│ items    │          │                  │          │ items    │
└──────────┘          └──────────────────┘          └──────────┘
```
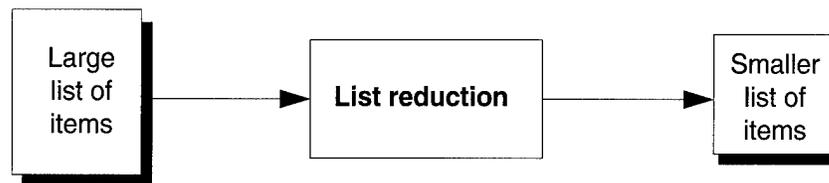
Personnel Requirements

List reduction can be done by an individual or a group. If performed by a group of three or more, one person should be the facilitator and recorder (but he or she could still participate or contribute).

Section 2

When to Use

When to Use   Use list reduction when dealing with a large number of items, such as risks or strategies, for a simple way to reduce the list to a manageable few.

Constraints   Efficiency of the method is dependent on the participants' understanding of the items on the list to be reduced and the filters used to reduce the list. Without a shared understanding, the process may take longer than expected or have to be redone.

Benefits   This method
- is simple, easy to use
- can be repeated until the list of items is reduced to a manageable size

Section 3

Conducting a List Reduction Session

Procedure

The table below documents the procedure for conducting a list reduction session. This procedure is written for use by a group of people with a facilitator, but it can be done by an individual.

Step	Action
1	**Clarify all items**. Facilitator reviews each item and ensures that all group members understand them.
2	**Define filters**. Participants identify criteria to be used to filter the list. For example, filters for mitigation strategies can include the following questions: • Will it mitigate the risk? • Is it feasible? • Can we afford it?
3	**Vote on items**. Keeping the filters in mind, each participant votes "yes" or "no" on each item.
4	**Tally results**. A simple majority (one-half plus one) keeps the item on the list. Fewer votes causes an item to be "bracketed"— that is, identified as as an item that might be removed from the list.
5	**Repeat steps 1-4, as necessary**. Repeat the process until the list contains about six items. A bracketed item can be added back to the list for consideration if requested by a member of the group. *Note*: Increasingly stringent filters are applied at each repetition of the process.

Section 4

4

Guidelines and Tips

Filters

Filters should be chosen carefully to avoid using an irrelevant filter that may eliminate a useful idea.

Take the time to ensure that all participants have a shared understanding of the filter to be used. A shared understanding will focus the effort and help you get to the desired result.

Reference

For more information on list reduction, see the following:

[Xerox 92]

Xerox Corporation and Carnegie Mellon University. *The University Challenge: Problem-Solving Process User Manual*. Stamford, Ct.: Xerox Corporation, 1992.

Chapter A-16

Mitigation Status Report
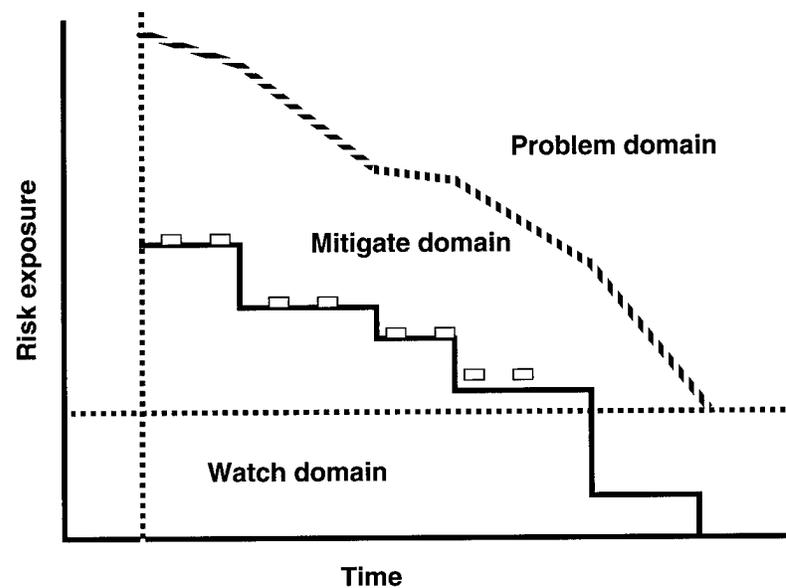
Section

Section 1

Mitigation Status Report[1] Description

Introduction

A mitigation status report is a technique for tracking risks and mitigation plans on a periodic basis [Clark 95]. It uses graphics to display risk exposure on a **Time Graph** [Chapter A-36] and also contains written information on the status and the causes of the risk or risk set. The format of the report and the information included in the report should be tailored to the needs of each organization. Ideally, this technique should

- visually display risk indicators to allow project personnel to make control decisions
- express the project's confidence in achieving the next milestone
- highlight contingency plans and their associated triggers

Diagram

The diagram below shows the inputs and outputs for generating mitigation status reports.
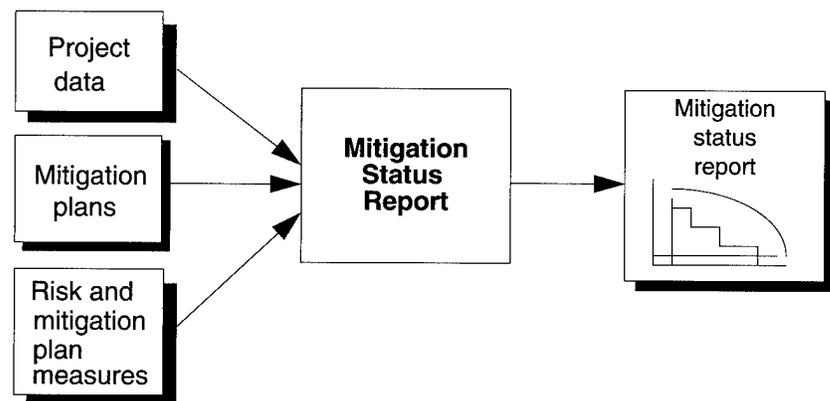
Personnel Requirements

Mitigation status reports are prepared by the person(s) responsible for tracking the risk or by a support staff member who compiles the information for the task leaders. The data required in the reports are defined by project personnel during the **Plan** function [Chapter 6]; the reports are prepared during the **Track** function [Chapter 7]; and control decisions are made during risk **Control** [Chapter 8].

---

1. Although this method is presently evolving and is undergoing validation in the field, it has sufficient merit to include here.

Section 2

When to Use

When to Use

Use this method
- when tracking detailed mitigation plans and schedules (usually those that require a task plan as opposed to a series of action items) for a risk or a set of risks
- when it is necessary to provide a concise but thorough summary of the mitigation plans associated with top N risks
- when it is necessary to use a forecasting tool to determine deviations from the mitigation plan

Constraints

It takes time and effort to properly structure mitigation status reports. However, the periodic updating of the information on the reports requires modest effort. In general, it is best to be selective in choosing those risks that will be tracked using mitigation status reports. This method is best used for top N risks with detailed mitigation plans.

If the impact and probability are evaluated qualitatively using ordinal numbers, the resulting risk exposure numbers must be used carefully. In this case, risk exposure should be used a guide to aid in decision making and to determine when plans are off track. Do not treat the risk exposure in this case as a cardinal number and attach more meaning to the value than it supports (see **Analyze** [Chapter 5]). In the end, project personnel must trust their experience and instinct when making decisions.

Benefits

Mitigation status reports
- provide concise and visual summaries of project risks
- can be used to summarize risk data and the status of mitigation efforts for management
- can be used to express the project's confidence in achieving the next milestone

Section 3

Constructing a Mitigation Status Report

Mitigation Status Report Form

The form below is an example of one type of mitigation status report format. This blank form will serve as the starting point for the discussion on how to construct a mitigation status report.

Risk information

Risk status

Root causes and mitigation actions

Mitigation function

Domain boundaries

Mitigation Status Report

<Classification information>

Risk ID

<Risk statement>

Date

Approach: ☐ Watch ☐ Accept ☐ Mitigate

Risk status

Impact (I)	___
Probability (P)	___
Current risk exposure (RE)	___
Initial risk exposure (RE)	___

☐ Green ☐ Yellow ☐ Red

Root causes

Description	Mitigation Summary	Actions

☐ Reported risk exposure

Risk Exposure: 50, 40, 30, 20, 10

Action

Overall Procedure

The following procedure table summarizes the major steps in constructing mitigation status reports. Further detail on each of the steps can be found in subsequent sections.

Step	Action
1	**Add risk information.** Basic information about the risk or set of risks (e.g., the risk statement, the risk identifier, the current approach, etc.) is added to the report.
2	**Add risk status.** The current values of risk exposure, impact, and probability along with the current stoplight status are added to the mitigation status report.
3	**Add the root causes and mitigation plan.** Textual information about the root causes of the risk, the mitigation summary, and the mitigation actions are added to the report.
4	**Add the mitigation function.** A representation of the mitigation plan is added to the time graph portion of the mitigation status report.
5	**Add the boundary domains.** The watch/mitigation boundary and the problem/mitigation boundary are derived and added to the time graph.
6	**Track risk exposure.** The current value of risk exposure is added to the time graph.

Note: The mitigation function and the boundary domains can be added to the time graph after the mitigation plan is built. They are redrawn only if replanning is required or if a contingency plan is implemented.

Mitigation Status Report Example

In each subsequent section of this chapter, an example highlighting the construction and use of a mitigation status report will be developed. In this example, the following top N project risk set will be mitigated:

The project is understaffed and the requirements have changed; the software delivery might be late.

Section 4

Adding Risk Information

Description

During this activity, basic information about a risk or risk set is added to the mitigation status report. The following information is added to the report during this task:
- the classification information (e.g., technical, schedule, or cost)
- the statement of the risk or risk set
- the risk identifier(s)
- the date
- the approach taken to deal with the risk or risk set

Procedure

The following table describes the procedure for adding basic risk information to the mitigation status report.

Step	Action
1	**Add the classification information**. Information about risk classification is added to the report. Choices for risk type can include technical, schedule, and cost, as well as others defined by project personnel.
2	**Add the risk statement**. The statement for the risk or set of risks is added to the report.
3	**Add the risk identifier**. The unique risk identifier assigned to the risk is included in the appropriate area. If a set of risks is being mitigated, all of the individual risk identifiers can be included.
4	**Add the date**. The date that the report is prepared is added to the form.
5	**Add current approach**. The approach for the risk or the set of risks is added to the report. Choices for risk approach include watch, accept, and mitigate.

Risk Information Example

The following top N project risk set will be mitigated:

The project is understaffed and the requirements have changed; the software delivery might be late.

Project personnel have decided to track the set using a mitigation status report. The following table outlines the risk information which is added to the mitigation status report.

Field	Definition/Formula	Example
Classification information	Technical, schedule, or cost	Schedule
Risk statement(s)	Description of the risk; usually in the form of a condition-consequence pair	The project is understaffed and the requirements have changed; the software delivery might be late.
Risk identifier(s)	Unique numbers identifying the risk(s) for tracking purposes	R23, R27
Date	The date the report was completed	4/15/96
Risk approach	Accept, watch, or mitigate	Mitigate

Risk Information Fields

The following diagram shows the "Risk information" portion of the mitigation status report with the appropriate information added.

Section 5

Adding Risk Status

Description

The impact and probability for the risk or set of risks are periodically estimated by the responsible person or team during risk mitigation, and risk exposure is then derived from the impact and probability. The current values of risk exposure, impact, and probability along with the current stoplight status are added to the mitigation status report during this task.

Procedure

The following table describes the procedure for adding current risk status information to the mitigation status report.

| Step	Action
1	**Add impact**. Through data gathering, discussion, and consensus, project personnel determine the current impact (I) of the risk or set of risks.
2	**Add probability**. Through data gathering, discussion, and consensus, project personnel determine the current probability (P) of the risk or set of risks.
3	**Add risk exposure**. The risk exposure (RE) is calculated from the impact and probability values for the risk or set of risks. $$RE = I * P$$ *Note*: Since the impact and probability have been evaluated qualitatively using ordinal numbers, the resulting risk exposure numbers must be used carefully. It should be used only as a guide to aid in decision making and to determine when plans are off-track.
4	**Add stoplight status**. The stoplight status (see Stoplight Chart [Chapter A-31]) is determined. The following are the stoplight status definitions: • *Red* indicates that the plan is not working and management action will be required to bring the situation under control. • *Yellow* indicates that the plan is not working as intended and while no management action is required at this point, future action may be required if the situation persists. • *Green* indicates that the plan is working as intended and no management action is required.

**Risk Status
Example**

During the weekly project meeting, project personnel discuss the set's current impact and probability. Through consensus, they determine the values of the impact and probability for the risk set. At the present time, one mitigation action has been completed. The following table outlines the risk status data that is added to the mitigation status report.

Field	Definition/Formula	Example
Impact	A measure of the loss that can occur (this example assumes a scale of 1 - 5 for impact)	The impact is determined to be 4. The initial impact prior to mitigation was determined to be 4.
Probability	The likelihood that the risk will occur (this example assumes a scale of 1 -10 for probability)	The probability is determined to be 4. The initial probability prior to mitigation was determined to be 5.
Current risk exposure	The current product of impact and probability RE = I * P	RE = 4 * 4 = 16
Initial risk exposure	The product of impact and probability prior to mitigation RE = I * P	RE = 4 * 5 = 20
Stoplight status	Red, yellow, or green	Yellow

**Risk Status
Fields**

The following diagram shows the "Risk status" portion of the mitigation status report with the appropriate information added.

Risk status

Impact (I)	4
Probability (P)	4
Current risk exposure (RE)	16
Initial risk exposure (RE)	20

☐ Green   ☒ Yellow   ☐ Red
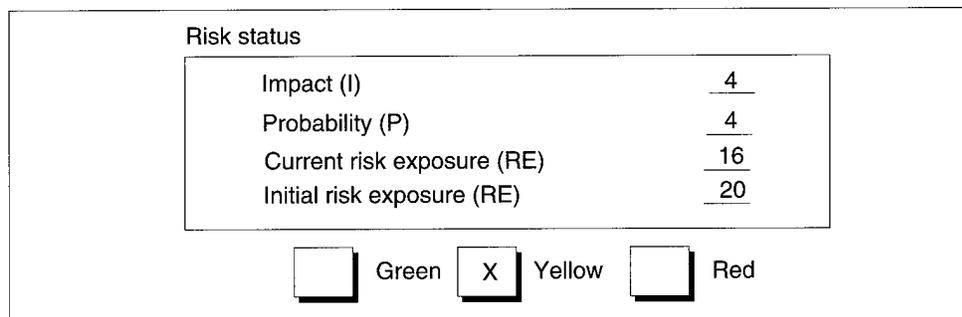
Section 6

Adding Root Causes and Mitigation Actions

Description

During this activity, the following information is added to the mitigation status report:

- textual information about the root causes (i.e., the conditions which create the risk or set of risks)
- a summary of the mitigation actions
- a mapping of the mitigation actions to the root causes

This information is generated during mitigation planning and remains stable unless there is a need to replan. In that case, the updated information is added to the report.

Procedure

The following table describes the procedure for adding the textual description of the root causes and mitigation actions to the mitigation status report.

Step	Action
1	**Add textual description of the root causes.** Any root causes or conditions of the risk or risk set are captured on the report. The root causes of a risk can be determined by using Cause and Effect Analysis [Chapter A-8]. Often, only the condition portions of the risk statements are listed here. This information is captured in the diagram on the next page under the "Description" field.
2	**Add textual summary of the mitigation actions.** A textual summary of mitigation actions is added to the mitigation status report. A summary of all milestones can be included in this area, or only the mitigation goal can be included. The decision of how much information to display is determined by the project personnel. This information is captured in the diagram on the next page under the "Mitigation Summary" field.
3	**Map mitigation actions to root causes.** A listing of the mitigation actions for each root cause is added to the form. This is especially helpful when a set of risks is being tracked. This information is captured in the diagram on the next page under the "Actions" field.

Root Cause and Mitigation Action Example

When the mitigation plan was being developed, the root causes of the risk set were determined by using cause and effect analysis. At the same time, project personnel used **Problem-Solving Planning** [Chapter A-24] to create the mitigation task plan, including milestones for the mitigation actions. In this example, there are five mitigation actions. This information has not changed since the original planning was completed and there has been no need to replan. This information is then added to the mitigation status report.

Root Cause and Mitigation Action Fields

The following diagram shows the "Root cause and mitigation action" portion of the mitigation status report with the appropriate information added.

Root causes

Description	Mitigation Summary	Actions
Inadequate development staff	Add 4 software engineers.	1, 3
The requirements have changed.	Capture requirements changes and update the development plan.	2, 4, 5

Section 7

Adding the Mitigation Function

Description

During this activity, the mitigation actions and milestones are added to the time graph. This portion of the mitigation status report will be used to track risk exposure over time. The information will remain stable unless there is a need to replan or there is a need to use a contingency plan. In either case, the time graph must be redrawn.

Procedure

The following table describes the procedure for adding the mitigation plan to the time graph portion of the mitigation status report. The mitigation plan as depicted on the time graph is actually an adapted representation of the **Gantt Chart** [Chapter A-12] for the mitigation actions in the form of a step function.

Step	Action
1	**Add the initial risk exposure**. The first step in drawing the mitigation plan is to add the initial risk exposure for the risk or risk set to the graph. This is the starting point for the reduction of risk exposure by the mitigation plan and is represented by point R_0 in the diagram on page 374. It is calculated by multiplying the initial impact estimate (I_0) by the initial probability estimate (P_0). $$R_0 = I_0 * P_0.$$
2	**Chronologically sort the mitigation plan actions**. The key actions are sorted chronologically with respect to their end dates and are plotted on the time axis of the graph according to those dates.
3	**Estimate the reduction in risk exposure**. When adding the mitigation actions to the graph, project personnel are required to estimate how much each action will reduce the risk exposure. They do this through discussion and consensus. The vertical spacing between the actions reflects the reduction in risk exposure that is anticipated upon the completion of each action. The size of each drop (R Drop) is the percentage reduction in risk exposure (% Reduction) multiplied by the initial risk exposure (R_0). $$R \text{ Drop} = \% \text{ Reduction} * R_0$$ *Note*: One convention is to require that the summation of all of the percentage reductions of the risk exposure for all actions equals 100%.

**Mitigation
Function
Example**

For the top N risk set being mitigated, the initial impact (I_0) was determined to be 4 on a scale of 1 - 5, and the initial probability (P_0) was 5 on a scale of 1 - 10. Project personnel have developed a mitigation plan with five milestones for this risk set. The following table summarizes the derivation of the data needed to construct the mitigation plan function.

Field	Definition/Formula	Example
Initial risk exposure (R_0)	The starting point for the mitigation plan function $R_0 = I_0 * P_0$	$R_0 = 4 * 5 = 20$
Drop in risk exposure (R Drop$_n$)	The drop in risk exposure after the completion of an action R Drop$_n$ = % Reduction * R_0	The drop in risk exposure for the mitigation plan function after the completion of Action 1 is calculated as follows: R Drop$_1$ = .4 * 20 = 8
Risk exposure after mitigation actions (R_n)	The risk exposure for the mitigation function is calculated by subtracting the drop in risk exposure from the previous value of risk exposure. $R_n = R_{n-1} - R$ Drop$_n$	The risk exposure after the completion of Action 1 is calculated as follows: $R_1 = 20 - 8 = 12$

**Time Graph
Table for
Mitigation
Plan**

The following table provides the values necessary to construct the mitigation plan function on the time graph for this example. Project personnel estimate that the percent reduction in risk exposure after the completion of each of the five milestones to be 40%, 20%, 10%, 20%, and 10% respectively.

Action	% Reduction	R Drop	R_n
Initial (0)	--	--	20
1	40	8	12
2	20	4	8
3	10	2	6
4	20	4	2
5	10	2	0

Plotting the Mitigation Plan

At this point, enough data exists to construct the mitigation plan function on the time graph. The mitigation plan for this example can be seen on the time graph in the following diagram.

R_n - The risk exposure of the mitigation plan
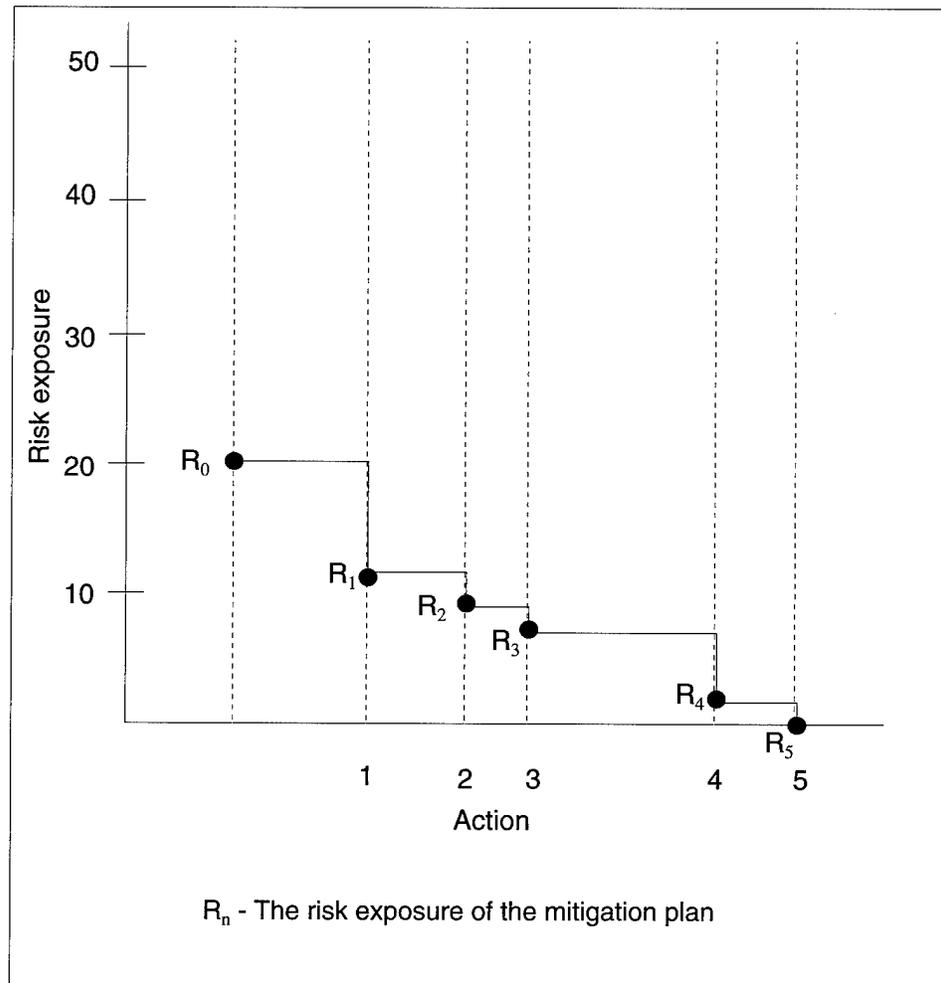
Note: The reduction in risk exposure results in the steps that can be seen in R_1 through R_5.

Section 8

Adding the Domain Boundaries

Description

The watch domain defines the region where the risk exposure is low enough that the risk can be watched; the mitigation domain defines the region where the risk exposure is such that the risk is mitigated; and the problem domain defines the region where the risk exposure is high enough that the risk has become a problem. When they are added to a time graph, these domains provide immediate visual cues regarding the success/failure of mitigation actions.

The boundary between the watch domain and the mitigation domain, called the watch/-mitigation boundary, and the boundary between the problem domain and the mitigation domain, called the problem/mitigation boundary, are derived and added to the time graph during this task. The information will remain stable unless there is a need to replan or there is a need to use a contingency plan. In either case, the time graph must be redrawn. The domain boundaries can be seen in the diagram on page 378.

Procedure: Watch/ Mitigation Boundary

The following table describes the procedure for adding the watch/mitigation boundary to the time graph portion of the mitigation status report.

Step	Action
1	**Select the watch/mitigation boundary value.** This boundary value is derived subjectively by project personnel. It is the maximum level of risk exposure below which the risk is not worth actively mitigating. This value of risk exposure is represented by point W_0 in the diagram on page 378.
2	**Draw the boundary on the time graph.** A horizontal line is drawn through watch/mitigation boundary value (W_0).

Watch/ Mitigation Boundary Example

Project personnel estimate the maximum level of risk exposure below which the risk is not worth actively mitigating. In this example, W_0 is estimated to be a value of 5. A horizontal line is drawn at a risk exposure level of 5. This is the watch/mitigation boundary and can be seen in the diagram on page 378.

Procedure: Problem/ Mitigation Boundary

The following table describes the procedure for adding the problem/mitigation boundary to the time graph portion of the mitigation status report. This curve is calculated from the mitigation plan and the watch/mitigation boundary functions. The curve is the boundary where a risk transitions from the mitigation state to the problem state.

Step	Action
1	**Determine the problem/mitigation boundary starting point.** The starting point of this curve is calculated by taking the initial impact value (I_0), multiplying it by the maximum value of the probability of the risk occurring (P_{MAX}). Point P_0 in the diagram on page 378 is the starting point of the problem/mitigation boundary. $$P_0 = I_0 * P_{MAX}$$
2	**Define the mitigation range.** The mitigation range (MR) is the total drop in risk exposure between the maximum value of risk exposure for the problem/mitigation boundary (P_0), which is calculated in the previous step, and the value of the watch/mitigation boundary (W_0). $$MR = P_0 - W_0.$$
3	**Calculate the problem/mitigation boundary.** As each action in the mitigation plan is completed, the risk exposure for the mitigation plan is reduced by an amount determined in Section 7 of this chapter. Likewise, the risk exposure for the mitigation range is reduced by the same percentage. However, the reduction is a linear function rather than a step function. The linear reductions in risk exposure from the starting value of P_0 results in the function shown in the diagram on page 378.

Problem/ Mitigation Boundary Example

For the risk set being mitigated, the initial impact, the watch/mitigation boundary, and the percentage reduction in risk exposure after the completion of an action have all been determined. The initial impact (I_0) was determined to be 4 and the watch/mitigation boundary value (W_0) was set at 5. Project personnel use this information to derive the problem mitigation boundary. The following table summarizes the derivation of the data needed to construct the problem/mitigation boundary.

Field	Definition/Formula	Example
Problem/ mitigation boundary starting point (P_0)	The starting point for the problem/mitigation boundary $$P_0 = I_0 * P_{MAX}$$	$P_0 = 4 * 10 = 40$
Mitigation range (MR)	The difference in risk exposure between the starting points of the problem/mitigation boundary and the watch/mitigation boundary $$MR = P_0 - W_0$$	$MR = 40 - 5 = 35$

Field	Definition/Formula	Example
Drop in risk exposure (P $Drop_n$)	The drop in risk exposure after the completion of an action $P Drop_n = \% \text{ Reduction} * MR$	The drop in risk exposure for the problem/mitigation boundary after the completion of Action 2 is calculated as follows: $P Drop_2 = .2 * 35 = 7$
Risk exposure after mitigation actions (P_n)	The risk exposure for the problem/mitigation boundary is calculated by subtracting the drop in risk exposure from the previous value of risk exposure. $P_n = P_{n-1} - P Drop_n$	The risk exposure for the problem/mitigation boundary after the completion of Action 2 is calculated as follows: $P_2 = 26 - 7 = 19$

Problem/ Mitigation Boundary Table

The following table shows the values necessary to construct the problem/ mitigation boundary.

Action	% Reduction	P Drop	P_n
Initial (0)	--	--	40
1	40	14	26
2	20	7	19
3	10	3.5	15.5
4	20	7	8.5
5	10	3.5	5

Plotting the Boundaries

At this point, enough data exists to construct the problem/mitigation boundary on the time graph. The problem/mitigation boundary for this example can be seen in the following diagram, along with the watch/mitigation boundary.

Note: The watch/mitigation boundary and the problem/mitigation boundary define the watch domain, the mitigation domain, and the problem domain. These three domains are shown in the figure in the following diagram.

P_n - The problem/mitigation boundary

W_0 - The watch/mitigation boundary

M_R - The mitigation range
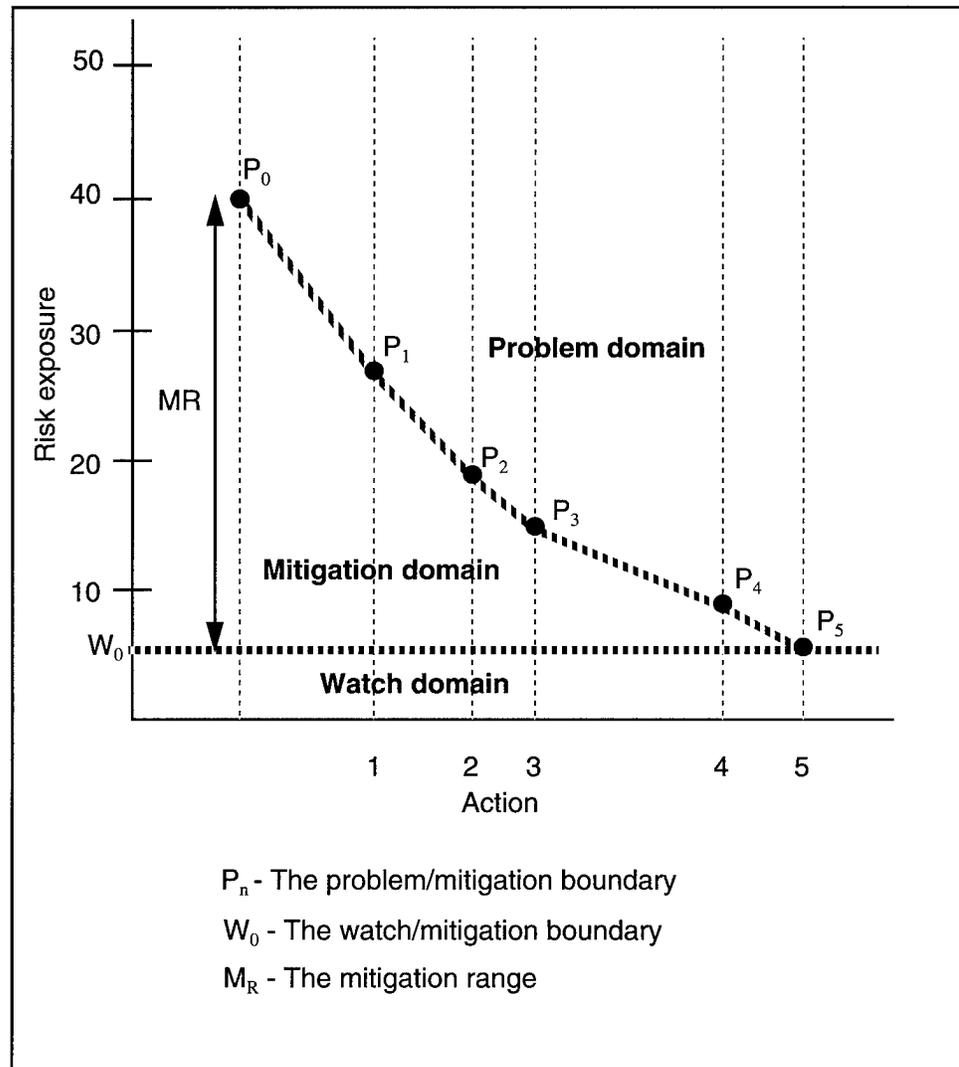
Section 9

Tracking Risk Exposure

Description

The impact and probability for the risk or risk set are periodically estimated by project personnel during risk mitigation, and risk exposure is then derived from them. The current value of risk exposure is added to the time graph in the mitigation status report during this task.

Note: Since the impact and probability have been evaluated qualitatively using ordinal numbers, the resulting risk exposure numbers must be used carefully. It should be used only as a guide to aid in decision making and to determine when plans are off-track.

Procedure

The following table describes the procedure for tracking risk exposure over time using a mitigation status report.

Step	Action
1	**Determine the current risk exposure.** The risk exposure is determined at regular time intervals by project personnel through discussion and consensus. The time intervals should be determined during planning and adjusted as necessary during tracking.
2	**Plot the risk exposure.** The risk exposure is plotted on the time graph portion of the mitigation status report.

Determining Risk Exposure Example

As described in Section 5 of this chapter, during the weekly project meeting, project personnel determine the risk set's current impact and probability through consensus and discussion. After the completion of one action of the mitigation plan, the risk exposure for the risk set under consideration is determined to be 16 from an impact of 4 and a probability of 4. This value is then plotted on the time graph.

Sample Mitigation Status Report

The completed mitigation status report for the example outlined in this chapter is shown in the following diagram.

Mitigation Status Report

Schedule
The project is understaffed and the requirements have changed; the software delivery might be late.

Risk ID

R23 R27

Date

4/15/95

Approach: ☐ Watch ☐ Accept ☒ Mitigate

Risk status

Impact (I)	4
Probability (P)	4
Current risk exposure (RE)	16
Initial risk exposure (RE)	20

☐ Green ☒ Yellow ☐ Red

Root causes

Description	Mitigation Summary	Actions
Inadequate development staff	Add 4 software engineers.	1, 3
The requirements have changed	Capture requirements changes and update the development plan.	2, 4, 5

**Example
Summary**

After the completion of Action 1, the risk exposure was not reduced to its expected level. This is visually shown on the mitigation status report on the previous page. The person or team responsible for controlling the risk set must decide whether alternative action is warranted. The decision is not solely based on the current value of risk exposure, because in this example the risk exposure was derived from ordinal values of impact and probability.

In this case, project personnel only use risk exposure as a guide. They will rely upon their experience and knowledge when they make decisions. In this example, project personnel have decided not to replan at this point; they will continue mitigating the risk set. The stoplight status has changed from green to yellow meaning that the plan is not working as intended, and while no management action is required at this point, future action may be required if the situation persists.

Section 10

Guidelines and Tips

General

Use templates to reduce the time necessary to construct the time graph and maintain a consistent appearance.

Use automated methods to do the calculations for constructing the time graph when appropriate. For example, a spreadsheet could be used to do the calculations necessary for constructing the graph.

Don't let the numbers dictate decisions. The numbers should be used as a guide to aid decision making and to determine when plans are off track. In the end, trust experience and instinct.

Consider using this report when reporting to senior managers; it can be effective if the managers are knowledgeable about risk and are interested in the details.

References

Cited in this chapter:

[Clark 95]

Clark, Bill. "Technical Performance Measurement in the Risk Management of Systems," Presented at the Fourth SEI Conference on Software Risk, Monterey, Ca., November 6-8, 1995. For information about how to obtain copies of this report, contact SEI customer relations at (412) 268-5800 or customer-relations@sei.cmu.edu.

Chapter A-17

Multivoting[1]

Ranked items

1 _____
2 _____
3 _____
4 _____
5 _____

 •
 •
 •

1. Multivoting is also referred to as "Weighted Voting" and as the "Making the Selection" part of the Nominal Group Technique method [Xerox 92] [Scholtes 88].

Section 1

Multivoting Description

Introduction

The multivoting method is a general voting method. It can be used to conduct a straw poll or select the most important items from a list with limited discussion and limited difficulty. For a large number of items, a series of votes is used to reduce the list to a workable number [Scholtes 88]. Each participant in the process votes on the items in the list.

Note: There are many variations on how to conduct the voting. This chapter outlines the SEI Risk Management Program's experience in conducting the multivoting method.

Diagram

The following diagram shows the input and output for multivoting.
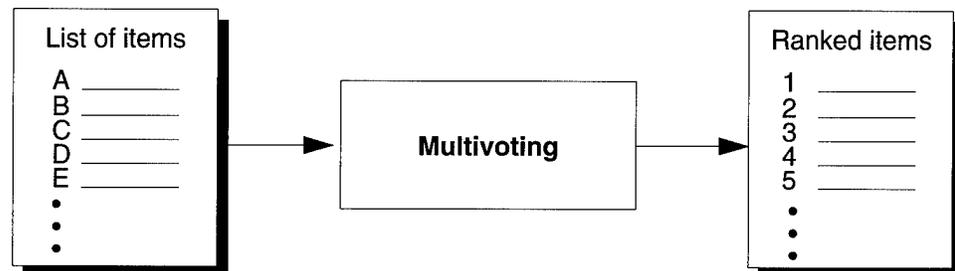
Personnel Requirements

The multivoting method requires a group of at least three participants. One person should be the facilitator and recorder (but he or she could still participate or contribute).

Section 2

When to Use

When to Use

Use this method
- to poll a group's position or preference
- to select the most important or popular items from a list
- when you have a large list of items (>20) to rank, and there is no need for degree of preference

Example: Item X is more important than item Y. We do not know how much more important item X is than item Y.

Constraints

Selecting the most important items from a large list (>20) cannot be achieved with one vote. A series of votes will be necessary to determine the priority of the top few items.

Benefits

This method
- is easy to use. All steps are straightforward.
- is quick. Each vote in a series can be conducted in a short period of time.

Section 3

Conducting a Multivoting Session

Procedure

The table below describes the procedure for conducting a multivoting session.

Step	Action
1	**Review items for understanding**. Facilitator ensures that all participants understand the items on the list.
2	**Select voting criteria**. This depends on the project objectives and constraints. The participants must decide what criteria are appropriate to use for ranking based on what's important to the project. *Examples* • Which items have a significant impact? • Which items are more likely to occur? • Which items have a greater impact on performance?
3	**Select number of votes**. Selecting the number of votes to be used depends on the number of items on the list. A general rule of thumb for the facilitator is to allow participants votes equal to one-third the number of items on the list [Scholtes 88, p. 2-41].
4	**Conduct voting**. Each participant votes individually. *Note*: There are two weighting variations • All votes are equal to one point. • Votes are weighted with respect to the total number of votes (example: With 5 votes, the #1 vote is weighted 5 points, the #2 vote is weighted 4 points, etc.).
5	**Rank items**. The facilitator calculates the final ranking. • Tally points. • Sort items by total points from highest to lowest.
6	**Review ranking with participants**. Facilitator reviews the results and allows the participants to react to and discuss the resultant ranking.
7	**If necessary, repeat steps 3-6**. For a large number of items, the final ranking may not be sufficiently distinct for the top items. In that case, reduce the list by removing items with few or no votes and conduct the voting again. This time members will have fewer votes to cast and the ranking of the top items will reflect the new vote.

Section 4

Multivoting Tools

**Sample
Voting Form**

Below is a sample voting form each participant would fill out.

Voting Form		
Item	**Points**
Item A	
Item B	
Item C	
• •	

**Sample Tally
Form**

Below is an example of a tally form [Scholtes 88] used to combine all individual votes. The total points per item is used to rank the items. In reviewing the ranking with the participants, the number of votes received per item can shed some light on why items were ranked a specific way. Did all the participants vote for an item but give it a low weight? Or did a few participants vote for the item and give it a high rank?

Tally of Votes

One participant's vote in points →

Item A
6, 10, 12, 5, 9 .... *42*   *Totals*

Number of votes →

Item B
15, 14, 15, 15, 13 ..... *72*

Item C
12, 12, 11 .... *35*
•
•
•

Total points per item

Example: Item A received 5 votes with a point total of 42. Item B received 5 votes with a point total of 72. Item C received 3 votes with a point total of 35.

Note: When all votes are of equal weight, the number of votes equals the number of points.

Sample Bar Chart

A bar chart [Scholtes 88] graphically displays the results of a multivoting session. The sample below corresponds to the results shown on the tally form.

Bar Chart
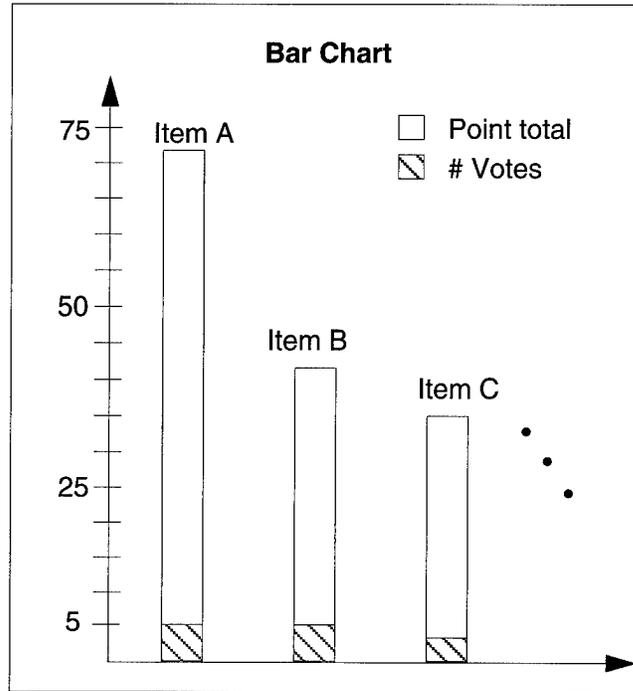
Section 5

Guidelines and Tips

General

There are a variety of ways to conduct the multivoting steps. For example if anonymity is not an issue, the participants could all put their votes on the same flipchart in the front of the room. Conduct the method using media that works for the group.

Large Lists

For lists with greater than 20 items, a series of votes will be necessary to determine the priority of the top few items.

Graphic Displays

If possible, use a graphic display of the results (e.g., bar chart) to show participants. It helps the participants to see why the ranking came out as it did and which items are close in the number of points and votes.

References

Cited in this chapter:

[Scholtes 88]

Scholtes, Peter R. *The Team Handbook: How to Use Teams to Improve Quality*. Madison, Wi.: Joiner Associates, Inc., 1988.

[Xerox 92]

Xerox Corporation and Carnegie Mellon University. *The University Challenge: Problem-Solving Process User Manual*. Stamford, Ct.: Xerox Corporation, 1992.

Chapter A-18

Pareto Top N
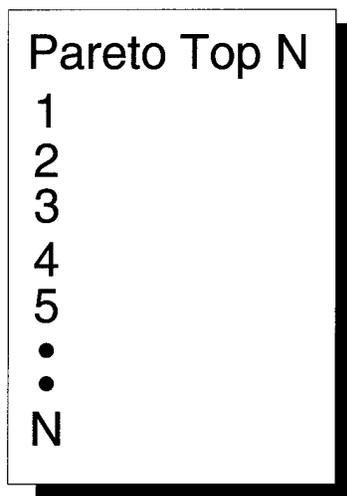
```
Pareto Top N
1
2
3
4
5
•
•
N
```

Section

Section 1

Pareto[1] Top N Description

Introduction   The Pareto top N method selects the most important risks to a project based on the attribute (impact, probability, and timeframe) information. The Pareto top N is generated by sequentially selecting risks based on the values for risk exposure (impact times probability) and timeframe. The result is an ordered list of important risks to the project.

Diagram   The following diagram shows the input and output for the Pareto top N method.

P = Probability
I   = Impact
RE = Risk exposure (IxP)
T = Timeframe
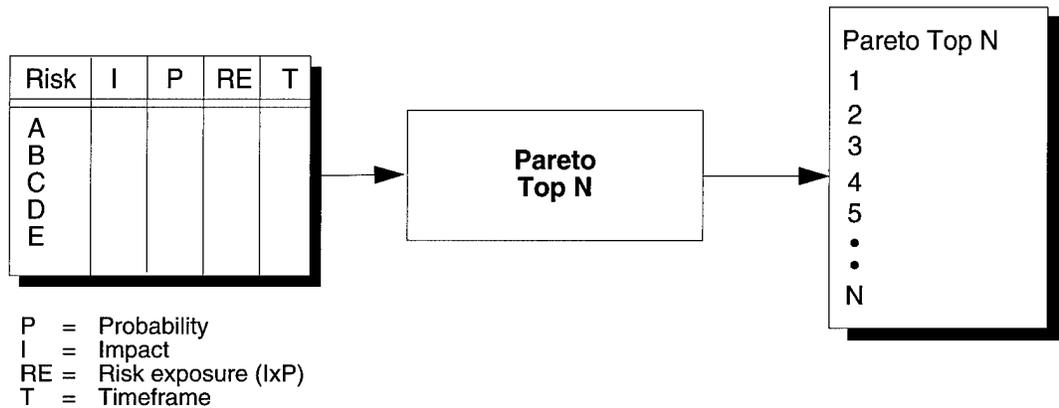
Personnel Requirements   One person is required to generate the Pareto top N.

---

1. This method is based on the Pareto principle where the "vital few" are separated from the "useful many" [Juran 89].

Section 2

When to Use

When to Use

Use this method

- to select the most important risks to the project based on the attribute (impact, probability, and timeframe) information
- after using the **Tri-level Attribute Evaluation** method [Chapter A-38]

Constraints

The method provides an ordered list of individual risks based on the risk exposure and timeframe values. It does not take into account a class or set of risks that individually have a low risk exposure but together represent a high level of risk exposure.

Benefits

This method

- provides a way to sort through a large amount of risks and determine which are the most important
- is easy to use. All steps are straightforward
- is not resource intensive

Section 3

Generating the Pareto Top N

Procedure

The table below describes the procedure for generating the Pareto top N.

Step	Action
1	**Gather all risks to be included in the Pareto analysis.** Gather all risk statements to be considered including the context, risk exposure, and timeframe information.
2	**Sort the risks based on the risk exposure and timeframe values.** Sort by risk exposure first, then timeframe. Order the risks from the risk with the highest value of risk exposure to the lowest value. If risks have the same risk exposure, then order the risk with the nearest timeframe first.
3	**Mark the break points for the top 10%, 20%, 30%, and 40%.** Count the total number of risks. Determine and mark where the cutoff points are for the top 10%, 20%, 30%, and 40%.
4	**Review the risks in the top 10%, 20%, 30%, and 40%.** Review the risks that made the 20% cutoff. Compare the risks below the cutoff (i.e., risks in the 30-40%) to those that did make the cutoff. Consider the following questions: • Are the risk exposure values the same or very close? • Are there any risks below the cutoff that should be included? • Is there a natural cutoff point?
5	**Select the top N percent.** Use your best judgment to draw the cutoff point at the appropriate place.

Section 4

Pareto Top N Tools

Sample Pareto Top N Summary Form

The following page shows a sample form used to determine the Pareto top N list following the use of the **Tri-level Attribute Evaluation** [Chapter A-38] method. It lists all of the risks in descending order based on the values for risk exposure and timeframe. The first column gives the risk ID number (or statement of risk). The second column shows the value for risk exposure. The third column shows the value for timeframe.

Note: If the tri-level attribute evaluation method was used, the risk exposure value will represent the consensus value for risk exposure reached by the participants. Similarly, the timeframe value will represent the consensus value reached by the participants in the method.

Pareto Top N Summary Form

		Risk ID	Risk Exposure	Timeframe
	1	19	High	Near-term
	2	23	High	Near-term
	3	21	High	Near-term
10%	4	39	High	Near-term
	5	20	High	Near-term
	6	13	High	Mid-term
	7	07	High	Mid-term
20%	8	01	High	Mid-term
	9	40	High	Mid-term
	10	22	High	Far-term
11	11	30	High	Far-term
30%	12	31	Moderate	Near-term
	13	09	Moderate	Near-term
	14	12	Moderate	Near-term
	15	08	Moderate	Mid-term
40%	16	18	Moderate	Mid-term
	17	02	Moderate	Far-term
	18	35	Moderate	Far-term
	19	05	Moderate	Far-term
	20	17	Moderate	Far-term
	•			
	•			
	40	11	Low	Far-term

Top 27.5%

Section 5

Guidelines and Tips

**Selecting
Percent for
Top N**

A rule of thumb is to select the top 20%. However, the project should consider whether this break point is appropriate. Are the risk exposure values so close that cutting off at 20% would arbitrarily omit important risks? Use the individual impact and probability attributes and context as background information when discussing the cutoff point. Use your best judgment in selecting the cutoff point.

**Automated
Support**

Having a computer application available which can sort the risks based on the risk exposure and timeframe values is helpful to complete Steps 1-3 in the procedure. A simple spreadsheet can save time and reduce the possibility of error.

References

Cited in this chapter:

[Juran 89]

Juran, J. M. *Juran on Leadership for Quality*. New York: The Free Press, 1989.

Chapter A-19

Periodic Risk Reporting

Status report	Date
Activities	
Problems	
Risks	

Section

Section 1

Periodic Risk Reporting Description

Introduction
The periodic risk reporting method integrates risk identification directly into project activities by requiring each individual or selected key individuals to periodically submit (mandatory and scheduled) risk forms or a status report that addresses any new risks they've identified.

Diagram
The following diagram shows the inputs and outputs of periodic risk reporting.

Risk Form

Individual uncertainties → **Periodic Risk Reporting**

Status report	Date
Activities	
Problems	
Risks	
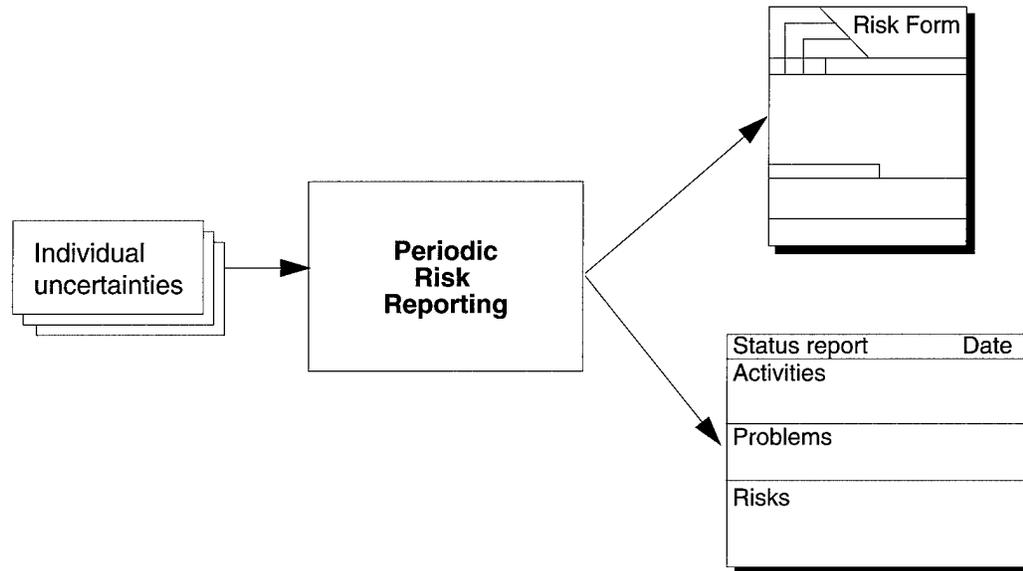
Personnel Requirements
All project personnel are required to add risk to their routine project status reports. Personnel should be trained in identifying risks, evaluating their attributes, and determining their classification.

Section 2

When to Use

When to Use   Use this method
- for continuous risk identification
- to integrate risk reporting directly into routine project activities
- for fostering a risk awareness throughout the project

Constraints   This method will not be effective in a culture that does not have open communication or where there is little trust or rapport between managers and other personnel.

Benefits   This method is easily integrated into routine project practices through expansion of existing reports and additional topics during routine meetings.

Section 3

Performing Periodic Risk Reporting

Procedure

The table below outlines basic steps for the periodic risk reporting method.

Step	Action
1	**Establish the policy**. Project management must • decide on who will participate • decide on the reporting frequency and instrument • decide on the forum to be used • communicate these decisions to all personnel involved
2	**Prepare**. Prior to a scheduled submission or project meeting, each individual involved should review the current listing of risks, the basis and structure for classification, and other triggers (e.g., the Short TBQ [Chapter A-29]) to determine if conditions have changed and whether or not any new risks have emerged.
3	**Conduct the submission/review process**. All project personnel will • submit reports • review and discuss them at appropriate meetings
4	**Document the newly identified risks**. If a risk database is being used, new risks should be added by whoever is in charge of data entry. If risks are being kept on paper, each person who identifies a risk is responsible for proper documentation.

Section 4

Periodic Risk Reporting Tools

Types of Tools or Reports

There are two types of tools or forms that can be used for periodic risk reporting, as shown in the table below:

Reporting Instrument	Description
Risk form	The Risk Form [Chapter A-26] is completed for each identified risk. If no risks have been identified, a risk form marked "none identified" can be submitted to help ensure that everyone's work was collected.
Project status report: risk identification summary	A section of a standard project status report is used. This section, the risk identification summary, includes the following information on newly identified risks: • statement of risk • context • impact • probability • timeframe • classification The word "none" can be used to indicate there are no new risks at this time.

Sample Risk Identification Summary

On the next page is a sample of a routine project status report with the addition of summary information on newly identified risks.

Weekly status for John Smith	**4/3/96**

Activities

Received new CPUs, completed installation, and began testing. See risk below.

Revised projections for coding assigned components and submitted to Master Schedule.

Took training class on new development tools.

Problems

No new problems to report.

Risks (include statement, context, impact, probability, timeframe and classification)

Risk: CPU performance is 20% slower than expected; deliverable performance is in jeopardy. We expected better performance from this machine, per manufacturer's specifications, but it's not there. Current design was based on those specifications and we may not be able to compensate.

Impact: High—Could fail to meet customer needs

Probability: High

Timeframe: Near—We'd better do something now.

Classification: Design/performance

Section 5

Guidelines and Tips

Approach

An effective approach is to integrate risk reporting with the project's routine development and status reporting processes.

Example:
- Risk reporting can be required concurrently with regular weekly status reporting.
- Newly identified risks (or lack of newly identified risks) can be addressed as an agenda item within regularly scheduled status or review meetings.
- Risks can be identified at the conclusion of other types of meetings (e.g., Have we surfaced any new risks during this design review?).

**Review
Effectiveness
of Method**

Monitor the process; if it does not appear to be working, consider alternative methods, perhaps regular individual **Taxonomy-Based Questionnaire Interviews** [Chapter A-33] to stimulate risk identification.

References

For more on the Software Development Risk Taxonomy, see the following:

[Carr 93]

Carr, Marvin; Konda, Suresh; Monarch, Ira; Ulrich, Carol; & Walker, Clay. *Taxonomy-Based Risk Identification* (CMU/SEI-93-TR-6, ADA266992). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

Chapter A-20

PERT Charts

Description

PERT (program evaluation and review technique) charts are a commonly used management tool for managing time and cost (along with critical path networks). They are one of many network management techniques.

How to Use

PERT charts can be used to manage a complex risk mitigation strategy and the interdependencies of the strategy activities. A PERT chart should at a minimum show
- the sequence of activities
- the duration of each activity
- the time necessary to complete the project (i.e., critical path)

Depending on its complexity, the following additional information can provide insight into the management of the mitigation strategy:
- the earliest expected time for starting and stopping all activities
- the latest expected time for starting and stopping all activities
- available slack on activities

Example Background

The following example looks at a sample risk statement and shows the mitigation goals for the mitigating actions, the key issues revolving around the risk, and the task activities.

Risk Statement
- The translation effort looks like it will slip; if it does, the whole test schedule will be in jeopardy.

Mitigation Goals
- Modify the schedule with possible completion date further out.
- Incur no cost increase.
- Identify a drop-dead date and include a buffer.
- Get to independent validation & verification with "quality" product (i.e., one that satisfies requirements).

Key Issues
- software and firmware maturity
- test lab time
- system performance requirements
- repair priority
- spares

Task Activities

- Produce aggressive test strategy for firmware-software (evaluate interface and performance).
- Develop test case and scenarios for areas of concern.
- Develop summary stress test.
- Clarify lab tasking and control.
- Establish priority for spares.
- Develop realistic serial-parallel schedules.

**Example
PERT Chart**

This PERT chart shows the sequence and duration of activities for the sample risk statement using the activity-on-arrow representation.

Critical path = 52 days
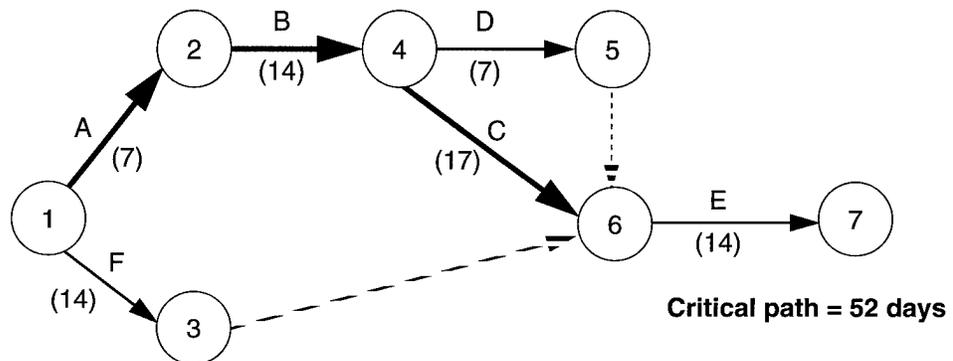
Key

(#)	Node (representing the beginning or ending of an activity)
——▶	Activity
----▮▶	Dummy activity
━━▶	Critical path
(#)	Duration in days

Activities

A   Produce aggressive test strategy for firmware-software (evaluate interface and performance).

B   Develop test case and scenarios for areas of concern.

C   Develop summary stress test.

D   Clarify lab tasking and control.

E   Develop realistic serial-parallel schedules.

F   Establish priority for spares.

Note: There are many variations on drawing the network (e.g., event-in-node, activity-in-node, activity-on-arrow). Different sources describe the PERT method differently.

References

For more information on PERT charts, see the following:

[Bennatan 92]   Bennatan, E. M. *On Time, Within Budget - Software Project Management Practices and Techniques*. McGraw-Hill International (UK) Limited, 1992.

[Mayrhauser 90]   Mayrhauser, Anneliese von. *Software Engineering: Methods and Management*. San Diego Ca.: Academic Press, Inc., 1990.

[Meredith 89]   Meredith, Jack R. & Mantel, Samuel J. Jr. *Project Management: A Managerial Approach*, 2nd ed. New York: John Wiley and Sons, 1989.

[Pfleeger 91]   Pfleeger, Shari Lawrence. *Software Engineering: The Production of Quality Software*, 2nd ed. New York: MacMillan Publishing Co., 1991.

[Pressman 92]   Pressman, Roger S. *Software Engineering: A Practitioner's Approach*, 3rd ed. New York: MacGraw-Hill, Inc., 1992.

[Shere 88]   Shere, Kenneth D. *Software Engineering and Management*. Englewood Cliffs, N.J.: Prentice Hall, 1988.

[Thayer 88]   Thayer, Richard H. *Software Engineering Project Management Tutorial*. Washington D.C.: Computer Society Press of the Institute of Electrical and Electronics Engineers, Inc., 1988.

[Umbaugh 89]   Umbaugh, Robert E. & Gitomer, Jerry. "Project Scheduling and Control," 37-48. *Handbook of Systems Management: Development and Support*. Boston, Ma.: Auerbach Publishers, 1989.

[Xerox 92]   Xerox Corporation and Carnegie Mellon University. *The University Challenge: Problem-Solving Process User Manual*. Stamford, Ct.: Xerox Corporation, 1992.

Chapter A-21

Planning Decision Flowchart

Description

The planning decision flowchart is an aid for planning a risk or set of related risks. It acts as a checklist and decision tool to assist planners in deciding what to do with a particular risk(s).

How to Use

Use the planning decision flowchart as a checklist to consider all the relevant aspects of deciding what to do with a risk. Follow the flowchart, asking the questions about the risk(s) being planned and making the appropriate decisions.

Assign Responsibility

The decisions made relative to assigning responsibility are

- *keep*: Retain responsibility, authority, and accountability for risk.
- *delegate*: Retain accountability and assign authority and responsibility to someone in the project who reports to the person delegating the risk.
- *transfer*: Shift accountability, authority, and responsibility to someone outside the organization (vertical or horizontal shift).

Determine Approach

The decisions made relative to the approach to be taken in planning are

- *research*: Investigate the risk until it is understood well enough to make a decision to accept, watch, or mitigate.
- *accept*: Live with the risk, do nothing and treat it as a problem if it occurs.
- *watch*: Monitor the risk for significant changes.
- *mitigate*: Determine the appropriate strategy and actions necessary to reduce the probability or impact of the risk.

Define Scope and Actions

The decisions made for scope and actions are the following:

- *action item list*: A series of action items is sufficient for identifying, describing, and tracking the mitigation strategy and actions.
- *task plan*: The mitigation strategy is complex and costly enough to deserve a detailed plan. The task plans should be consistent with the project's task plan standards and include schedules, **Gantt Charts** [Chapter A-12], **Work Breakdown Structures** [Chapter A-40], budgets, resource allocations, etc.

Flowchart

The planning decision flowchart is provided on the following page.

Planning Decision Flowchart

Statement of risk

Context
Impact
Probability
Timeframe
Classification
Rank

Review risks

Responsibility:
Is it my risk?

Is it my task to deal with this risk?

no → Is it internal to my organization?

no →

yes ↓

yes ↓

Keep

Delegate

Transfer

Approach: Can I do anything?

Do I know enough about this risk?

no → **Research**

Research plan

yes ↓

Can I live with this risk?

no → Can I act on this risk?*

no →

Tracking requirements

Acceptance rationale

yes ↓

yes ↓

Accept

Mitigate

Watch

Scope and actions:
What should I do?

Mitigation plan

Mitigation Plan

Risk action item list

Item 1- do xxxx
Item 3-do yyyy
Item 12- do zzz

yes ← Is an action item list enough?

no →

Task plan

Responsibility
Goals
Tasks

WBS

Schedule
____
____

* Or "Do I need to act on this risk?"

Chapter A-22

Planning Worksheet

Description

The planning worksheet is a support tool used during risk planning to identify, analyze, and document alternative mitigation actions and decisions. It also acts as a historical record of the information and alternatives gathered and considered while deciding on the mitigation actions.

How to Use

Planning worksheets can be used by individuals or groups as they develop mitigation plans. Data is filled in during group sessions or as they become available. Data may be gathered from multiple sources or personnel. Once a decision has been made on which mitigation strategies and actions to take, the decision is documented and the chosen strategies and actions can be moved to another form, such as an **Action Item List** [Chapter A-1] or task plans (see **Problem-Solving Planning** [Chapter A-24]).

Note: If used to plan a set of related risks, the field for identifying related risks becomes one for identifying the rest of the set, rather than documenting an existing (already implemented) risk and mitigation plan.

Planning Worksheet Template

A planning worksheet template is shown on the next page. Modifications can be made to suit the needs of the organization or project.

Planning Worksheet	
Risk ID	**Responsibility**
Risk statement	
Mitigation goals and constraints (in observable terms)	
Additional data (e.g., root causes, impacted elements)	
Related risks	
Alternative strategies/actions	
Related mitigation plans	
Strategy evaluation criteria	
Chosen strategy/actions	**Success measures**
Contingency strategy	**Contingency trigger**

**Field
Descriptions**

The following table provides a description of the fields on the planning worksheet.

Field Name	Description
Risk ID	Unique identifier for the risk
Responsibility	Person or personnel responsible for this risk and its mitigation
Risk statement	Statement of risk
Mitigation goals and constraints	Goals and constraints for mitigation of this risk—e.g., risk exposure reduction target, resource limitations, schedule drivers, etc. These are used to evaluate the success of the strategy.
Additional data	Other relevant data needed to help define strategies or understand the risk, such as root causes, quantified impact and probability, etc.
Related risks	From the classification information—the risks which may benefit from or impact the mitigation of this risk. Or, the other risks in a set of related risks.
Alternative strategies/actions	The most viable alternative strategies for mitigating this risk. This is useful information in case the chosen strategy fails. Cost estimates should be documented, if known.
Related mitigation plans	Any mitigation plans already implemented that may have an effect on the plans for mitigating this risk
Strategy evaluation criteria	Criteria for evaluating the alternatives in order to make a decision—e.g., cost of strategy, effect on risk, schedule impacts, etc.
Chosen strategy/actions	The selected strategy for mitigating the risk
Success measures	Measures or indicators used to evaluate progress and success of the mitigation strategy
Contingency strategy	A contingency strategy to be used if the selected strategy fails
Contingency trigger	What triggers the implementation of the contingency strategy, e.g., a specific date or threshold condition

**Sample
Planning
Worksheet**

A completed version of the previous template for a planning worksheet is shown on the next page.

Planning Worksheet	
Risk ID 121	**Responsibility** John Smith

Risk statement No system simulation was done; we may not meet performance requirements.	

Mitigation goals and constraints (in observable terms)
Reduce impact of risk by 50%.

Additional data (e.g., root causes, impacted elements)
Root causes: inadequate simulation done at start of the project, poorly defined performance from customer

Worst case impact: loss of contract—$10 million, if we fail to meet whatever performance requirements are in the contract

Related risks   79, 62

Alternative strategies/actions	Estimated costs:
1. Redo simulation and request change in requirements.	1. $200,000
2. Monitor performance and hope it doesn't happen.	2. $1,000
3. Monitor performance; research and prepare a contingency plan to change the contract.	3. $34,000
4. Use plans for risk #79.	4. No cost

Related mitigation plans   Risk #79's plan asks for a contract modification to upgrade CPU memory—will improve system performance by 36%— enough to meet the requirements associated with this risk.

Strategy evaluation criteria	Cost is sole criteria—schedule not important at this point.

Chosen strategy/actions	Success measures
4. Use risk #79's plan if their contract modification for upgrading the CPU memory is approved.	• Contract mod is approved by 7/8/95.
	• Performance tests meet average 2 second response time.

Contingency strategy	Contingency trigger
1b. Request a change in requirements. (no cost)	• #79's contract mod request is disapproved.

Chapter A-23

Potential Top N

Potential Top N

1

2

3

4

5

•

•

N

Section

Section 1

Potential Top N Description

Introduction

The potential top N method selects the most important risks to a project based on the individual knowledge of the participants in the project (using the results of the **Top 5** [Chapter A-37] method). The potential top N is generated by sequentially selecting risks from each individual top 5 list in rounds until all risks are selected. The result is a non-ordered list of important risks to the project.

Note: When this method is being used during a **Baseline Identification and Analysis** [Chapter A-4] event or any other group activity, there is an individual top 5 list per each participant.

Diagram

The following diagram shows the input and output for the potential top N method.
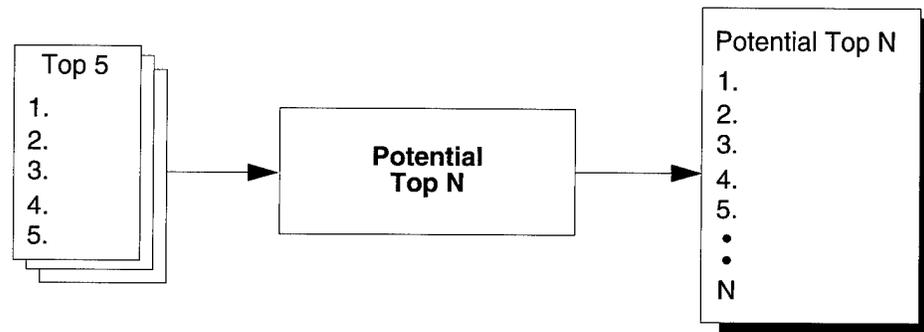
Personnel Requirements

Generating the potential top N requires one person.

Section 2

When to Use

When to Use

Use this method
- to select the most important risks to the project from each participant's point of view
- following the use of the **Top 5** [Chapter A-37] method

Constraints

The potential top N provides broad categories of risks based on the highest individual top 5 evaluations. Within each category there is no relative ranking. For example, there is no distinction between all the risks evaluated as number one.

Benefits

This method
- is easy to use. All steps are straightforward.
- does not require resource-intensive activities
- is quick. The potential top N can be generated in less than a half hour.
- focuses on the individual perspective which may carry unique knowledge

Section 3

Generating the Potential Top N

Procedure

The table below describes the procedure for generating the potential top N.

Step	Action
1	**Conduct first round**. Select the number one risk from each "top 5" list.
2	**Repeat for rounds 2-5**. Select the number two risk from each "top 5" list. Repeat this step for risks ranked as number three, four, and five respectively.

Note: If the choice of one participant in a given round is already on the list, move on to the next participant. A risk will show up only once on the list—at the highest round selected.

Example: Participant A selected risk X as #2, participant B selected risk X as #3. The result would show risk X with the other risks ranked #2.

Section 4

Potential Top N Tools

Sample Top 5 Summary Form

Below is a sample form used to construct the potential top N list during baseline risk identification and analysis. It represents a summary of all the top 5 lists. As each round is conducted the results are captured on the form. The first column gives the risk ID number (or statement of risk). Each subsequent column shows which risks were selected as the top 5 by each participant, labelled as P1, P2, etc.

Top 5 Summary Form

	Risk ID	Group 1			Group 2		Group 3		
		P1	P2	P3	P1	P2	P1	P2	P3
1	G1.14	1	2						
2	G1.21		1						
3	G1.22	4		1					
4	G2.3				1	1			
5	G3.4						1		1
6	G3.14						2	1	
7	G1.3	2							
8	G1.18			2					
9	G2.11				2				
10	G2.23					2			
•									
•									
X	G3.11						5		

First round risks (arrows point to rows 1–6)
Second round risks (arrows point to rows 7–10 and below)

Note: Each risk is denoted by a GX.Y identifier where X is the group session number and Y is the number the risk was given during that session.

Example: In the above example, group 1 had three participants, group 2 had two participants; group 3 had three participants. The form shows:
- There are six distinct risks that were labelled number one.
- There are two cases where participants chose the same risk as number one (group 2 risk G2.3 and group 3 risk G3.4).
- There are three cases where a risk was chosen as number one by one participant and that risk was chosen by another participant in the same group as one of their other top 5 risks.

Section 5

Guidelines and Tips

Number of Risks

The size of the potential top N list will vary based on the number of participants and the overlap on the top 5 risks.

Chapter A-24

Problem-Solving[1] Planning

Section

1. This process is adapted and derived from three key works: Xerox's problem solving process, provided to SEI as a part of quality improvement methods [Xerox 92] in a Xerox/SEI initiative; Scholtes' Team Handbook [Scholtes 88]; and the Lumsdaines' Creative Problem Solving [Lumsdaine 90]
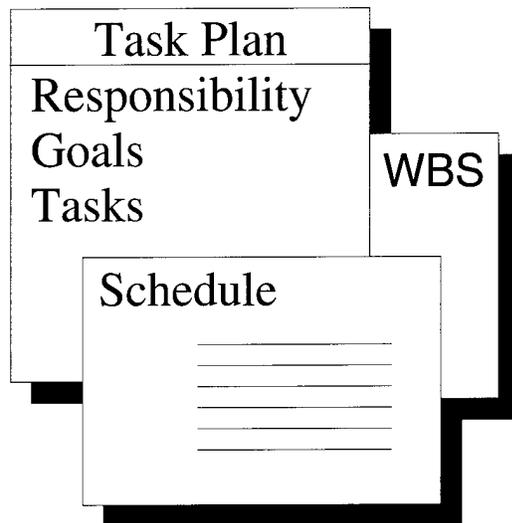
Section 1

Problem-Solving Planning Description[1]

Introduction

Problem-solving planning is a process to produce task plans for mitigating a risk or a set of related risks. It is a multi-step procedure with a suite of methods that can be used at each step. The end result is a risk mitigation task plan, similar to a project task plan, that describes the actions to be taken in mitigating the risk(s).

Note: It is assumed that each project will have its own standards for content and format of task plans.

Diagram

The following diagram shows the inputs and outputs for problem-solving planning.
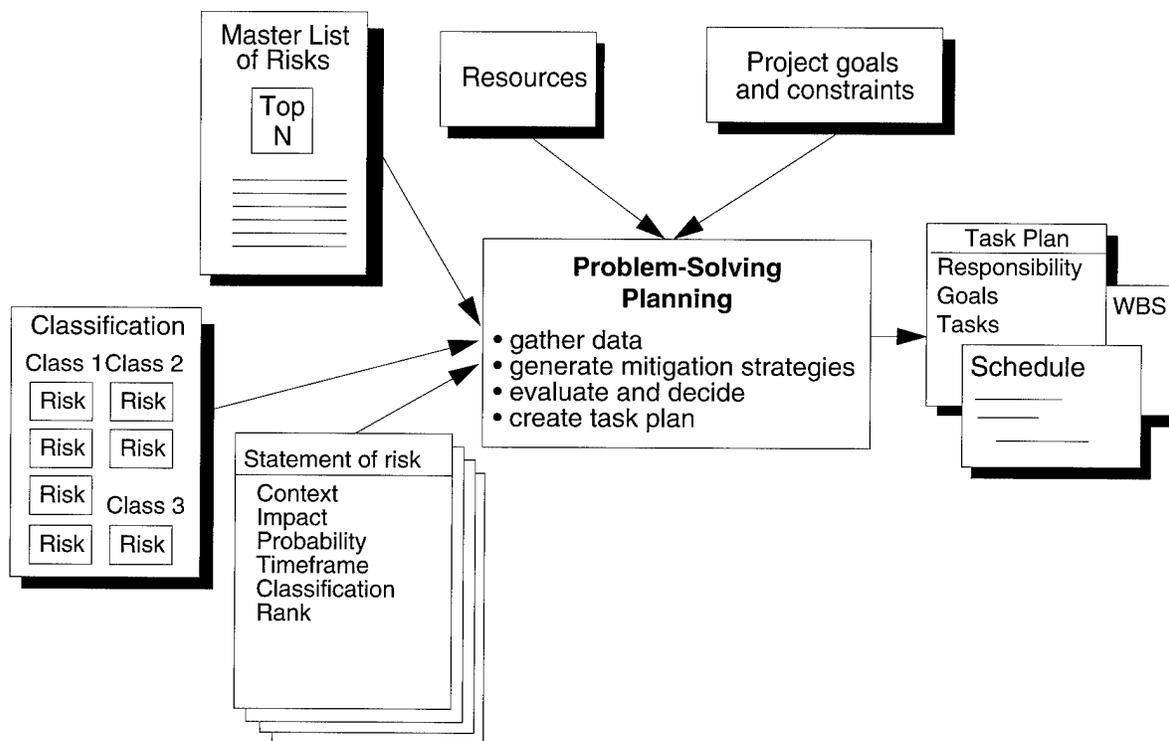
Personnel Requirements

This method can be used by one person, but is generally used by a group of knowledgeable personnel brought together to specifically address the risk(s). Typically, the group will be most effective when a trained facilitator leads the procedure. All of the activities and methods referenced in problem-solving planning can also be performed by a group or individual.

Overall Procedure

The following procedure table summarizes the major steps in problem-solving planning. Each major step is further decomposed in later sections.

---

1. **Baseline Planning** [Chapter A-5] is a variation for dealing with several sets of related risks, where coordination is needed across mitigation plans. It does not, however, necessarily reach the actual development of a task plan as the primary intent is to avoid conflicts and duplicated effort in the plans.

Step	Action
1	**Gather data**. Identify the data needed to understand this risk and develop effective mitigation plans. Select and apply the appropriate methods for data gathering.
2	**Generate mitigation strategies**. Generate ideas, eliminate the obviously inappropriate ones, review and clarify the remainder.
3	**Evaluate and decide**. Select evaluation criteria, evaluate the alternative strategies, decide which strategies to use and, optionally, select a contingency strategy.
4	**Build and approve a task plan**. The task plan should include tasks, responsibilities, schedules, success measures, and risk metrics. Task plans should be consistent with existing project planning methods and tools.

Methods and Tools

The following table provides a summary of the methods and tools that support problem-solving planning, and associated activities.

Activities	Methods and Tools
For all activities	Planning Worksheet [Chapter A-22]
Gather data	Brainstorming [Chapter A-7]
	Cause and Effect Analysis [Chapter A-8]
	Interrelationship Digraph [Chapter A-14]
	More detailed attribute analysis (e.g., go from Binary Attribute Evaluation [Chapter A-6] to Tri-level Attribute Evaluation [Chapter A-38])
Generate mitigation strategies	Brainstorming [Chapter A-7] and its variation—brainwriting
Evaluate and decide	Affinity Grouping [Chapter A-2]
	Cost-Benefit Analysis [Chapter A-11]
	Interrelationship Digraph [Chapter A-14]
	List Reduction [Chapter A-15]
	Multivoting [Chapter A-17]
Build and approve a task plan	Gantt Charts [Chapter A-12]
	Goal-Question-Measure [Chapter A-13]
	Interrelationship Digraph [Chapter A-14]
	PERT Charts [Chapter A-20]
	Work Breakdown Structure [Chapter A-40]

Section 2

When to Use

When to Use

Use this method
- to plan a complex risk, or set of risks
- when planning for this risk or set of risks requires the expertise and knowledge of several people
- when a complex set of actions is needed to mitigate the risk(s)
- when mitigation resource expenditure will be significant
- when detailed plans and schedules are required
- when management approval of the mitigation plan will be needed

Constraints

This method will involve applying a series of other methods, and thus requires more time than other options.

Personnel need to be familiar with the methods used by problem-solving planning or have a leader or facilitator available who can direct the group in using the methods.

Benefits

This method
- provides an organized structure and flow for applying multiple methods while planning a complex risk or set of risks
- provides the additional depth and breadth of planning needed for critical (top N) risks
- when used by a group of people, supports the synergy needed to identify new insights and possibilities
- supports the use of common strategies from other risks; the classification data can identify related risks when a new risk is being planned. For example, if a new risk relating to requirements stability is identified, looking at the set of other requirements stability risks will tell planners if the existing mitigation plans already address the new risk or if the plans need to be updated.

Section 3

Gather Data

Description For the risk(s) to be planned, decide if there is enough data about the risks to begin generating strategies and making informed decisions. If more data is needed, use the appropriate analysis or data gathering methods. There is a trade-off between how much data is enough and the value added of more data.

Procedure The following table describes the procedure for gathering data.

Step	Action
1	**Identify needed data.** • Decide what additional information is needed about these risks (e.g., root causes, quantitative impact estimates, etc.). • Review the mitigation goals and constraints for understanding. • Check for related risks (using classification data as pointers) and gather information about implemented mitigation plans (e.g., Is the plan working?). • Use the expertise of project personnel to determine what type of additional information could be useful.
2	**Select and apply methods.** Based on what data is needed (mitigation goals, constraints, planning effort, and other criteria), select appropriate methods to gather and analyze data and execute those methods to build the risk picture.
3	**Verify data.** Verify that there are no conflicts, unexpected results, or unexplained gaps. If there are, resolve them before proceeding.

Example of Data Gathering Two critical, interrelated risks with major impact must have their impact eliminated. The planners look for root causes, fully identify all system components that could be affected by these risks, and quantify the impact and probability to support careful evaluation of strategies.

**Types of
Information**

The table below identifies some of the types of additional information that can be gathered and why it would be needed.

Information	Purpose
Risk causes	Support reduction or elimination of the risks by attacking the causes
	Determine which root causes to correct due to their degree of influence on the risks
More detailed evaluation of attributes	Justify cost of mitigation strategy
	Enable more informed decisions on strategy selection— return-on-investment (ROI)
Impact targets	Understand what is being impacted, and how much
	Decide between mitigation strategies based on relative importance of the affected targets
Nature of risk relationships	Understand interdependencies
	Example: If the consequences of Risk A cause Risk B, it may be more effective to tackle Risk A before B.
Condition information	Improve knowledge of the conditions leading to the risk and their relative influence to better understand what needs to be mitigated
Other influences	Help determine effective solutions by knowing what other factors will influence these risks and their mitigation
	Example: The identifier of risk A, which impacts several components, may have been unaware of a pending change request by the customer that would eliminate the risk.

Methods and Tools

The table below summarizes the methods and tools that can be used to gather additional data.

Method or Tool	Description	When to Use
Brainstorming [Chapter A-7]	Idea generation method	To identify all information and possibly useful data related to the risk(s)
Cause and Effect Analysis [Chapter A-8]	Diagramming technique used to look for the root causes of risks.	To identify targets for mitigation strategies (e.g., eliminate the root causes)
Interrelationship Digraph [Chapter A-14]	Diagrams the relationships between risks in a set, their causes, and sometimes their impacts.	To increase understanding of a set of risks To find cycles of dependencies, root causes (or risks) To identify critical risks in a set (which ones must be mitigated)
Planning Worksheet [Chapter A-22]	Worksheet to document information gathered	As a checklist for planning and for documenting information and decisions
More detailed risk attribute analysis* Tri-level Attribute Evaluation [Chapter A-38]	Expands the analysis of the risk attributes of probability, impact, and timeframe through • more levels or quantitative • types (e.g., determine type of impact, such as technical, cost or schedule)	To provide greater depth of detail in support of more refined strategy evaluation and mitigation success measures

*Note: See **Analyze** [Chapter 5] for additional explanation.

Section 4

Generate Mitigation Strategies

Description

This activity develops a list of alternative mitigation strategies for the risks. This is an idea-generation activity to look at the risks from many viewpoints and think about new and unique ways to resolve them. When risks are being planned, all viable alternatives need to be considered. The most effective solution is not always the first, most obvious, or immediate one, particularly with complex risks. Effective risk management requires a system perspective in order to find the most effective mitigation plans. This often requires spending time considering the possibilities.

Procedure

The table below describes the procedure for generating alternative strategies.

Step	Action
1	**Generate ideas.** Using one or more of the methods below, generate as many ideas as possible.
2	**Eliminate the obvious.** Filter out any strategies that do not meet project constraints.
3	**Review and clarify.** Review each alternative for understanding and clarify as needed. *Note*: Consistent evaluation would be difficult without mutual understanding from all members of the group.

Methods and Tools

The table below summarizes the methods and tools that can be used to generate alternative strategies.

Method or Tool	Description	When to Use
Brainstorming [Chapter A-7]	Group technique in which people state ideas as they occur to them; each can build on the ideas of others	Need a lot of ideas Need to think beyond traditional boundaries
Brainwriting [Chapter A-7]	A variation of brainstorming but each participant writes their ideas down instead. Fewer, but better-developed ideas generally result.	Need quality over quantity Personality conflicts are likely
Planning Worksheet [Chapter A-22]	Worksheet to document information gathered	As a checklist for planning and for documenting information and decisions

Section 5

Evaluate and Decide on Strategies

Description

This activity reduces the list of alternative strategies to a reasonable few from which a final decision can be made to achieve an acceptable trade-off between the mitigation goals and what is affordable.

This includes
- minimizing risk to the project
- maximizing return on investment in mitigation strategies
- maximize opportunity and value

"Making good choices depends on three elements: the quality of our definition of specific factors that must be satisfied, the quality of our evaluation of the available alternatives, and the quality of our understanding of what these alternatives can produce—for better or worse." [Kepner 81]

Procedure

The following table describes the steps to be taken in evaluating the list of alternative strategies and deciding which one(s) is best.

Step	Action
1	**Identify existing mitigation plans**. Plans that relate to the strategies on this list or belong to the related risks should be reviewed. These plans may already be in place, with either contingency actions or actions already in progress. Collect the following data on the related action plans: • strategies • progress • indication of success of strategies
2	**Identify evaluation criteria**. These criteria are used in evaluating the strategies for selection. See the following table for examples of evaluation criteria.
3	**Evaluate alternative strategies**. Choose and apply a method from the Methods and Tools table to reduce the list. Repeat as needed until a reasonable few (e.g., two to five) remain. *Example*: Look for • strategies that meet the most criteria • strategies that can be merged • conflicting strategies
4	**Review existing mitigation plans**. Determine if any strategies on the reduced list will adversely impact those plans. *If yes*: Identify responsible personnel to coordinate the actions, should the conflicting strategies be chosen. *If no*: Skip to step 5.

Step	Action
5	**Decide on strategies.** Review reduced list and, using all the information available as well as judgment and experience, choose the strategy (or combination of strategies) that best mitigates the risks (merge and decompose strategies as necessary to arrive at a viable strategy). Decide if the selected strategy is to be implemented now or held for contingency.
6	**(Optional) Select contingency strategy.** From the remaining alternatives, decide if one would be useful as a contingency plan if the primary strategy fails. Identify a trigger point to use as an indicator for when the contingency plan should be put into effect.

Evaluation Criteria

The following table identifies some of types of criteria for evaluating strategies.

Criteria Type	Examples
Reducing risk	Reduction in one or both of the following: • impact • probability
Minimizing investment	Strategy cost factors include • personnel • capital equipment • documentation • other resources (facilities, time, etc.)
Minimizing schedule impact	Strategy enables schedule to be met but requires more personnel resources.
Minimize delivered system impacts	Changes to • requirements • design • performance
Minimize customer impact	Strategies may require effort by the customer, such as acquiring or delivering customer-furnished equipment.
Minimize process impact	Changes in the way the project is managed can cause ripples across the project. For example, tightening configuration management processes could add work at the beginning of the schedule but would improve control of the product.
History of success	This strategy has been tried before and been successful.
Influence of external factors	Strategies can be impacted by changes in corporate funding, federal and local regulation, competitor activities, etc. [Kepner 81].

**Cost vs.
Benefits**

A **Cost-Benefit Analysis** [Chapter A-11] determines the acceptable ratio between the total costs for a particular strategy and its benefits. Fixing a *potential* problem now may cost less than fixing the actual problem later, when the impact could be more severe.

Consider the following:
- cost of risk impact if not mitigated
- cost of risk impact if mitigated ($0 if eliminated, >$0 if reduced)
- cost of risk mitigation (e.g., resources, schedule, impacts on the project)

Risk mitigation return-on-investment then might be:

$$\text{Cost of risk impact (if not mitigated)}$$

$$\text{Cost of risk impact (mitigated)} + \text{Cost of risk mitigation}$$

**Methods and
Tools**

The following table summarizes the methods and tools that can be used individually or in groups to evaluate the alternative strategies.

Method or Tool	Description	When to Use
Affinity Grouping [Chapter A-2]	Group related strategies based on some criteria, including the evaluation criteria	To eliminate duplicates To identify distinct strategies, which could be combined into a more complex strategy
Cost-Benefit Analysis [Chapter A-11]	Estimates the costs and benefits for each strategy.	To compare strategies based on their costs and benefits
Interrelationship Digraph [Chapter A-14]	Graphic depiction of relationships and dependencies between items	To help reduce the list by determining which strategies or actions depend on each other
List Reduction [Chapter A-15]	Reduction is achieved by applying the evaluation criteria. Consensus or voting is used. Process is repeated until the desired or some reasonable number (e.g., six) of strategies is reached, at which time another method can be used.	To eliminate the obvious To reduce a large list When criteria can distinguish alternatives
Multivoting [Chapter A-17]	Individual votes are distributed across the risks, with the option to cast more than one vote (including all of one's votes) on one risk.	To work towards consensus within a group When a simple, fast method is needed
Planning Worksheet [Chapter A-22]	Worksheet to document information gathered	As a checklist for doing planning and to document information and decisions

Multi-Method Example

Given a list of 30 alternatives, list reduction can be used to pare it down to eight. An interrelationship digraph would indicate any dependencies among the choices that would prevent elimination or would eliminate groups of strategies. Mulitvoting could then be used to get to the best three. A cost-benefit analysis of the remaining three would point out which one would provide the optimal solution.

Section 6

Create Task Plan

Description

Once a strategy is selected, the decision is documented and the work is assigned. As part of integrating risk management with project management, existing corporate or organization standards for documenting task plans should be used. It is important to ensure that relevant data and decisions are captured. The risk mitigation task plan should

- support tracking the plan and determining successful completion
- allow identifying deviations from the expected results
- ensure understanding by all personnel on required actions
- facilitate management approval before proceeding with actions

Procedure

The following table describes the steps in creating a task plan.

Step	Action
1	**Build task plan.** Select the appropriate plan template and document the plan based on the data collected and evaluated. Gather and develop additional data (e.g., specific personnel assignments) as needed to complete the plan.
2	**Approve task plan (if required).** When risks are delegated throughout the organization, the delegator makes it clear whether or not final approval of the mitigation plan is required. Management approval may be needed to ensure that • resources are not overcommitted • conflicting plans are not implemented • project objectives and constraints are not unintentionally violated

Use Project's Task Plan Standards or Templates

Risk mitigation task plans are similar to the typical task plans developed within a project for managing large, complex tasks. It is a project decision as to the format and contents for risk mitigation task plans, but if there are project standards or templates for task plans, they should be used or adapted for risk mitigation task plans. The risk mitigation task plan needs enough detail to support management of the mitigation actions.

Recommended Contents

The table below provides a list of the key information that should be in a task plan.

Required Elements	Description
Risks	IDs and statements of risks being mitigated Context is optional if documented elsewhere.
Mitigation goals	Goals or objectives of this task plan
Success criteria (what defines successful completion of plan)	Indicators for reporting plan progress and success Ranges of acceptable results
Personnel assignments and responsibilities	Work breakdown structure Personnel availability (optional) Training requirements (if needed) Qualifications or skills required (optional)
Related risks	Related risks from a set and pointers to applicable mitigation plans for those related risks
Due dates and schedules	Detailed schedules and milestones, such as • PERT charts • Gantt charts Due date for completion of task plan is also required if it will take an extended length of time.
Strategy(ies)	Brief description of the chosen mitigation strategy(ies)
Specific actions to take	List of actions Interrelationship digraphs for action dependencies and predecessor relationships
Cost of strategy/actions	Cost model and budget estimates
Risk tracking requirements	Specific indicators to report current risk status along with • threshold conditions or ranges • data gathering mechanisms/tools • reporting frequency
Contingency strategy and triggers	Contingency strategy and actions, and triggers which would activate the contingency plans

Methods and Tools

The table below summarizes the methods and tools used to develop the information in the task plan. These are common methods and tools used during project planning. Consideration should be given those methods and tools already used in the project or familiar to project personnel.

Method or Tool	Description	When to Use
Gantt Charts [Chapter A-12]	Shows tasks, their duration, begin and end points, and other relevant information against a schedule	To show tasks, duration, start and end points
Goal-Question-Measure [Chapter A-13]	Identifies the indicators to track task plan progress and risks No specific method exists to determine other tracking requirements (e.g., reporting frequency, reporting format).	To set up risk and mitigation plan tracking
Interrelationship Digraph [Chapter A-14]	Graphic depiction of relationships between actions	To show dependencies between actions
PERT Charts [Chapter A-20]	Supports ranges, dependencies, and probabilities for completion in schedules	When the schedule has high degree of uncertainty
Planning Worksheet [Chapter A-22]	Worksheet to document information gathered	To document final decisions and selected contingency plans; a historical record of gathered information and unselected strategies
Work Breakdown Structure [Chapter A-40]	Describes the breakdown of major tasks into increasingly smaller tasks which can be tracked according to the resulting hierarchical structure	To decompose and allocate tasks

Section 7

Guidelines and Tips

General

Return to or repeat earlier activities as needed.

Methods for gathering data on risks can be used to gather data on strategies as well.

Innovative Thinking

Trust instincts and experience and don't forget to think "outside the box" for innovative solutions.

Don't ignore the impossible; impossible solutions can foster the generation of more realistic solutions.

References

Cited in this chapter:

[Kepner 81]

Kepner, Charles H. & Tregoe, Benjamin B. *The New Rational Manager.* Princeton, N.J.: Princeton Research Press, 1981.

[Lumsdaine 90]

Lumsdaine, Edward & Lumsdaine, Monika. *Creative Problem Solving.* New York: McGraw-Hill, 1990.

[Scholtes 88]

Scholtes, Peter R. *The Team Handbook: How to Use Teams to Improve Quality.* Madison, Wi.: Joiner Associates, 1988.

[Xerox 92]

Xerox Corporation and Carnegie Mellon University. *The University Challenge: Problem-Solving Process User Manual.* Stamford, Ct.: Xerox Corporation, 1992.

Chapter A-25

Project Profile Questions

Description

The project profile questions are used to tailor the **Taxonomy-Based Questionnaire (TBQ)** [Chapter A-32] to eliminate irrelevant questions.

- The answers to the project profile questions help the teams conducting interviews by giving them a better understanding of the project.
- If an outside facilitation team is being used to establish a baseline set of risks, then the project profile helps that team understand the project.
- These answers will also help eliminate unnecessary questions and allow the **TBQ Interviews** [Chapter A-33] to proceed smoothly and efficiently.

How to Use

Based on the answers to the profile questions, questions or sections of the taxonomy may be skipped. The TBQ includes "If...." phrases before specific sections of interview questions that may be skipped based on the profile answers.

Example:

The taxonomy class of *Product Engineering*, the *Design* element, includes a bolded phrase, **If COTS software is being used**, before question 29. If the answer to the profile question, "Are you using COTS software?" is that COTS software is not being used, questions 29 and 30 in the questionnaire may be skipped.

Project Profile Questions

The project profile questions are provided on the following pages.

Project Profile Questions

1. What are the normal work hours of the project (e.g., 8:00-5:00)?_____

2. What is your project's contractual role?

    Prime____   Subcontractor____   Integrator____   Other_____

3. What are the start and delivery dates for your project?

    Start_____   Delivery_____

4. What phases does the contract life cycle cover?
    - demonstration and validation   Yes____ No____
    - full-scale development   Yes____ No____
    - maintenance   Yes____ No____
    - other:

    _____

5. What is the current phase of your project?

    _____

6. Specifically, are you in or past the implementation phase of your project?

    Yes____ No____

7. Has your company implemented other systems of this application type?

    Yes____ No____

8. Has your company built other systems of this size?   Yes____ No____

9. How big is the software portion of your project?

    LOC_____   Number of CSCI's_____   Number of CSC's_____

10. Are there any requirements which require unprecedented or state-of-the-art technology to implement?
    - technologies   Yes____ No____
    - methods   Yes____ No____
    - languages   Yes____ No____

    Page 1 of 2

Project Profile Questions (cont.)

11. Are you using any reused, re-engineered software?   Yes___ No___

12. Are you using any COTS software?   Yes___ No___

13. Is any developmental hardware being used?   Yes___ No___

14. Are you doing any prototyping?   Yes___ No___

15. Are there distributed development sites?   Yes___ No___

16. Do you have any associate contractors?   Yes___ No___

17. Do you have any subcontractors?   Yes___ No___

18. Are there any security requirements allocated to software?   Yes___ No___

19. Are there any safety requirements allocated to software?   Yes___ No___

20. Are there multiple installation sites?   Yes___ No___

Page 2 of 2

Skipping Questions in the TBQ

The following table defines which answers to the project profile questions can permit questions in the TBQ to be skipped. No other answers to the profile have any effect on the TBQ—they only provide general data that may be useful to the interview team before the interviewing begins.

Caution: Make sure that the questions struck through on the interviewer's copy remains legible. In the course of an interview the team may learn that one or more of the questions was incorrectly eliminated. Legibility will permit immediate re-introduction.

For this profile question...	if the answer is...	strike through these TBQ questions
2. What is your project's contractual role?	NOT Subcontractor	[184] - [187]
6. Specifically, are you in or past the implementation phase of your project?	No	[76]
11. Are you using any reused, re-engineered software?	No	[28]
12. Are you using any COTS software?	No	[29] - [30], [55]
13. Is any developmental hardware being used?	No	[43] - [44]
14. Are you doing any prototyping?	No	[71.a.1] - [71.a.1a.3]
15. Are there distributed development sites?	No	[83]
16. Do you have any associate contractors?	No	[175] - [177]
17. Do you have any subcontractors?	No	[178] - [183]
18. Are any security requirements allocated to the software?	No	[68]-[70]
19. Are any safety requirements allocated to the software?	No	[66]-[67]
20. Are there multiple installation sites?	No	[132]

Chapter A-26

Risk Form

Description   The risk form is a one page form used to document new risks as they occur. These can then be submitted to the appropriate person or database for inclusion with the existing project risks. The form can include directions or they can be separate.

Note: Unless it is readily available elsewhere, the basis and structure for risk classification should appear on the back of the form. This form uses the Software Development Risk Taxonomy[1] as the basis for classification.

How to Use   Follow the procedure below to fill out the risk form. These instructions can also appear on the risk form itself (below the Classification field).

Step	Action
1	**Write a brief statement of risk.** Write the risk statement using the "condition; consequence" format for a risk statement. A simple statement of the conditions and consequence(s) of the risk will help to clearly define the risk and support effective action. *Example*: We have no experienced graphics programmers on the project; the graphics code may be late
2	**Write the context.** Write additional information that provides more details regarding the circumstances associated with the risk. *Note*: Use informal prose and address the who, what, when, where, and why as these relate to risk.
3	**Fill in the attribute information.** Evaluate the risk based on the evaluation criteria the project has selected (e.g., Binary Attribute Evaluation [Chapter A-6], Tri-level Attribute Evaluation [Chapter A-38]). The attributes are • *impact*: the loss or effect on the project if the risk occurs • *probability*: the likelihood the risk will occur • *timeframe*: the period when action is required in order to mitigate the risk
4	**Mark for immediate management attention, if required.** Check the box marked *Requires immediate management attention* if you feel a risk may be a showstopper or threatens failure of the project.
5	**(Optional) Describe recommended strategy.** If you have a recommendation for dealing with this risk, briefly describe it in the space provided.
6	**Fill in classification information.** Classify the risk using the basis and structure for classification the project has selected.

1. Carr, Marvin; Konda, Suresh; Monarch, Ira; Ulrich, Carol; & Walker, Clay. *Taxonomy Based Risk Identification* (CMU/SEI-93-TR-6, ADA266992). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

**Sample Risk
Form: Front**

The risk form, shown below, enables individuals to write down what they consider to be new risks or changes in known risks that the project faces.

Impact		**Risk Form**	**ID#**_____
	Probability		(for internal use only)
		Timeframe	**Date:**_____
			Statement of risk (with context)

Requires immediate management attention

Recommendation for dealing with the risk (optional):

Classification:

Sample Risk Form: Back

The back of the risk form, shown below, has the Software Development Risk Taxonomy to aid in classifying the risks.

Note: The back of the form should show the classification structure and basis the project has selected.

Taxonomy of Software Development Risks

Class ➤ **A. Product Engineering**
  1. Requirements
      a. Stability
      b. Completeness
      c. Clarity
      d. Validity
      e. Feasibility
      f. Precedent
      g. Scale

Element ➤ 2. Design
      a. Functionality
      b. Difficulty
      c. Interfaces
      d. Performance
      e. Testability
      f. Hardware Constraints

Attribute ➤ g. Non-Developmental Software
  3. Code and Unit Test
      a. Feasibility
      b. Testing
      c. Coding/Imple-mentation
  4. Integration and Test
      a. Environment
      b. Product
      c. System
  5. Engineering Specialties
      a. Maintainability
      b. Reliability
      c. Safety
      d. Security
      e. Human Factors
      f. Specifications

B. Development Environment
  1. Development Process
      a. Formality
      b. Suitability
      c. Process Control
      d. Familiarity
      e. Product Control
  2. Development System
      a. Capacity
      b. Suitability
      c. Usability
      d. Familiarity
      e. Reliability
      f. System Support
      g. Deliverability
  3. Management Process
      a. Planning
      b. Project Organization
      c. Management Experience
      d. Program Interfaces
  4. Management Methods
      a. Monitoring
      b. Personnel Management
      c. Quality Assurance
      d. Configuration Management
  5. Work Environment
      a. Quality Attitude
      b. Cooperation
      c. Communication
      d. Morale

C. Program Constraints
  1. Resources
      a. Schedule
      b. Staff
      c. Budget
      d. Facilities
  2. Contract
      a. Type of Contract
      b. Restrictions
      c. Dependencies
  3. Program Interfaces
      a. Customer
      b. Associate Contractors
      c. Subcontractors
      d. Prime Contractor
      e. Corporate Management
      f. Vendors
      g. Politics

Classification basis: Classify the risks based on the source or root cause.

Example   An example of a completed risk form is shown below.

Impact			Risk Form	ID#_____
	Probability			(for internal use only)
		Timeframe		Date:___*4/5/96*___
H	H	N	**Statement of risk (with context)**	

The GUI must be coded using X Windows and we do not have expertise in X; the GUI code may not be completed on time and may be inefficient.

Context: The graphical user interface is an important part of the system and we do not have anyone trained in the X Window System. We all have been studying the language but it is complex and only one person in the group has any graphics experience and that is with Windows on the PC.

✓	**Requires immediate management attention**

Recommendation for dealing with the risk (optional):

Identify an expert in X to work with the team and begin a formal training project for the staff assigned to the GUI.

Classification:

          Program Constraints, Resources, Staff (Risk Taxonomy)

Chapter A-27

Risk Information Sheet

Description

The risk information sheet is a means of documenting information about a risk, much as a software trouble or problem report documents a problem in software. Information is added to the sheet or modified as it is acquired or developed. For paper-based risk management systems, the risk information sheet serves as the primary means for documenting and retaining information about a risk. With a database, the risk information sheet could be the report generated for a single risk. A database would also make it easier to keep information such as the risk context and priority current.

Note: The risk information sheet on the following page is an example of what one could look like, and the types of information that would be kept. Adaptation to suit a specific project or organization would generally be required.

How to Use

The fields on the risk information sheet are completed as information is gathered about the risk. For example, during the **Identify** [Chapter 4] function, a risk identifier, the statement, and context are added to the sheet. Eventually, when the risk is closed, the last fields (i.e., closure signature, closing date, and closing rationale) are completed.

Template

A risk information sheet template is shown on the next page.

ID	Risk Information Sheet		Identified: __/__/__
Priority	**Statement**		
Probability			
Impact			
Timeframe	**Origin**	**Class**	**Assigned to:** _____

Context

Mitigation strategy

Contingency plan and trigger

Status   **Status date**

Approval	Closing date	Closing rationale
_____	__/__/__	

**Field
Descriptions**

This table describes the fields in the risk information sheet.

Field Name	Description
ID	Unique identifier for the risk
Identified	Date when the risk was identified
Statement	Statement of the risk
Context	Associated information that clarifies the risk. Context is usually gathered at the time of identification
Origin	Organization or person who identified the risk (organization is used if the risk was transferred)
Priority	Priority ranking of the risk
Probability	Likelihood of occurrence—exact value depends on type of analysis
Impact	Degree of impact—exact value depends on type of analysis
Timeframe	Timeframe in which the risk will occur or action is needed
Class	Classification of the risk (could be more than one value)
Assigned to	Who is responsible for mitigating the risk
Mitigation strategy	The selected strategy for mitigating the risk
Contingency plan and trigger	A contingency plan, if one exists, and the event or time that triggers it, should the mitigation strategy fail
Status/status date	Running status that provides a history of what is being done for the risk and changes in the risk
Approval	Approval for mitigation strategies or closure. For transferred risks, this may require the transferrer's signature
Closing date	Date when the risk was closed
Closing rationale	Rationale for closure of the risk, e.g., probability is zero

Example

An example of a completed risk information sheet is shown on the next page. The status field contains a running status with the most recent status first.

ID ABC 23	Risk Information Sheet	Identified: 3 / 2 / 95

Priority 6	**Statement**
Probability High	With our lack of experience in X Windows software, we may not be able to complete the GUI code on time and it may not be the quality
Impact High	of code we need.

Timeframe Near	**Origin** G. Smith	**Class** Personnel experience	**Assigned to:** S. Jones

Context

The graphical user interface is an important part of the system and we do not have anyone trained in the X Window system. We all have been studying it, but is complex and only one person in the group has any graphics/user interface experience and that was with a completely different type of system and interface requirements. There are other personnel within the company who have relevant experience and training, but they may not be available in time to support this project.

Mitigation strategy

1. Update coding estimates and schedules to reflect the need for increased training and for hiring an expert in X Windows (changes due 5/1/95).
2. Coordinate with customer and get approval for changing schedule (approve by 6/1/95).
3. Identify an available expert from other projects in this division (hired by 6/15/95).
4. Bring in outside training source for current programmers (training complete by 7/30/95).

Contingency plan and trigger

Plan: Subcontract GUI development to LMN Corp. and accept the increase in our cost, $25,000. LMN has a level of effort contract with ABC Headquarters and can support with 1 week notice.

Trigger: if internal expert is not onboard and training not completed by 7/30/95

Status	Status date
GUI code delivered on time, required quality	1/30/96
GUI code has been delivered for testing on schedule	11/13/95
Code 50% complete and 1 week ahead of schedule	9/15/95
Personnel completed 2 week training; will monitor progress and quality of work	7/15/95
Brown from project XYZ will be available on 6/5/95 to provide quality assurance, mentoring, and critical path programs	6/1/95
Customer approved revised schedule milestones	5/3/95
Revised estimates and schedule complete; indicates a worst-case 3 week slip if we get the additional expert	4/23/95

Approval	Closing date	Closing rationale
J.Q. Jones, ABC Project Manager	2 / 15 / 96	Code delivered on time, Acceptance test excellent. Risk is gone.

Chapter A-28

Risk Management Plan

Description

The risk management plan documents how risks will be managed on the project: the processes, activities, milestones, and responsibilities associated with risk management. Ideally, it is a subset or companion piece to the project management plan and is written before the project begins. The contents of a risk management plan can also be integrated with the project management plan; however, the recommended contents for a risk management plan, as defined here, are written as a stand-alone plan for clarity and understanding.

How to Use

This is a suggested content for a risk management plan. The plan should be adjusted to suit the particular processes, methods, and tools used by the project organization. The material can be integrated into a project management plan in the appropriate places or be used as a lower level plan.

When building the risk management plan for the project, start with this list and tailor and expand as needed. This is the minimal, recommended content.

Every project should have a risk management plan. The degree of formality is dictated by the organization's standard processes and project management requirements.

Example Risk Management Plan Contents

The major parts of a risk management plan are
• introduction
• overview of processes
• organization
• process details
• resources and schedule
• documentation of risks

Note: The current list of risks and mitigation plans are sometimes included in the risk management plan. If Continuous Risk Management is done effectively, then this could create a burdensome revision cycle for the risk management plan. It is recommended that risks and their mitigation plans be maintained and updated separately from the risk management plan.

The following tables provide detailed explanations and content descriptions for each of the components of a risk management plan.

Introduction

This part of the plan is a general introduction to the plan and why it exists.

Component	Description
Purpose and scope	Defines the purpose, scope, and overall contents of this plan (e.g., Is this for software risk management or system risk management?)
Assumptions, constraints, and policies	Lists any assumptions made and applicable constraints and policies for implementing the processes (e.g., customer-imposed risk analysis method, required joint customer-supplier risk database, or corporate limits for mitigation resources)
Related documents and standards	Lists the related plans, documents, and standards—includes description of relationship or dependencies as needed

Overview of Processes

This provides an overview of the processes and how they relate to project management.

Component	Description
Overview	Describes all of the activities and how they are related
Flows	Provides process flows and data flows
Project management integration	Describes how the activities integrate with other project management activities (not needed if this plan's content are integrated with the rest of the project plan)

Organization

This part of the plan describes the organization's involvement in carrying out risk management activities.

Component	Description
Project organization and responsibilities	Includes project organization description and chart Maps risk management activities to project roles Lists risk management responsibilities associated with each project role
Customer responsibilities	Lists the responsibilities or expected activities/products from the customer as related to risk management (e.g., Do you expect the customer to report the top N risks they see?)
Supplier responsibilities	Lists the responsibilities or expected activities/products from the supplier as related to risk management (e.g., Do you expect the supplier to report the top N risks they see? their mitigation plans and status?)

Component	Description
Co-developer responsibilities	Lists the responsibilities or expected activities/products from the co-developers as related to risk management (e.g., Do you expect the co-developer to report the top N risks they see? their mitigation plans and status? to coordinate mutual risks?)

Process Details

This provides the details of each major activity in risk management and how it is to be accomplished. It also documents how the processes are to be measured and improved.

Component	Description
Define the processes for the following functions: • Establish a baseline • Identify • Analyze • Plan • Track • Control • Communicate	Describes the processes and required procedures Describes methods to implement the function; specifies the criteria for selection of one method over the other, if alternatives are permitted Describes tools to support the function and its methods; specifies the criteria for selection of one tool over the other, if alternatives are permitted References other plans, handbooks, training materials, etc., for those methods and tools that are documented elsewhere in project's, organization's, or customer's materials *Note*: includes both internal communication within the project and external communication with customers, suppliers, senior management, etc.
Process improvement	Identifies measures or indicators to be collected and reported along with other project management measures (e.g., number of risks opened, their classification, trends in risk processing time from identification to closure, number of successful mitigations vs. number of failed mitigations, etc.) Describes process to be followed for evaluation and improvement of the risk management processes for this project (e.g., quarterly evaluation of methods for efficiency, periodic review of reports to customers for usefulness)

Resources and Schedule

This identifies the schedule and milestones for when risk management activities are carried out and the required resources.

Component	Description
Resources for risk management activities and for risk mitigation	Identifies resources (cost, staff effort, equipment, software) for the activities of risk management (Identify, Analyze, etc.)
	Defines allocated budget and source of mitigation funds (e.g., Does each team or functional group have a specific percentage of their total funds allocated for mitigation or does the project have a single funding pool that must be allocated over the lifetime of the project?)
Project schedule and risk management activities	Maps of risk management activities against the project schedule and milestones. This includes when the baseline is established (and re-established), major reviews of risk status, routine activities, and notes for continuous activities. For example, if risk identification can occur at any time, note it; if it is to be done at regularly scheduled intervals, mark those on the schedule.
Risk management-related deliverables and receivables	Identifies and describes all major risk-related deliverables to customers and from suppliers and co-developers, such as risk summary reports, baseline results, top N mitigation plans, etc.

Documentation of Risks

Describes how risk information is documented, retained, controlled and used.

Component	Description
Database requirements	Defines database tool specifications
	Defines access, control, and management of database
Templates	Includes or references any templates that are to be used (e.g., a risk information sheet)
Data management	Provides procedures and requirements for completing, processing, controlling, and retaining risk-related documents and forms

When Risk Management Is Part of the Proposal Process

Risk management may also be part of the request for proposals (RFPs) or a supplier's proposal. RFPs may specify the major risks to the project and request submission of proposed mitigation strategies [Air Force 95] based on the customer's performance of **Baseline Identification and Analysis** [Chapter A-4]. **Baseline Planning** [Chapter A-5] can be done by potential suppliers to address those risks. While the supplier's performance of baseline identification and analysis is not required, it could provide significantly useful results and risks not foreseen by the customer.

If risk management is included in the proposal, baseline identification and analysis and baseline planning should be performed, and the results included in the proposed risk management plan as an appendix. The following table describes what to add to the risk management plan (and proposal) to address the baseline results.

Component	Description
Top N risks and risk information and analysis	Describes the top N risks to the project, including their probability, impact, timeframe, and priority. Includes context as needed to fully explain the risks
For each top N risk	Lists strategies and, optionally, actions Documents schedules and required resources Identifies tracking measures and success criteria (Optional) Describes contingency plans and triggers
Integrated strategy	Describes the overall, integrated strategy and high level actions for the top N risks
Integrated schedule and resources	Documents the integrated schedule for accomplishing mitigation of the top N risks

References

Cited in this chapter:

[Air Force 95]   Department of the Air Force, Software Technology Support Center. *Guidelines for Successful Acquisition and Management of Software Intensive Systems: Weapon Systems, Command and Control Systems, Management Information Systems* Volume 1, Version 1.1. Salt Lake City, Utah: Department of the Air Force, Software Technology Support Center, 1995.

For more information on risk management plans, see the following:

[Boehm 89]   Boehm, Barry. *IEEE Tutorial on Software Risk Management.* New York: IEEE Computer Society Press, 1989.

[Charette 89]   Charette, Robert N. *Software Engineering Risk Analysis and Management.* New York: McGraw-Hill, 1989.

Chapter A-29

Short Taxonomy-Based Questionnaire (Short TBQ)

Description   The short taxonomy-based questionnaire (short TBQ) provides a summary of the Software Development Risk Taxonomy and questions in the **Taxonomy-Based Questionnaire** [Chapter A-32].

How to Use   The short TBQ can be used for risk identification and analysis—for example, identifying risks in meetings, in one-on-one interviews, or as a memory jogger or trigger at any time.

Short TBQ   The short TBQ is shown on the following pages.

A Short Taxonomy-Based Questionnaire

Product Engineering

Think about risks to the project that may arise from the nature of the product that you are trying to develop...

A.1	Requirements	Are there risks that may arise from requirements being placed on the product? Examples: stability; completeness; clarity; validity; feasibility; precedent; scale.
A.2	Design	Are there risks that may arise from the design the project has chosen to meet its requirements? Examples: functionality; difficulty; interfaces; performance; testability; hardware constraints; non-developmental software.
A.3	Code and Unit Test (Manufacturability)	Are there risks that may arise from the way the project is choosing to subdivide the design and construct the pieces? Examples: feasibility; testing; coding/implementation.
A.4	Integration and Test	Are there risks that may arise from the way the project is choosing to bring the pieces together and prove that they work as a whole? Examples: the hardware and software support facilities; integration of the parts of the product; integration with the larger system
A.5	Engineering Specialties	Are there risks that may arise from special attributes of the product, such as maintainability, reliability, safety, security, human factors, etc.?
A.99	(Other)	Are there other risks that may arise from the product itself, but are not covered by the above categories?

Development Environment

Think about risks to the project that may arise from the way you are going about developing the product...

B.1	Development Process	Are there risks that may arise from the process the project has chosen to develop the product? Examples: formality; suitability; process control; familiarity; product control.
B.2	Development System	Are there risks that may arise from the hardware and software tools the project has chosen for controlling and facilitating its development process? Examples: capacity; suitability; usability; familiarity; reliability; system support; deliverability.
B.3	Management Process	Are there risks that may arise from the way the project budget or schedule is planned, monitored, or controlled, management experience, the project's organization structure, or its handling of internal and external organization interfaces?
B.4	Management Methods	Are there risks that may arise from the way the development or program personnel are managed, in areas such as status monitoring, personnel management, quality assurance, or configuration management?
B.5	Work Environment	Are there risks that may arise from the general environment in which the project is found, such as quality attitude, cooperation, communication, or morale?

B.99   (Other)   Are there other risks that may arise from the way the project is going about its development, but not covered by the above categories?

Program Constraints

Think about risks to the project that may arise from sources outside the project's control...

C.1	Resources	Are there risks that may arise from resources the project needs but that are outside its control to obtain or maintain? Examples: schedule; staff; budget; facilities.
C.2	Contract	Are there risks that may arise from the [already legally binding] contract? Example areas include the contract's type, restrictions, or dependencies.
C.3	Program Interfaces	Are there risks that may arise from outside interfaces which the project cannot reasonably expect to control? Examples: customer; associate contractors; subcontractors; prime contractor; corporate management; vendors; politics.
C.99	(Other)	Are there other risks that may arise from factors outside project control, but not covered by the above categories?

Chapter A-30

Spreadsheet Risk Tracking

Risk Spreadsheet						
ID	Priority	Statement	Status	P	I	Assign

Section

Section 1

Spreadsheet Risk Tracking Description

Introduction

Spreadsheet risk tracking is a method which monitors project risks by summarizing and periodically reviewing their statuses. The data for this method are documented in a spreadsheet format. The basic process involves a periodic (e.g., weekly or monthly) update and review of the risks. The review is generally held in conjunction with a regularly scheduled project status meeting. Spreadsheet risk tracking reports are normally included as read-ahead material for project meetings where they are reviewed and updated as appropriate.

Diagram

The following diagram shows the input and output for spreadsheet risk tracking.
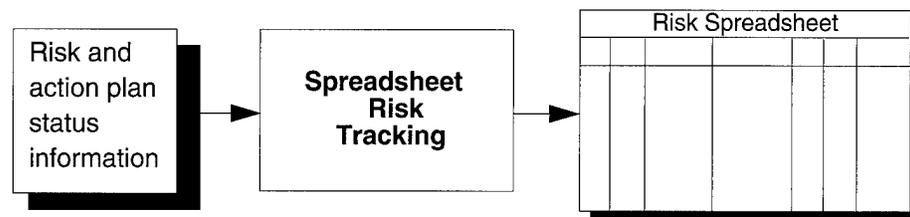
Personnel Requirements

The project manager, other managers, and selected project personnel (such as quality assurance) participate in the use of this method. Input for the spreadsheet may also be collected from project personnel not directly involved in the review and discussion of the spreadsheet. The spreadsheet is maintained and updated by one member of the project, and all updates and changes are provided to that person.

Section 2

When to Use

When to Use

When a concise set of risk and status information is needed in a format that is easy to read and comprehend. This is normally in support of routine project meetings where risks are being reviewed and discussed.

Constraints

This method does not provide detailed status information and might not be sufficient for new personnel unfamiliar with the risks. Individual risk status reports, **Risk Information Sheets** [Chapter A-27], or a detailed chronicle of updates [Section 4] may be required to convey detailed information.

The information must be kept up-to-date and meaningful or the spreadsheet will lose its effectiveness.

Benefits

This method provides a large amount of risk information in a concise format that is easy for project personnel to read.

Successive versions of the spreadsheet provide a history of the changes in risks across time (e.g., as they move up and down in priority).

Section 3

Using Spreadsheet Risk Tracking

Procedure

The following table describes the procedure for spreadsheet risk tracking.

Step	Action
1	**Create an initial version of the spreadsheet.** This is only required for the first review.
2	**Circulate copies of the current spreadsheet.** Prior to the review session, each individual involved with the risk-tracking process reviews the spreadsheet.
3	**Update risk information.** Each person responsible for a risk then • updates the status of the risk (e.g., changes in probability or impact for the risk). Only updates are noted. • notes any condition that may affect the risk. Only changes in the risk's conditions are noted. • records a recommendation considering or reconsidering the approach being taken for the risk (e.g., accept, watch, mitigate, or close). This is based on whether there has been a significant change in the risk's impact, probability, etc., or whether there have been other significant changes in the project. *Note*: An individual may be responsible for more than one risk. This step must be performed for each of those risks.
4	**Conduct a review session.** A review session is normally held as part of a regular, scheduled project meeting. The review consists of the following actions: • *review*: The spreadsheet is reviewed sequentially, and each risk is considered separately. • *discuss and decide*: Each risk is discussed. The focus is on changes and updates since the last review. The discussion results in a decision on what control decisions will be made (e.g., change the mitigation plan, continue watching, change the risk's priority, etc.) • *assign*: Action items are assigned as needed.
5	**Update the spreadsheet.** The spreadsheet, chronicle of updates, database, master list of risks, etc., are updated after the review session if this action wasn't completed during the session (e.g., if this is electronically maintained).

Section 4

The Risk Tracking Spreadsheet

Description

The risk tracking spreadsheet is a listing of the risks and related risk information and is presented in a spreadsheet format.

Example Spreadsheet

An example spreadsheet is shown below. This example provides an overview of the key measures for the risks. In this case, the risks are ranked from highest to lowest priorities, and a field for status comments on each risk is also included.

Risk Spreadsheet						**6/10/94**
Risk ID	**Prior-ity**	**Risk Statement**	**Status Comments**	**Proba-bility**	**Impact**	**Assigned To**
12	1	No simulation; may not meet performance	Latest simulation results indicate we will miss required performance by 25%.	high	high	Jones, L.
5	2	Inadequate test time scheduled	No change, working to secure more time at test facility	high	high	Block, R.
19	3	Lack of C++ expertise; may not make first build	Mitigation plan is 50% complete. The probability has been decreased by 90%.	low	medium	Smith, F.

Spreadsheet Content

The following table describes the typical content included in a risk spreadsheet.

Field Name	**Description**
Risk ID	Unique identifier for each risk
Priority	Ranking of the risk
Risk Statements	Statement of the risk
Status Comments	Current status and actions
Probability	Likelihood of occurrence (could be qualitative or quantitative)
Impact	Impact if the risk occurs (could be qualitative or quantitative)
Assigned To	The person responsible for the risk

Spreadsheet Variations

The exact format of and the data included in the spreadsheet can vary depending upon an organization's needs. During a management review, the focus of the meeting is normally different than that of a technical review. There might be separate formats for the spreadsheet based on the focuses of the required reviews. See the **Stoplight Chart** [Chapter A-31] for one specific variation.

Chronicle of Updates

A chronicle of updates is a summary of the changes made to the spreadsheet. Often this summary is in the form of meeting minutes. The most recent version of the spreadsheet can be included with the chronicle of updates, if desired. The list of updates is structured by the date of the review, starting with the most recent review. A chronicle of updates can provide useful trending information on the frequency of priority changes, on historical data documenting decision rationale, etc.

Example Chronicle of Updates

An example chronicle of updates is shown below. Chronicles can be fairly simple, with only changes in risk attributes noted, or more extensive, documenting rationale.

Date	Actions
8/1/94	Risk 13 was closed. It has now become a problem, see Problem Report #35.
	Risk 11 was moved to priority 4 after the performance improvements reduced the impact from high to medium.
7/27/94	Risk 8's probability was increased to high based on industry reports of ABC Company heading for bankruptcy.
	Risk 14 was closed; it has been overtaken by events.
7/20/94	Risk 7's probability was lowered to medium after preliminary tests on the upgraded CPU indicate improved timing.
	Risk 15 was added as a new risk.
...	... etc.

Section 5

Guidelines and Tips

Supporting Routine Project Updates

Spreadsheets can be effectively included as part of routine project updates that are received by project personnel and can also be included with other types of risk reports as supporting material.

Project Database

Establishing and using a project database to electronically store and maintain risk data can be useful. When desired, a paper copy of the risk spreadsheet could be automatically generated from the database or the data could be reviewed on-line by project personnel. A database of risk information can save time and reduce the possibility of error.

Current Status

Avoid the temptation to oversimplify the current status. If additional information needs to be recorded to ensure that everyone remembers what is happening, add it to the meeting minutes or to the chronicle of updates.

Variations

Spreadsheets can also contain specific mitigation information, such as the latest action accomplished and the next pending action or milestone.

Spreadsheets should be adapted to a project's needs. They should contain enough information to help personnel make informed decisions but should also be concise and easy to read.

Chapter A-31

Stoplight Chart

Description

Stoplight charts provide a means of communicating the status of risk mitigation actions. They indicate to the decision maker how well the current plans are doing and whether or not management action is required.

While stoplight charts do not generally have sufficient detail to explain why a plan may be off-track, they provide the decision maker with a big picture of how all plans are doing, and a way to inquire about specific plans, if necessary.

How to Use

Use of a stoplight chart is simple. Each mitigation plan is assigned one of three conditions at any given point in time:
- *green*—indicates that the plan is working as intended and that no management action is required
- *yellow*—indicates that the plan is not working as intended and that while no management action is required at this point, future action may be required if the situation persists
- *red*—indicates that the plan is not working and that management action will be required to bring the situation under control

The frequency with which stoplight charts are used should be agreed to by the decision maker and those executing the mitigation activities.

Note: It is often recommended that a stoplight chart include the prior period's condition to denote if there has been a change since the last reporting period.

Color Definitions

The definition of red, yellow, and green should be defined at the start. The above definitions refer to how well the mitigation plan is working. An alternate definition might focus on the impact to the project. The key is to agree on a definition so that all parties understand what they are reporting.

Note: Blue or white can be used to indicate new risks which have not yet been taken through the planning process (and, therefore, there is no valid indication of how a mitigation plan is progressing).

Example Stoplight Chart

The stoplight chart information can be added to any risk management status tracking chart. The form on the following page is one example of how stoplight information is used.

Stoplight Chart

Condition	Risk ID	Risk Statement	Assigned To:	Action Plan	Key Milestones	Comments
RED	23	Test case development is past due and the variability in the level of detail of low level requirements may result in testability problems and rework.	S. Smith	Re-evaluate the test schedules in light of current resources	Test case development completed by 9/15	Test case development will not be completed when expected Previously: Yellow
YELLOW	34	Training in tools and processes has not kept up with needs. It's taking longer to proceed due to the learning curve.	G. Samms	Institute weekly process training sessions with the software team Institute daily software project reviews to identify immediate issues and assign mentors	50% of staff through training by 8/14 75% of staff through training by 9/1 100% of staff through training by 9/15	Weekly training sessions and mentor assignments are helping but demand is still more than we can accommodate Previously: Red
GREEN	41	No system simulation was done; we may not meet the performance requirements	G. Samms	Conduct simulation	Simulation completed by 8/1	Early performance tests meet average 2 second response time Previously: Green
• • •						

Chapter A-32

Taxonomy-Based Questionnaire (TBQ)

Description   The taxonomy-based questionnaire (TBQ) consists of questions, along with specific cues and follow-up probe questions, under each attribute in the Software Development Risk Taxonomy.

Taxonomy of Software Development Risks

Class → **A. Product Engineering**

1. Requirements
    a. Stability
    b. Completeness
    c. Clarity
    d. Validity
    e. Feasibility
    f. Precedent
    g. Scale

Element → 2. Design
    a. Functionality
    b. Difficulty
    c. Interfaces
    d. Performance
    e. Testability
    f. Hardware Constraints

Attribute → g. Non-Developmental Software

3. Code and Unit Test
    a. Feasibility
    b. Testing
    c. Coding/Implementation

4. Integration and Test
    a. Environment
    b. Product
    c. System

5. Engineering Specialties
    a. Maintainability
    b. Reliability
    c. Safety
    d. Security
    e. Human Factors
    f. Specifications

B. Development Environment

1. Development Process
    a. Formality
    b. Suitability
    c. Process Control
    d. Familiarity
    e. Product Control

2. Development System
    a. Capacity
    b. Suitability
    c. Usability
    d. Familiarity
    e. Reliability
    f. System Support
    g. Deliverability

3. Management Process
    a. Planning
    b. Project Organization
    c. Management Experience
    d. Program Interfaces

4. Management Methods
    a. Monitoring
    b. Personnel Management
    c. Quality Assurance
    d. Configuration Management

5. Work Environment
    a. Quality Attitude
    b. Cooperation
    c. Communication
    d. Morale

C. Program Constraints

1. Resources
    a. Schedule
    b. Staff
    c. Budget
    d. Facilities

2. Contract
    a. Type of Contract
    b. Restrictions
    c. Dependencies

3. Program Interfaces
    a. Customer
    b. Associate Contractors
    c. Subcontractors
    d. Prime Contractor
    e. Corporate Management
    f. Vendors
    g. Politics

How to Use

Because the TBQ is comprehensive, it contains questions that may not be relevant for all stages of a software development life cycle, for specific software domains, or for specific project organizations. Typically, the questionnaire is tailored to a particular project and its stage in the development life cycle by deleting questions not relevant to it. This can be accomplished by using the **Project Profile Questions** [Chapter A-25].

The TBQ is generally used during a 2.5 hour interview session with project participants which is facilitated by people external to the project, such as described in **TBQ Interviews** [Chapter A-33]. The general steps include:
- Ask a TBQ question.
- Ask follow-up question(s), as needed.
- Pursue risk, as needed.
- Capture and record the risk statement and context information, as needed.

Taxonomy-Based Questionnaire

The following pages contain a reprint of the taxonomy-based questionnaire, taken from the following technical report:

Carr, Marvin; Konda, Suresh; Monarch, Ira; Ulrich, Carol; & Walker, Clay. *Taxonomy-Based Risk Identification* (CMU/SEI-93-TR-6, ADA266992). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

Note: The report also contains descriptions of each class, element, and attribute.

A. Product Engineering

1. Requirements

a. Stability
[Are requirements changing even as the product is being produced?]

[1] Are the requirements stable?

    (No)   (1.a)   What is the effect on the system?

- *Quality*
- *Functionality*
- *Schedule*
- *Integration*
- *Design*
- *Testing*

[2] Are the external interfaces changing?

b. Completeness
[Are requirements missing or incompletely specified?]

[3] Are there any TBDs in the specifications?

[4] Are there requirements you know should be in the specification but aren't?

    (Yes)   (4.a)   Will you be able to get these requirements into the system?

[5] Does the customer have unwritten requirements/expectations?

    (Yes)   (5.a)   Is there a way to capture these requirements?

[6] Are the external interfaces completely defined?

c. Clarity
[Are requirements unclear or in need of interpretation?]

[7] Are you able to understand the requirements as written?

    (No)   (7.a)   Are the ambiguities being resolved satisfactorily?

    (Yes)   (7.b)   There are no ambiguities or problems of interpretation?

d. Validity
[Will the requirements lead to the product the customer has in mind?]

[8] Are there any requirements that may not specify what the customer really wants?

    (Yes)   (8.a)   How are you resolving this?

[9] Do you and the customer understand the same thing by the requirements?

    (Yes)   (9.a)   Is there a process by which to determine this?

[10] How do you validate the requirements?

- Prototyping
- Analysis
- Simulations

e. Feasibility
[Are requirements infeasible from an analytical point of view?]

[11] Are there any requirements that are technically difficult to implement?

(Yes) (11.a) What are they?

(Yes) (11.b) Why are they difficult to implement?

(No) (11.c) Were feasibility studies done for these requirements?

(Yes) (11.c.1) How confident are you of the assumptions made in the studies?

f. Precedent
[Do requirements specify something never done before, or that your company has not done before?]

[12] Are there any state-of-the-art requirements?
- Technologies
- Methods
- Languages
- Hardware

(No) (12.a) Are any of these new to you?

(Yes) (12.b) Does the program have sufficient knowledge in these areas?

(No) (12.b.1) Is there a plan for acquiring knowledge in these areas?

g. Scale
[Do requirements specify a product larger, more complex, or requiring a larger organization than in the experience of the company?]

[13] Is the system size and complexity a concern?

(No) (13.a) Have you done something of this size and complexity before?

[14] Does the size require a larger organization than usual for your company?

2. Design

a. Functionality
[Are there any potential problems in meeting functionality requirements?]

[15] Are there any specified algorithms that may not satisfy the requirements?

(No) (15.a) Are any of the algorithms or designs marginal with respect to meeting requirements?

[16] How do you determine the feasibility of algorithms and designs?
- Prototyping
- Modeling

- Analysis
- Simulation

b. Difficulty
[Will the design and/or implementation be difficult to achieve?]

[17] Does any of the design depend on unrealistic or optimistic assumptions?

[18] Are there any requirements or functions that are difficult to design?

(No) (18.a) Do you have solutions for all the requirements?

(Yes) (18.b) What are the requirements?

- Why are they difficult?

c. Interfaces
[Are the internal interfaces (hardware and software) well defined and controlled?]

[19] Are the internal interfaces well defined?
- Software-to-software
- Software-to-hardware

[20] Is there a process for defining internal interfaces?

(Yes) (20.a) Is there a change control process for internal interfaces?

[21] Is hardware being developed in parallel with software?

(Yes) (21.a) Are the hardware specifications changing?

(Yes) (21.b) Have all the interfaces to software been defined?

(Yes) (21.c) Will there be engineering design models that can be used to test the software?

d. Performance
[Are there stringent response time or throughput requirements?]

[22] Are there any problems with performance?
- Throughput
- Scheduling asynchronous real-time events
- Real-time response
- Recovery timelines
- Response time
- Database response, contention, or access

[23] Has a performance analysis been done?

(Yes) (23.a) What is your level of confidence in the performance analysis?

(Yes) (23.b) Do you have a model to track performance through design and implementation?

e. Testability
    [Is the product difficult or impossible to test?]

[24] Is the software going to be easy to test?

[25] Does the design include features to aid testing?

[26] Do the testers get involved in analyzing requirements?

f. Hardware Constraints
    [Are there tight constraints on the target hardware?]

[27] Does the hardware limit your ability to meet any requirements?
- Architecture
- Memory capacity
- Throughput
- Real-time response
- Response time
- Recovery timelines
- Database performance
- Functionality
- Reliability
- Availability

g. Non-Developmental Software
    [Are there problems with software used in the program but not developed by the program?]

If re-used or re-engineered software exists

[28] Are you reusing or re-engineering software not developed on the program?
      (Yes) (28.a) Do you foresee any problems?
- Documentation
- Performance
- Functionality
- Timely delivery
- Customization

If COTS software is being used

[29] Are there any problems with using COTS (commercial off-the-shelf) software?
- Insufficient documentation to determine interfaces, size, or performance
- Poor performance
- Requires a large share of memory or database storage
- Difficult to interface with application software
- Not thoroughly tested
- Not bug free
- Not maintained adequately
- Slow vendor response

[30] Do you foresee any problem with integrating COTS software updates or revisions?

3. Code and Unit Test

a. Feasibility
[Is the implementation of the design difficult or impossible?]

[31] Are any parts of the product implementation not completely defined by the design specification?

[32] Are the selected algorithms and designs easy to implement?

b. Testing
[Are the specified level and time for unit testing adequate?]

[33] Do you begin unit testing before you verify code with respect to the design?

[34] Has sufficient unit testing been specified?

[35] Is there sufficient time to perform all the unit testing you think should be done?

[36] Will compromises be made regarding unit testing if there are schedule problems?

c. Coding/Implementation
[Are there any problems with coding and implementation?]

[37] Are the design specifications in sufficient detail to write the code?

[38] Is the design changing while coding is being done?

[39] Are there system constraints that make the code difficult to write?
- Timing
- Memory
- External storage

[40] Is the language suitable for producing the software on this program?

[41] Are there multiple languages used on the program?

(Yes) (41.a) Is there interface compatibility between the code produced by the different compilers?

[42] Is the development computer the same as the target computer?

(No) (42.a) Are there compiler differences between the two?

If developmental hardware is being used

[43] Are the hardware specifications adequate to code the software?

[44] Are the hardware specifications changing while the code is being written?

4. Integration and Test

a. Environment
    [Is the integration and test environment adequate?]

[45] Will there be sufficient hardware to do adequate integration and testing?

[46] Is there any problem with developing realistic scenarios and test data to demonstrate any requirements?
- Specified data traffic
- Real-time response
- Asynchronous event handling
- Multi-user interaction

[47] Are you able to verify performance in your facility?

[48] Does hardware and software instrumentation facilitate testing?

(Yes) (48.a) Is it sufficient for all testing?

b. Product
    [Is the interface definition inadequate, facilities inadequate, time insufficient?]

[49] Will the target hardware be available when needed?

[50] Have acceptance criteria been agreed to for all requirements?

(Yes) (50.a) Is there a formal agreement?

[51] Are the external interfaces defined, documented, and baselined?

[52] Are there any requirements that will be difficult to test?

[53] Has sufficient product integration been specified?

[54] Has adequate time been allocated for product integration and test?

If COTS

[55] Will vendor data be accepted in verification of requirements allocated to COTS products?

(Yes) (55.a) Is the contract clear on that?

c. <u>System</u>
[System integration uncoordinated, poor interface definition, or inadequate facilities?]

[56] Has sufficient system integration been specified?

[57] Has adequate time been allocated for system integration and test?

[58] Are all contractors part of the integration team?

[59] Will the product be integrated into an existing system?

(Yes) (59.a) Is there a parallel cutover period with the existing system?

(No) (59.a.1) How will you guarantee the product will work correctly when integrated?

[60] Will system integration occur on customer site?

5. Engineering Specialties

a. <u>Maintainability</u>
[Will the implementation be difficult to understand or maintain?]

[61] Does the architecture, design, or code create any maintenance difficulties?

[62] Are the maintenance people involved early in the design?

[63] Is the product documentation adequate for maintenance by an outside organization?

b. <u>Reliability</u>
[Are the reliability or availability requirements difficult to meet?]

[64] Are reliability requirements allocated to the software?

[65] Are availability requirements allocated to the software?

(Yes) (65.a) Are recovery timelines any problem?

c. <u>Safety</u>
[Are the safety requirements infeasible and not demonstrable?]

[66] Are safety requirements allocated to the software?

(Yes) (66.a) Do you see any difficulty in meeting the safety requirements?

[67] Will it be difficult to verify satisfaction of safety requirements?

d. Security
  [Are the security requirements more stringent than the current state of the practice or program experience?]

[68] Are there unprecedented or state-of-the-art security requirements?

[69] Is it an Orange Book system?

[70] Have you implemented this level of security before?

e. Human Factors
  [Will the system will be difficult to use because of poor human interface definition?]

[71] Do you see any difficulty in meeting the Human Factors requirements?
  (No) (71.a) How are you ensuring that you will meet the human interface requirements?

If prototyping

    (Yes) (71.a.1) Is it a throw-away prototype?
      (No) (71.a.1a) Are you doing evolutionary development?
       (Yes) (71.a.1a.1) Are you experienced in this type of development?
       (Yes) (71.a.1a.2) Are interim versions deliverable?
       (Yes) (71.a.1a.3) Does this complicate change control?

f. Specifications
  [Is the documentation adequate to design, implement, and test the system?]

[72] Is the software requirements specification adequate to design the system?

[73] Are the hardware specifications adequate to design and implement the software?

[74] Are the external interface requirements well specified?

[75] Are the test specifications adequate to fully test the system?

If in or past implementation phase

[76] Are the design specifications adequate to implement the system?
  • Internal interfaces

B. Development Environment

1. Development Process

a. Formality
[Will the implementation be difficult to understand or maintain?]

[77] Is there more than one development model being used?
- Spiral
- Waterfall
- Incremental

(Yes) (77.a) Is coordination between them a problem?

[78] Are there formal, controlled plans for all development activities?
- Requirements analysis
- Design
- Code
- Integration and test
- Installation
- Quality assurance
- Configuration management

(Yes) (78.a) Do the plans specify the process well?

(Yes) (78.b) Are developers familiar with the plans?

b. Suitability
[Is the process suited to the development model, e.g., spiral, prototyping?]

[79] Is the development process adequate for this product?

[80] Is the development process supported by a compatible set of procedures, methods, and tools?

c. Process Control
[Is the software development process enforced, monitored, and controlled using metrics? Are distributed development sites coordinated?]

[81] Does everyone follow the development process?

(Yes) (81.a) How is this insured?

[82] Can you measure whether the development process is meeting your productivity and quality goals?

If there are distributed development sites

[83] Is there adequate coordination among distributed development sites?

d. Familiarity
[Are the project members experienced in use of the process? Is the process understood by all staff members?]

[84]   Are people comfortable with the development process?

e. Product Control
[Are there mechanisms for controlling changes in the product?]

[85]   Is there a requirements traceability mechanism that tracks requirements from the source specification through test cases?

[86]   Is the traceability mechanism used in evaluating requirement change impact analyses?

[87]   Is there a formal change control process?

    (Yes) (87.a)   Does it cover all changes to baselined requirements, design, code, and documentation?

[88]   Are changes at any level mapped up to the system level and down through the test level?

[89]   Is there adequate analysis when new requirements are added to the system?

[90]   Do you have a way to track interfaces?

[91]   Are the test plans and procedures updated as part of the change process?

2.   Development System

a. Capacity
[Is there sufficient work station processing power, memory, or storage capacity?]

[92]   Are there enough workstations and processing capacity for all staff?

[93]   Is there sufficient capacity for overlapping phases, such as coding, integration and test?

b. Suitability
[Does the development system support all phases, activities, and functions?]

[94]   Does the development system support all aspects of the program?
- Requirements analysis
- Performance analysis
- Design
- Coding
- Test
- Documentation
- Configuration management
- Management tracking
- Requirements traceability

c.   Usability
      [How easy is the development system to use?]

[95] Do people find the development system easy to use?

[96] Is there good documentation of the development system?

d.   Familiarity
      [Is there little prior company or project member experience with the development system?]

[97] Have people used these tools and methods before?

e.   Reliability
      [Does the system suffer from software bugs, down-time, insufficient built-in back-up?]

[98] Is the system considered reliable?
      • Compiler
      • Development tools
      • Hardware

f.   System Support
      [Is there timely expert or vendor support for the system?]

[99] Are the people trained in use of the development tools?

[100] Do you have access to experts in use of the system?

[101] Do the vendors respond to problems rapidly?

g.   Deliverability
      [Are the definition and acceptance requirements defined for delivering the development system to the customer not budgeted? HINT: If the participants are confused about this, it is probably not an issue from a risk perspective.]

[102] Are you delivering the development system to the customer?

      (Yes) (102.a) Have adequate budget, schedule, and resources been allocated for this deliverable?

3.   **Management Process**

a.   Planning
      [Is the planning timely, technical leads included, contingency planning done?]

[103] Is the program managed according to the plan?

      (Yes) (103.a) Do people routinely get pulled away to fight fires?

[104] Is re-planning done when disruptions occur?

[105] Are people at all levels included in planning their own work?

[106] Are there contingency plans for known risks?

(Yes) (106.a) How do you determine when to activate the contingencies?

[107] Are long-term issues being adequately addressed?

b. Project Organization
[Are the roles and reporting relationships clear?]

[108] Is the program organization effective?

[109] Do people understand their own and others' roles in the program?

[110] Do people know who has authority for what?

c. Management Experience
[Are the managers experienced in software development, software management, the application domain, the development process, or on large programs?]

[111] Does the program have experienced managers?
- Software management
- Hands-on software development
- With this development process
- In the application domain
- Program size or complexity

d. Program Interfaces
[Is there poor interface with customer, other contractors, senior and/or peer managers?]

[112] Does management communicate problems up and down the line?

[113] Are conflicts with the customer documented and resolved in a timely manner?

[114] Does management involve appropriate program members in meetings with the customer?
- Technical leaders
- Developers
- Analysts

[115] Does management work to ensure that all customer factions are represented in decisions regarding functionality and operation?

[116] Is it good politics to present an optimistic picture to the customer or senior management?

4. **Management Methods**

a. Monitoring
[Are management metrics defined and development progress tracked?]

[117] Are there periodic structured status reports?

(Yes) (117.a) Do people get a response to their status reports?

[118] Does appropriate information get reported to the right organizational levels?

[119] Do you track progress versus plan?

    (Yes) (119.a) Does management have a clear picture of what is going on?

b.   Personnel Management
[Are project personnel trained and used appropriately?]

[120] Do people get trained in skills required for this program?

    (Yes) (120.a) Is this part of the program plan?

[121] Do people get assigned to the program who do not match the experience profile for your work area?

[122] Is it easy for program members to get management action?

[123] Are program members at all levels aware of their status versus plan?

[124] Do people feel it's important to keep to the plan?

[125] Does management consult with people before making decisions that affect their work?

[126] Does program management involve appropriate program members in meetings with the customer?
- Technical leaders
- Developers
- Analysts

c.   Quality Assurance
[Are there adequate procedures and resources to assure product quality?]

[127] Is the software quality assurance function adequately staffed on this program?

[128] Do you have defined mechanisms for assuring quality?

    (Yes) (128.a) Do all areas and phases have quality procedures?

    (Yes) (128.b) Are people used to working with these procedures?

d.   <u>Configuration Management</u>
        [Are the change procedures or version control, including installation site(s), adequate?]

[129] Do you have an adequate configuration management system?

[130] Is the configuration management function adequately staffed?

[131] Is coordination required with an installed system?

        (Yes)   (131.a)   Is there adequate configuration management of the installed system?

        (Yes)   (131.b)   Does the configuration management system synchronize your work with site changes?

[132] Are you installing in multiple sites?

        (Yes)   (132.a)   Does the configuration management system provide for multiple sites?

5.   Work Environment

a.   <u>Quality Attitude</u>
        [Is there a lack of orientation toward quality work?]

[133] Are all staff levels oriented toward quality procedures?

[134] Does schedule get in the way of quality?

b.   <u>Cooperation</u>
        [Is there a lack of team spirit? Does conflict resolution require management intervention?]

[135] Do people work cooperatively across functional boundaries?

[136] Do people work effectively toward common goals?

[137] Is management intervention sometimes required to get people working together?

c.   <u>Communication</u>
        [Is there poor awareness of mission or goals, poor communication of technical information among peers and managers?]

[138] Is there good communication among the members of the program?
- Managers
- Technical leaders
- Developers
- Testers
- Configuration management
- Quality assurance

[139] Are the managers receptive to communication from program staff?

(Yes) (139.a) Do you feel free to ask your managers for help?

(Yes) (139.b) Are members of the program able to raise risks without having a solution in hand?

[140] Do the program members get timely notification of events that may affect their work?

(Yes) (140.a) Is this formal or informal?

d. Morale
[Is there a non-productive, non-creative atmosphere? Do people feel that there is no recognition or reward for superior work?]

[141] How is morale on the program?

(No) (141.a) What is the main contributing factor to low morale?

[142] Is there any problem keeping the people you need?

C. Program Constraints

1. Resources

a. Schedule
[Is the schedule inadequate or unstable?]

[143] Has the schedule been stable?

[144] Is the schedule realistic?

(Yes) (144.a) Is the estimation method based on historical data?

(Yes) (144.b) Has the method worked well in the past?

[145] Is there anything for which adequate schedule was not planned?
- Analysis and studies
- QA
- Training
- Maintenance courses and training
- Capital equipment
- Deliverable development system

[146] Are there external dependencies which are likely to impact the schedule?

b. Staff
[Is the staff inexperienced, lacking domain knowledge, lacking skills, or understaffed?]

[147] Are there any areas in which the required technical skills are lacking?
- Software engineering and requirements analysis method
- Algorithm expertise
- Design and design methods
- Programming languages
- Integration and test methods
- Reliability
- Maintainability
- Availability
- Human factors
- Configuration management
- Quality assurance
- Target environment
- Level of security
- COTS
- Reuse software
- Operating system
- Database
- Application domain

- Performance analysis
- Time-critical applications

[148] Do you have adequate personnel to staff the program?

[149] Is the staffing stable?

[150] Do you have access to the right people when you need them?

[151] Have the program members implemented systems of this type?

[152] Is the program reliant on a few key people?

[153] Is there any problem with getting cleared people?

c. Budget
    [Is the funding insufficient or unstable?]

[154] Is the budget stable?

[155] Is the budget based on a realistic estimate?

    (Yes) (155.a) Is the estimation method based on historical data?

    (Yes) (155.b) Has the method worked well in the past?

[156] Have features or functions been deleted as part of a design-to-cost effort?

[157] Is there anything for which adequate budget was not allocated?
- Analysis and studies
- QA
- Training
- Maintenance courses
- Capital equipment
- Deliverable development system

[158] Do budget changes accompany requirement changes?

    (Yes) (158.a) Is this a standard part of the change control process?

d. Facilities
    [Are the facilities adequate for building and delivering the product?]

[159] Are the development facilities adequate?

[160] Is the integration environment adequate?

2. Contract

a. Type of Contract
    [Is the contract type a source of risk to the program?]

[161] What type of contract do you have? (Cost plus award fee, fixed price,....)

(161a) Does this present any problems?

[162] Is the contract burdensome in any aspect of the program?
- SOW (Statement of Work)
- Specifications
- DIDs (Data Item Descriptions)
- Contract parts
- Excessive customer involvement

[163] Is the required documentation burdensome?
- Excessive amount
- Picky customer
- Long approval cycle

b. Restrictions
[Does the contract cause any restrictions?]

[164] Are there problems with data rights?
- COTS software
- Developmental software
- Non-developmental items

c. Dependencies
[Does the program have any dependencies on outside products or services?]

[165] Are there dependencies on external products or services that may affect the product, budget, or schedule?
- Associate contractors
- Prime contractor
- Subcontractors
- Vendors or suppliers
- Customer furnished equipment or software

3.   Program Interfaces

<u>a.</u>   Customer
[Are there any customer problems such as: lengthy document-approval cycle, poor communication, and inadequate domain expertise?]

[166] Is the customer approval cycle timely?
- Documentation
- Program reviews
- Formal reviews

[167] Do you ever proceed before receiving customer approval?

[168] Does the customer understand the technical aspects of the system?

[169] Does the customer understand software?

[170] Does the customer interfere with process or people?

[171] Does management work with the customer to reach mutually agreeable decisions in a timely manner?
- Requirements understanding
- Test criteria
- Schedule adjustments
- Interfaces

[172] How effective are your mechanisms for reaching agreements with the customer?
- Working groups (contractual?)
- Technical interchange meetings (contractual?)

[173] Are all customer factions involved in reaching agreements?

(Yes)   (173.a)   Is it a formally defined process?

[174] Does management present a realistic or optimistic picture to the customer?

If there are associate contractors

<u>b.</u>   Associate Contractors
[Are there any problems with associate contractors, such as inadequately defined or unstable interfaces, poor communication, or lack of cooperation?]

[175] Are the external interfaces changing without adequate notification, coordination, or formal change procedures?

[176] Is there an adequate transition plan?

(Yes)   (176.a)   Is it supported by all contractors and site personnel?

[177] Is there any problem with getting schedules or interface data from associate contractors?

(No)   (177.a) Are they accurate?

If there are subcontractors

c.   Subcontractors
[Is the program dependent on subcontractors for any critical areas?]

[178] Are there any ambiguities in subcontractor task definitions?

[179] Is the subcontractor reporting and monitoring procedure different from the program's reporting requirements?

[180] Is subcontractor administration and technical management done by a separate organization?

[181] Are you highly dependent on subcontractor expertise in any areas?

[182] Is subcontractor knowledge being transferred to the company?

[183] Is there any problem with getting schedules or interface data from subcontractors?

If program is a subcontract

d.   Prime Contractor
[Is the program facing difficulties with its Prime contractor?]

[184] Are your task definitions from the Prime ambiguous?

[185] Do you interface with two separate prime organizations for administration and technical management?

[186] Are you highly dependent on the Prime for expertise in any areas?

[187] Is there any problem with getting schedules or interface data from the Prime?

e.   Corporate Management
[Is there a lack of support or micro management from upper management?]

[188] Does program management communicate problems to senior management?
(Yes) (188.a) Does this seem to be effective?

[189] Does corporate management give you timely support in solving your problems?

[190] Does corporate management tend to micro-manage?

[191] Does management present a realistic or optimistic picture to senior management?

f.   Vendors
[Are vendors responsive to programs needs?]

[192] Are you relying on vendors for deliveries of critical components?

- Compilers
- Hardware
- COTS

g. <u>Politics</u>
[Are politics causing a problem for the program?]

[193] Are politics affecting the program?
- Company
- Customer
- Associate contractors
- Subcontractors

[194] Are politics affecting technical decisions?

Chapter A-33

Taxonomy-Based Questionnaire (TBQ) Interviews

List of risks

Section

Section 1

TBQ Interviews Description

Introduction

Taxonomy-based questionnaire interviews (TBQ interviews) are structured interviews of project personnel. The primary instrument for the interviews is the **Taxonomy-Based Questionnaire** [Chapter A-32]. There are two basic interview types:
- group (interviews of peer groups of project personnel)
- individual (interviews of individual project personnel)

Diagram

The following diagram shows the inputs, supporting material, and outputs for TBQ interviews.
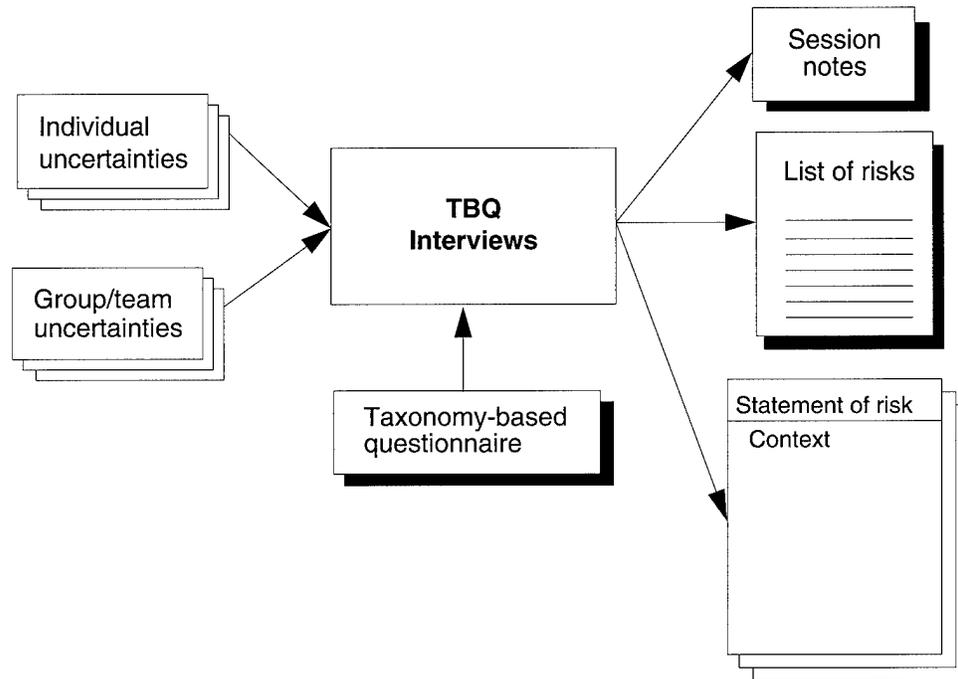
Personnel Requirements

TBQ interviews may be performed with one to five participants from the project identifying risks. Conducting a TBQ interview requires at least one person (trained in facilitating) to do the interviewing. Additional personnel (also trained in facilitating) may be needed to adequately capture the statements of risk and context information and support the interviewer.

Section 2

When to Use

When to Use The table below discusses when to use each interview type.

Interview Type	When to Use
Group	The group interviews are an effective method for identifying an initial set (baseline) of risks for the project. When used this way, they also help to establish a risk awareness throughout the project.
	Group interviews can also be used periodically to re-assess the risk status of the project for major milestones.
Individual	These interviews are effective in allowing the individual voice to be heard.
	They can be used to probe more deeply into a technical domain. Individual interviews can be used to broaden the direct involvement of personnel in the project.

Constraints Trained facilitators must be available to conduct the interview. In general, they should not be from the project organization staff in order to encourage open communication about risk.

Interviews take time—e.g., at least 2-1/2 hours for a group interview and 1-1/2 hours for an individual interview.

Benefits Interviews are, in general, effective stimuli for risk awareness and can be used to systematically involve and motivate personnel.

The TBQ interview method can be used at any time.

Interviews provide an opportunity to re-assess the risk condition of the project.

Section 3

Conducting a TBQ Interview

Procedure

The steps for either a group or individual interview are described in the following table. These activities are carried out by the interviewer and supporting facilitators, referred to as the facilitation team.

Step	Action
1	**Tailor the questionnaire**. Use the Project Profile Questions [Chapter A-25] to determine which questions or sections of the taxonomy may be skipped.
2	**Select participants**. Identify the participants, secure their commitment to participate, and advise them of their scheduled interview time. *Note:* The group interview session requires 2-1/2 hours. Individual interview sessions require 1-1/2 hours.
3	**Prepare facilities**. Schedule the interview rooms and ensure that the appropriate materials for capturing risk information are available in the room. *Note*: Capturing statements of risk may be done using a flipchart, whiteboard, overhead projector and transparency, etc.
4	**Conduct the interview**. Review the process steps with the participants and iteratively proceed through the following: • Ask a TBQ question. • Ask follow-up question(s), as needed. • Pursue risk, as needed. • Capture and record the risk statement and context information, as needed. Ten minutes before the scheduled end of the interview, ask the closing question: Are there any issues, concerns or risks that have not been satisfactorily addressed in this session?
5	**Document the data**. Record each statement of risk and its context on a Risk Information Sheet [Chapter A-27] or equivalent project document. Compile a list of risks for the session. Consolidate all of the data. *Note*: This step is optional for any single interview session. The data from multiple interview sessions can be consolidated in a single data consolidation session. *Note*: The interview participants need not be present for Step 5.

Selection of Project Personnel

Participants should be selected by the facilitation team by working with the project manager and using the guidelines shown in the following table.

Guideline	Description
Willingness and openness	The personnel selected (the participants) should be willing and able to express themselves in a focused meeting setting. The quality of information will suffer if the people are unable to attend or unwilling to share their views.
Experience and project knowledge	Participants should be drawn from the project's most experienced and knowledgeable people. They should have knowledge of both their job and the project to identify risks endemic to the project.
Peer relationships—group interviews only	To promote a free flow of information, it is important there be no reporting relationship among the members of each group. Although in many cases there is a good working relationship of people with their managers, past experience has shown that managers or technical leaders dominate sessions where subordinates are part of the same group.

Section 4

TBQ Interview Tools

Software Development Risk Taxonomy and TBQ

The following diagram shows the structure of the Taxonomy with all of the classes, elements, and attributes. The **Taxonomy-Based Questionnaire** [Chapter A-32] includes one or more non-judgemental questions associated with each of these attributes that are used to elicit risks within a software development project. It is the primary tool for conducting a risk identification interview.

Taxonomy of Software Development Risks

Class → A. Product Engineering

1. Requirements
   a. Stability
   b. Completeness
   c. Clarity
   d. Validity
   e. Feasibility
   f. Precedent
   g. Scale

Element → 2. Design
   a. Functionality
   b. Difficulty
   c. Interfaces
   d. Performance
   e. Testability
   f. Hardware Constraints

Attribute → g. Non-Developmental Software

3. Code and Unit Test
   a. Feasibility
   b. Testing
   c. Coding/Implementation

4. Integration and Test
   a. Environment
   b. Product
   c. System

5. Engineering Specialties
   a. Maintainability
   b. Reliability
   c. Safety
   d. Security
   e. Human Factors
   f. Specifications

B. Development Environment

1. Development Process
   a. Formality
   b. Suitability
   c. Process Control
   d. Familiarity
   e. Product Control

2. Development System
   a. Capacity
   b. Suitability
   c. Usability
   d. Familiarity
   e. Reliability
   f. System Support
   g. Deliverability

3. Management Process
   a. Planning
   b. Project Organization
   c. Management Experience
   d. Program Interfaces

4. Management Methods
   a. Monitoring
   b. Personnel Management
   c. Quality Assurance
   d. Configuration Management

5. Work Environment
   a. Quality Attitude
   b. Cooperation
   c. Communication
   d. Morale

C. Program Constraints

1. Resources
   a. Schedule
   b. Staff
   c. Budget
   d. Facilities

2. Contract
   a. Type of Contract
   b. Restrictions
   c. Dependencies

3. Program Interfaces
   a. Customer
   b. Associate Contractors
   c. Subcontractors
   d. Prime Contractor
   e. Corporate Management
   f. Vendors
   g. Politics

Section 5

Guidelines and Tips

Non-Judgemental Atmosphere

It is important that the interviews are conducted in a non-judgemental atmosphere and the information is held as confidential. Nothing said in the interview is attributed to the group or any individual.

Establish an environment that encourages a candid discussion of risks.

Example: Conduct the interviews in an enclosed room with table and chairs in a location different from the daily work environment. Ensure that there are no interruptions during the interviews.

Interview Groups

Generally there are three to four separate group interview sessions. A representative set of group interviews would include

- software engineers
- technical managers
- support groups (configuration management, quality assurance, testing)
- project manager

Group Interview Scheduling

Group interviews should be held periodically throughout the life of the project. The exact number and schedule for conducting these interviews is based upon the individual project's size, duration, objectives, and related management measures. They are planned at specific times throughout the life of the project or are conducted as part of key project milestone events.

Example: A series of group interviews might be scheduled
- annually throughout the life of the project
- in conjunction with key milestones (e.g., PDR, CDR)
- in response to a major event or change within the project

Once scheduled, it is important that everyone attend and be on time to the interviews. The interview should begin and end precisely at the scheduled times.

Individual Interview Scheduling

Individual interviews should be scheduled periodically (for example, quarterly) as a sequence of six to ten individual interview sessions conducted over a one- or two-day period.

Capturing Risk Information

It is useful to display the identified statements of risk so they are visible to all interview participants. Participants can see if the risks are captured adequately as well as review what risks have already been identified. Throughout the interview, it is not uncommon to identify information relevant to a risk which has already been identified. This information may suggest a need to alter the risk statement or add more information to the context.

Chapter A-34

Taxonomy Classification

Software development risk

Product engineering	Development environment	Program constraints
Requirements risk • • risk	**Development process** risk • • risk	**Resources** risk • • risk
• •	• •	• •
Engineering specialties risk • • risk	**Work environment** risk • • risk	**Program interfaces** risk • • risk

Section 1

Taxonomy Classification Description

Introduction   The taxonomy classification method organizes risks into groups based on the elements of the software development risk taxonomy [Carr 93]. The criteria or basis for the classification (e.g., most proximate cause, condition, or impact) is selected and used to determine where each risk fits in the software development risk taxonomy.

Diagram   The following diagram shows the inputs and output for taxonomy classification.
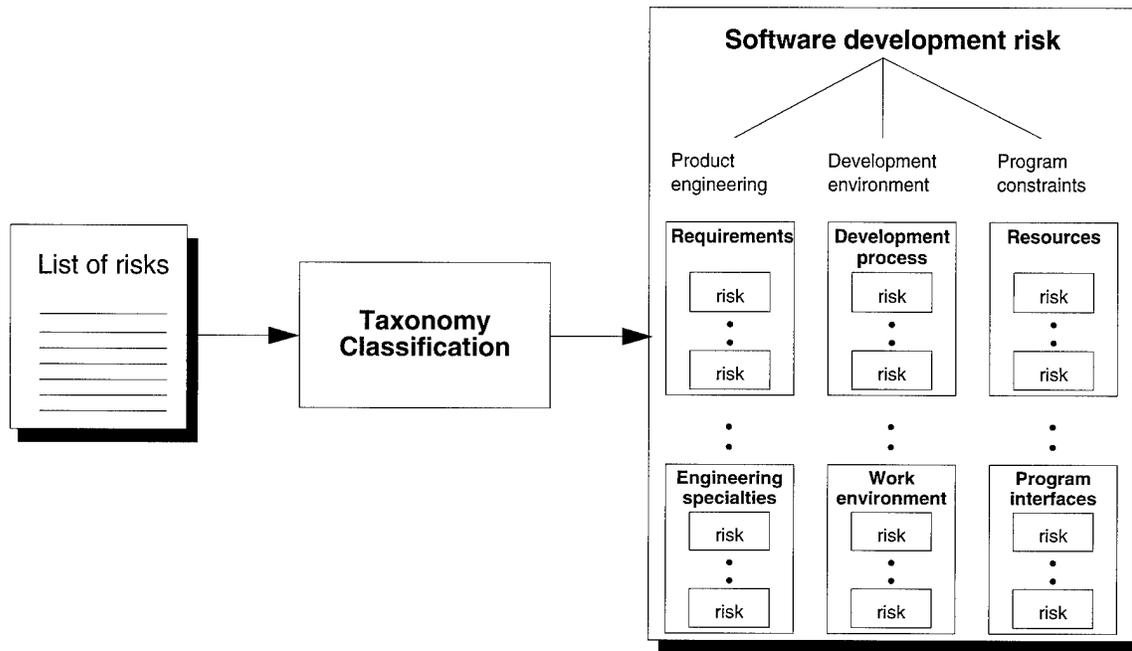
Personnel Requirements   Taxonomy classification may be performed by an individual or a group. If performed by a group of three or more, one person should be the facilitator and recorder (but he or she could still participate or contribute).

Section 2

When to Use

When to Use

Use this method

- to classify risks in a software context
- when you need a structure to begin classification

Constraints

The concepts of proximate cause or impact are not always clear for each risk. Different people may come up with different causes or impacts. If used as the basis for classification, these need to be clearly defined to minimize unnecessary differences. Proximate cause, for example, is generally considered to be the "closest" cause to the risk as opposed to a root cause. Note that subjective judgment is still required, even with a clear definition.

Benefits

This method

- provides a structure to group risks.
- produces results that provide input into planning mitigation strategies for the risks

Section 3

Constructing a Taxonomy Classification

Procedure

The table below describes the procedure for classifying risks according to the software development risk taxonomy [Carr 93].

Step	Action
1	**Review risks for understanding**. The participants review the statement of risk and context for each risk for understanding.
2	**Select the classification criterion**. The participants come to consensus on the how risks will be organized according to the Software Development Risk Taxonomy. Common criteria selected include the condition, most proximate cause, or impact. *Note*: The most proximate cause is the immediate cause but may not necessarily be the root cause
3	**Determine the class**. The participants come to consensus on which of the following classes the risk fits in based on the selected criteria [Carr 93, p.8]: • *product engineering*: the technical aspects of the work to be accomplished • *development environment*: the methods, procedures, and tools used to produce the product • *program constraints*: the contractual, organizational, and operational factors within which the software is developed but which are generally outside the direct control of the local management If the class chosen is development environment, skip to Step 5. If the class chosen is program constraints, skip to Step 6.
4	**Determine element in the product engineering class**. The participants come to consensus on which element the risks fits in based on the selected criteria [Carr 93, p. 10]. • *requirements*: the definition of what the software product is to do, the needs it must meet, how it is to behave, and how it will be used. This element also addresses the feasibility of developing the product and the scale of the effort. • *design*: the translation of requirements into an effective design within project and operational constraints • *code and unit test*: the translation of software designs into code that satisfies the requirements allocated to individual units • *integration and test*: the integration of units into a working system and the validation that the software product performs as required • *engineering specialties*: product requirements or development activities that may need specialized expertise such as safety, security, and reliability Skip to Step 7.

Step	Action
5	**Determine element in the development environment class.** The participants come to consensus on which element the risks fits in based on the selected criteria [Carr 93, p.10]. • *development process*: the definition, planning, documentation, suitability, enforcement, and communication of the methods and procedures used to develop the product • *development system*: the tools and supporting equipment used in product development, such as computer-aided software engineering (CASE) tools, simulators, compilers, and host computer systems • *management process*: the planning, monitoring, and controlling of budgets and schedules; controlling factors involved in defining, implementing, and testing the product; the project manager's experience in software development, management, and the product domain; and the manager's expertise in dealing with external organizations, including customers, senior management, matrix management, and other contractors • *management methods*: the methods, tools, and supporting equipment that will be used to manage and control the product development, such as monitoring tools, personnel management, quality assurance and configuration management • *work environment*: the general environment within which the work will be performed, including the attitudes of people and the levels of cooperation, communication, and morale Skip to Step 7.
6	**Determine element in the program constraint class.** The participants come to consensus on which element the risks fits in based on the selected criteria [Carr 93, p.11]. • *resources*: the external constraints imposed on schedule, staff, budget, or facilities • *contract*: the terms and conditions of the project contract • *program interfaces*: the external influences to customers, other contractors, corporate management, and vendors
7	**Repeat steps 3-6 for each remaining risk.**
8	**Review the groups of risk in each class/element.** After all risks have been classified, the participants look at all the risks grouped under each specific class and element. If a risk does not appear to belong with the other risks in that group, the participants make adjustments as necessary. Repeating steps 3 - 6 for the risk may be necessary.

Section 4

Taxonomy Classification Tools

Taxonomy of Software Development Risks

Below is an overview of the taxonomy groups and their hierarchical organization into class, element, and attribute [Carr 93]. Once you are familiar with the definitions for the classes and elements, this overview is a helpful aid when classifying risks. It serves as a quick reference to the entire software development taxonomy.

Taxonomy of Software Development Risks

Class → **A. Product Engineering**

1. Requirements
   a. Stability
   b. Completeness
   c. Clarity
   d. Validity
   e. Feasibility
   f. Precedent
   g. Scale

Element → 2. Design
   a. Functionality
   b. Difficulty
   c. Interfaces
   d. Performance
   e. Testability
   f. Hardware Constraints

Attribute → g. Non-Developmental Software

3. Code and Unit Test
   a. Feasibility
   b. Testing
   c. Coding/Implementation

4. Integration and Test
   a. Environment
   b. Product
   c. System

5. Engineering Specialties
   a. Maintainability
   b. Reliability
   c. Safety
   d. Security
   e. Human Factors
   f. Specifications

B. Development Environment

1. Development Process
   a. Formality
   b. Suitability
   c. Process Control
   d. Familiarity
   e. Product Control

2. Development System
   a. Capacity
   b. Suitability
   c. Usability
   d. Familiarity
   e. Reliability
   f. System Support
   g. Deliverability

3. Management Process
   a. Planning
   b. Project Organization
   c. Management Experience
   d. Program Interfaces

4. Management Methods
   a. Monitoring
   b. Personnel Management
   c. Quality Assurance
   d. Configuration Management

5. Work Environment
   a. Quality Attitude
   b. Cooperation
   c. Communication
   d. Morale

C. Program Constraints

1. Resources
   a. Schedule
   b. Staff
   c. Budget
   d. Facilities

2. Contract
   a. Type of Contract
   b. Restrictions
   c. Dependencies

3. Program Interfaces
   a. Customer
   b. Associate Contractors
   c. Subcontractors
   d. Prime Contractor
   e. Corporate Management
   f. Vendors
   g. Politics

Section 5

Guidelines and Tips

Collaborate

The method works best when two to three people collaborate on determining the classification criteria and where it fits in the software development risk taxonomy structure.

Best Guess

If consensus cannot be reached easily at any step for a specific risk (e.g., within three minutes), make a best guess and move on to the next risk. The process is self-correcting. When you see all the risks in the groups it will become clear which risks have been misplaced.

Attributes

Looking at the attributes under each element can be helpful in determining which element the risk best fits into based on the classification criteria.

Review and Adjust

The method results must not be used rigidly. After classifying the risks, if the project discovers that a risk does not really fit with the other risks under the element it was placed, the risk should be moved to the appropriate place. The taxonomy classification provides a guide to grouping risks.

Reference

Cited in this chapter:

[Carr 93]

Carr, Marvin; Konda, Suresh; Monarch, Ira; Ulrich, Carol; & Walker, Clay. *Taxonomy-Based Risk Identification* (CMU/SEI-93-TR-6, ADA266992). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

Chapter A-35

Time Correlation Chart

Description

Time correlation charts show the relationship of one measure with respect to another over time. They are a form of scatter diagrams and are used to study and identify potential relationships between observed changes in two sets of variables.

How to Use

Time correlation charts are used during the **Track** [Chapter 7] and **Control** [Chapter 8] paradigm functions to determine if there is a relationship between two variables over time. Trends can be identified before trigger values are reached. The independent variable (cause) is plotted on the x-axis, and the dependent variable (effect) is plotted on the y-axis. If a correlation between the variables exists, it can be linear or nonlinear, positive or negative. There are a variety of statistical methods available to analyze the data. These diagrams are often a good follow-up to **Cause and Effect Analysis** [Chapter A-8]. Time correlation charts do not predict cause and effect relationships; they show the strength of the relationship between the two variables over time.

Positive Correlation Example

A risk concerning the high amount of frametime being used to update sensor information relative to the amount of screen display code implemented has been identified. Project personnel are interested in tracking the relationship between the indicators using a time correlation chart. From the time correlation chart below, it is determined that a positive correlation between the two variables exists. Personnel can use this information in evaluating the severity of the risk.
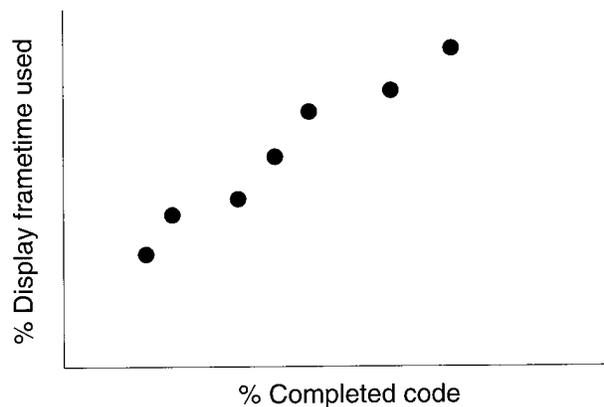
No Correlation Example

A risk associated with incomplete requirements documents and their effect on quality has been identified. The mitigation plan calls for project personnel to receive quality improvement training, because it is believed that a lack of training is the root cause of the risk. During risk mitigation, the relationship between the number of personnel who have received the training and the defect density of the software is tracked. From the time correlation chart shown below, it is determined that no correlation between the two variables exists. Project personnel must reassess their mitigation plan to identify the real causes of the risk and to address them.
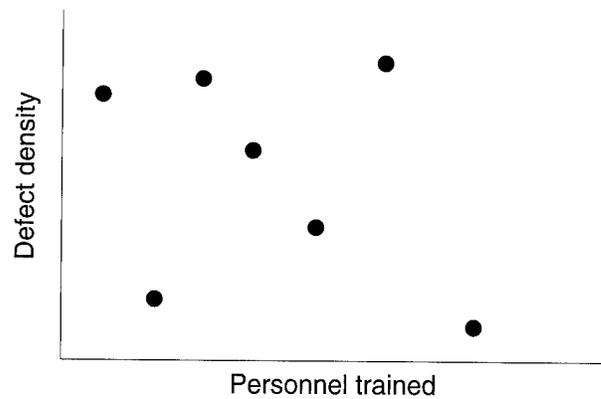
Negative Correlation Example

A new contract requires project personnel to use a programming language that they haven't used before. To mitigate the risk associated with using a new language, project personnel will receive training. During risk mitigation, the relationship between the number of personnel trained in the programming language and the defect density of the software will be tracked. From the time correlation chart below, it is determined that a negative correlation between the two variables exists. As more project personnel receive training, a corresponding drop in the defect rate is seen, justifying the expense of the training. Personnel can continue to use this information to determine if they will achieve their mitigation goals for the risk.
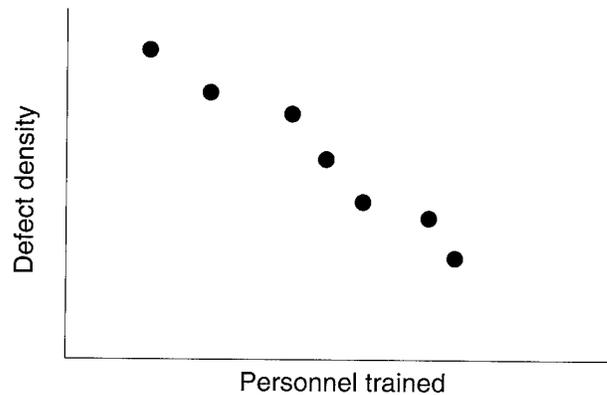
References

For more information on time correlation charts, see the following:

[Brassard 89]   Brassard, Michael. *The Memory Jogger +™: featuring the seven management and planning tools*. Methuen, Ma.: GOAL/QPC, 1989.

[Hays 88]   Hays, William L. *Statistics*. New York: Holt, Reinhart and Winston, Inc., 1988.

[Moran 90]   Moran, John W.; Talbot, Richard P.; & Benson, Russell M. *A Guide to Graphical Problem-Solving Processes*. Milwaukee Wi.: ASQC Quality Press, 1990.

Chapter A-36

Time Graph

Description   Time graphs, also known as run charts, allow data to be tracked for trends or patterns over a period of time.

How to Use   Time graphs are used during the **Track** [Chapter 7] and **Control** [Chapter 8] paradigm functions to document the values of risk status indicators over time. The indicators along with their associated triggers are defined during the **Plan** function [Chapter 6], and indicator values are periodically acquired during risk tracking. The values of the data are then graphically plotted as a function of time. The graphs are used to identify trends in the chosen status indicators.

Example   On a project, the mitigation plan defines risk exposure as the indicator that must be tracked over time. During risk tracking, project personnel periodically reassess the impact and probability measures for the risk and calculate the risk exposure from them. Risk exposure is then plotted on a time graph as shown in the diagram below. Note that the trigger values are also shown on the graph.
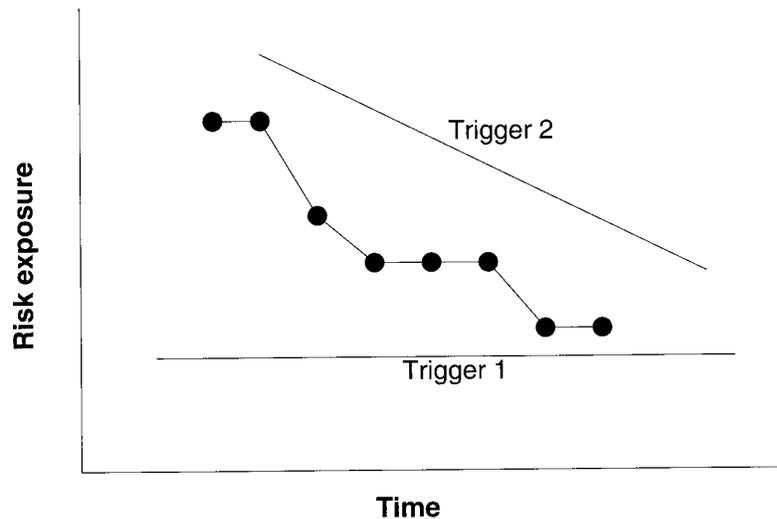
Note: Time graphs are used as part of **Mitigation Status Reports** [Chapter A-16] where risk exposure is tracked against the mitigation plan over time.

References

For more information on time graphs, see the following:

[Brassard 89]   Brassard, Michael. *The Memory Jogger +*™*: featuring the seven management and planning tools*. Methuen, Ma.: GOAL/QPC, 1989.

[Hays 88]   Hays, William L. *Statistics*. New York: Holt, Reinhart and Winston, Inc., 1988.

[Moran 90]   Moran, John W.; Talbot, Richard P.; & Benson, Russell M. *A Guide to Graphical Problem-Solving Processes*. Milwaukee Wi.: ASQC Quality Press, 1990.

Chapter A-37

Top 5
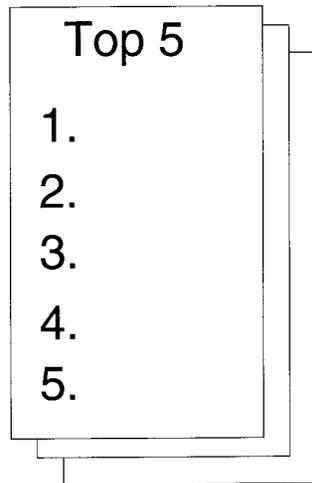
Top 5

1.

2.

3.

4.

5.

Section 1

Top 5 Description

Introduction

Top 5 is a simple method for an individual to select the five most important risks to the project, generally used as part of a group analysis effort. An individual (participant) reviews the statements of risk, context, and his or her own attribute values for each risk and selects the top 5 most important risks to the project. The intent is collect the individual perspectives on what is most important to the project as opposed to a group consensus.

Diagram

The following diagram shows the input and output of the top 5 method.
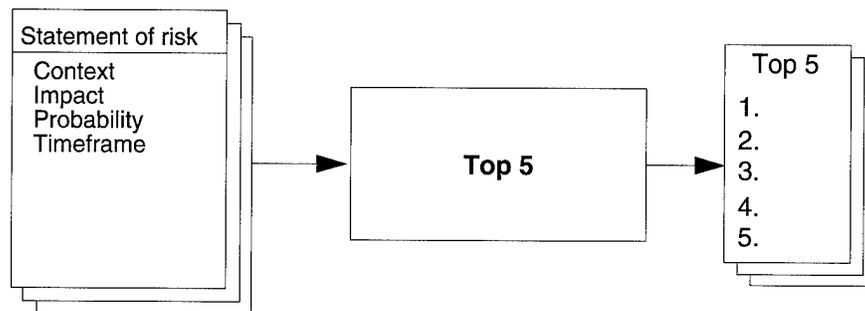
Note: There is one top 5 list for each participant.

Personnel Requirements

A top 5 list is completed by each participant. This can be each participant during a **Baseline Identification and Analysis** [Chapter A-4], each person in the entire project, or a sample of selected individuals within the project.

Section 2

When to Use

When to Use

Use this method
- when you want to know the individual perspectives of the top risks to the project
- following the use of **TBQ Interviews** [Chapter A-33] and either the **Binary Attribute Evaluation** [Chapter A-6] or **Tri-level Attribute Evaluation** [Chapter A-38] method

Constraints

Each individual will select the top 5 based on his or her definition of most important. If the project doesn't specify what "most important" means, the individual selections may not best meet the project's needs.

Benefits

This method
- is simple. All steps are straightforward.
- does not require resource-intensive activities. The method works with the knowledge the participants bring.
- is quick. Top 5 can be accomplished in a few minutes.

Section 3

Generating a Top 5 List

**Top 5
Selection
Procedure**

The following table describes how a participant should evaluate the top 5 risks identified.

Step	Action
1	**Review risks and attributes**. Review the statement of risk, context, and attribute values for each risk.
2	**Mark the most important risks to the project**. Without worrying about order, mark the most important risks to the project. If the number is greater than five, compare risks and reduce the list.
3	**Order top 5 risks**. Compare the five risks and order them from one to five with a "1" being the most important risk to the project.

Section 4

Top 5 Tools

Sample Evaluation Form

Below is a sample of an evaluation form (described under the **Binary Attribute Evaluation** method [Chapter A-6] augmented with a column for the top 5 risks.

Evaluation Form

Top 5	Risk		Significant Impact	Likely to Occur	Near-term Timeframe
2	Risk A	X	✓	✓	✓
	Risk B			✓	
	Risk C		✓		
5	Risk D	X	✓		
	Risk E				✓
1	Risk F	X	✓	✓	✓
4	Risk G	X	✓	✓	
3	Risk H	X	✓		✓
	Risk I		✓	✓	

Section 5

Guidelines and Tips

Project vs. Individual

Emphasize to the participants that they should consider the top risks to the project as a whole, not just their own part of the project.

Attribute Values First

This method should be conducted after the attributes of the risk have been given values. The attribute values can help the participant decide on the top 5 risks.

Definition of "Most Important"

A shared project definition of what "most important" means will aid individual selection of top 5 and simplify the consolidation into a project perspective of most important risks.

Chapter A-38

Tri-level Attribute Evaluation

Evaluation Form

Risk	Impact	Probability	Risk Exposure	Timeframe
Statement of risk A	Catastrophic	Probable	High	Mid-term
Statement of risk B	Critical	Probable	Moderate	Far-term
Statement of risk C	Catastrophic	Very likely	High	Near-term
Statement of risk D	Critical	Very likely	High	Near-term
Statement of risk E	Critical	Improbable	Low	Far-term

Section

Section 1

Tri-level Attribute Evaluation Description

Introduction

Tri-level attribute evaluation is a simple method for evaluating the impact, probability, and timeframe of a risk, providing a qualitative analysis for risks. The attribute values for each risk are determined based on specific criteria.

Note: When a group conducts a tri-level attribute evaluation on a set of risks, each participant evaluates the impact, probability, and timeframe. The final output represents the consensus evaluations for each risk.

Diagram

The following diagram shows the input and output of the tri-level attribute evaluation method.
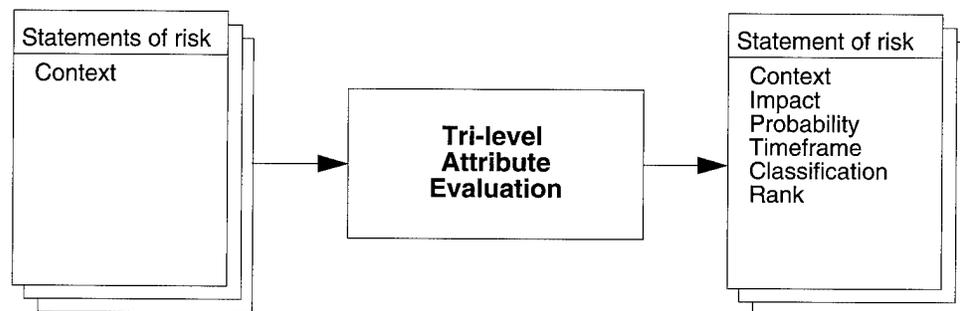
Personnel Requirements

Tri-level attribute evaluation can be completed by an individual or a group. If performed by a group of three or more, one person should be the facilitator and recorder (but he or she could still participate or contribute).

Section 2

When to Use

When to Use

Use this method

- to discriminate among a large number of risks such as during **Baseline Identification and Analysis** [Chapter A-4]
- following the use of **TBQ Interviews** [Chapter A-33]

Constraints

This method provides a qualitative level of analysis. Many risks can have the same evaluation, yet the degree of each attribute may be different. This method cannot distinguish between the risks when this occurs.

Example: Risk A and Risk B may both have been separately evaluated as having a catastrophic impact, very likely to occur, and in the near-term timeframe. However, for Risk A the impact is a schedule slip of 20%; for Risk B, the impact is that the users can't use the system.

In a group application, this method can be time consuming if there is a wide variation in individual evaluations and the group cannot reach consensus quickly.

Benefits

This method

- does not require resource-intensive activities. The method works with the knowledge the participants bring.
- separates risks into high, moderate, and low risk categories

Section 3

Conducting a Tri-level Attribute Evaluation

Attribute Definitions

Each attribute can have one of three values:
- *impact*: catastrophic, critical, marginal
- *probability*: very likely, probable, improbable
- *timeframe*: near-term, mid-term, far-term

Risk Exposure

The table below shows the risk exposure (impact times probability) or magnitude of the risk based on the evaluation of the severity of impact and the probability of occurrence [Sisti 94] which is adapted from the Air Force [Air Force 88] example of risk exposure.

Probability

		Very Likely	Probable	Improbable
Impact	Catastrophic	High	High	Moderate
	Critical	High	Moderate	Low
	Marginal	Moderate	Low	Low

Individual vs. Group

The following two tables provide procedures for conducting tri-level attribute evaluation as an individual and with a group. The group procedure will include the procedure for individuals for those steps that are conducted by the individual.

Individual Procedure

The following table describes how an individual is to evaluate each risk.

Step	Action
1	**Review criteria for attributes**. Ensure you understand the criteria: • *impact*: catastrophic, critical, marginal • *probability*: very likely, probable, improbable • *timeframe*: near-term, mid-term, far-term
2	**Review risks for understanding**. Ensure you understand the statement of risk and context for each risk.
3	**Evaluate the impact of the risk**. Mark the impact severity of the risk as either catastrophic, critical, or marginal based on the defined criteria.
4	**Evaluate the probability of the risk**. Mark the probability of the risk as very likely, probable, or improbable based on the defined criteria.
5	**Determine the risk exposure of the risk**. Mark the risk exposure as high, moderate, or low based on the values for impact and probability.
6	**Evaluate the timeframe of the risk**. Mark the timeframe of the risk as near-term, mid-term, or far-term based on the defined criteria.
7	**Repeat Steps 3-6 for each remaining risk**.

**Group
Procedure**

This table describes the procedure for a facilitator conducting a tri-level attribute evaluation with a group. When this method is used with a group, the individual results will be combined into a single evaluation of risk exposure and timeframe.

Step	Action
1	**Explain individual evaluation procedure**. The facilitator describes to participants how they should evaluate the risks.
2	**Conduct individual evaluation**. Each participant individually evaluates each risk (see individual evaluation procedure).
3	**Determine the range of individual risk exposure and timeframe values**. Record the lowest individual risk exposure value and the highest individual risk exposure value. Record the lowest individual timeframe value and the highest individual timeframe value.
4	**Discuss the ranges and reach consensus on the risk exposure and timeframe values**. Participants discuss why they evaluated as they did. Individuals have the opportunity to adjust their evaluations. If possible, consensus is reached. If consensus cannot be reached, the differences are noted.
5	**Record final evaluation**. Facilitator records/documents the final evaluation with statement of risk and context information.

**Defining
Attribute
Criteria**

The evaluation will work best if the project tailors the general attribute values (e.g., catastrophic impact) by describing criteria for each attribute value (e.g., catastrophic impact means the schedule slips by > 25%).

**Example
Attribute
Criteria**

Below is an example of how the criteria for each attribute value was defined for a specific project.

Value	Impact	Probability	Timeframe
3	A risk is *catastrophic* if one of the following could happen: • schedule slip > 20% • cost overrun > 25% • project loses funding • higher lifecycle costs • end users can't use • morale suffers; people leave	A risk is *very likely* if there is > 70% probability that it will occur.	A risk is *near-term* if the project must take action or will be impacted by the risk in the next 90 days.

Value	Impact	Probability	Timeframe
2	A risk is *critical* if one of the following could happen: • schedule slip 10-20% • cost overrun 10-25% • workarounds for quality problems • morale suffers	A risk is *probable* if there is 30-70% probability that it will occur.	A risk is *mid-term* if the project must take action or will be impacted by the risk in 90-180 days.
1	A risk is *marginal* if it is neither catastrophic nor critical.	A risk is *improbable* if there is < 30% probability that it will occur.	A risk is *far-term* if the project need not take action or will not be impacted by the risk in the next 180 days.

Section 4

Tri-level Attribute Evaluation Tools

Sample Evaluation Form

Below is a sample of an evaluation form each participant would fill out.

Evaluation Form

Risk	Impact	Probability	Risk Exposure	Timeframe
Statement of risk A	Catastrophic	Probable	High	Mid-term
Statement of risk B	Critical	Probable	Moderate	Far-term
Statement of risk C	Catastrophic	Very Likely	High	Near-term
Statement of risk D	Critical	Very Likely	High	Near-term
Statement of risk E	Critical	Improbable	Low	Far-term

Key:

Probability

Impact		Very Likely	Probable	Improbable
	Catastrophic	High	High	Moderate
	Critical	High	Moderate	Low
	Marginal	Moderate	Low	Low

Example: Risk A is evaluated as catastrophic impact, probable, a high level of risk exposure, and in the mid-term timeframe. Risk C is evaluated as having a catastrophic impact, very likely, a high level of risk exposure, and in the near-term timeframe. Risk E is evaluated as having critical impact, improbable, a low level of risk exposure, and in the far-term timeframe.

Sample Consolidation Sheet

A sample of a worksheet the facilitator would use to determine which risks to discuss (Step 4 in the group procedure) based on the ranges for the risk exposure and timeframe values is shown on the next page.

Evaluation Form

Risk	Mary		Joe		Phil		RE Range	Timeframe Range
	RE	T	RE	T	RE	T		
Statement of risk A	H	Mid	H	Near	M	Near	M-H	Mid-near
Statement of risk B	M	Far	M	Mid	M	Mid	M	Far-mid
Statement of risk C	H	Near	H	Far	H	Mid	H	Far-near

Key:

Risk exposure (RE):   Timeframe (T):

H   High   Near   Near-term

M   Moderate   Mid   Mid-term

L   Low   Far   Far-term

Example: Risk A is evaluated as high by two individuals and as a moderate by another individual. Since there is a difference in how the risk is perceived, this risk would be marked for discussion.

Section 5

Guidelines and Tips

General

This method works well as a first attempt at analysis, especially on a large number of risks. It requires few resources and helps to highlight which risks need a more detailed level of analysis.

Experience with the establishing baselines (**Baseline Identification and Analysis** [Chapter A-4]) shows that for a group application, 60 minutes is sufficient for evaluating a set of 30-40 risks. Time will vary based on the number of risks that need to be discussed and the group's ability to reach consensus.

Attribute Value Criteria

The results will be more useful if the project defines the criteria for the attribute values that make sense to the project. The more specific the criteria are, the easier it will be for participants to evaluate the risks. Vague criteria leave the door open to interpretation. The criteria should be applied consistently by project personnel.

Providing participants with a one-page handout containing the attribute definitions and criteria helps them to remember as they evaluate each risk.

Reaching Consensus

It is possible that discussion will be required for every risk based on the range values. This isn't necessarily bad but it can be time consuming to reach consensus depending on the group dynamics.

Automated Support

For group applications, having a computer application available to automatically generate the ranges is helpful. A simple spreadsheet can save time and reduce the possibility of error. A common approach is to assign ordinal numbers (first, second, third, etc.) to the attributes values and derive risk exposure values. When using this approach, beware of performing math on ordinal numbers (see **Analyze** [Chapter 5] for more information).

References

Cited in this chapter:

[Air Force 88]

Air Force Systems Command/Air Force Logistics Command Pamphlet 800-45. *Software Risk Abatement*, September 30, 1988.

[Sisti 94]

Sisti, Frank J. & Joseph, Sujoe. *Software Risk Evaluation Method Version 1.0* (CMU/SEI-94-TR-19, ADA290697). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

Chapter A-39

Voluntary Risk Reporting
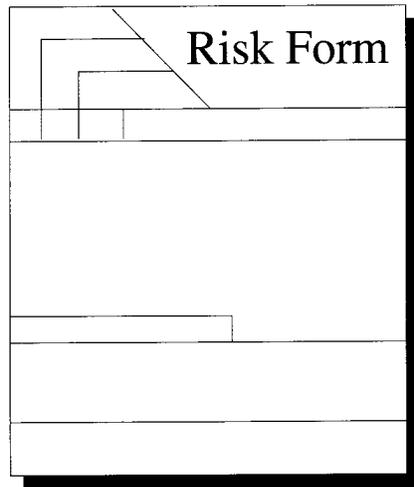
Section

Section 1

Voluntary Risk Reporting Description

Introduction

Voluntary risk reporting is the systematic distribution and regular submission of risk forms as part of routine project activities.

Diagram

The following diagram shows the input and output for voluntary risk reporting method.
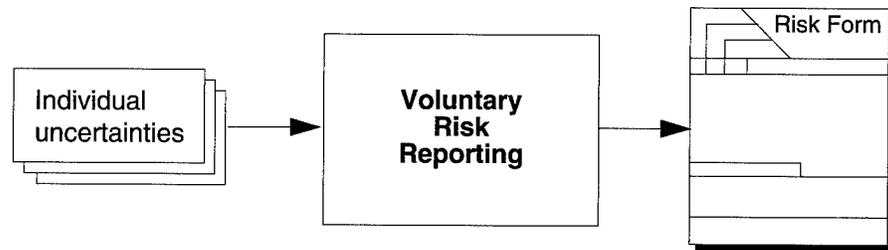
Personnel Requirements

Any member of the project personnel can voluntarily report a risk. One person may be needed to collect and process forms if this is not supported electronically. A person independent of the project could also perform the function of clarifying submitted risks if the submitter's name is included. Such an independent person would be responsible for removing attribution before passing the new risks on to project management.

All project personnel should be familiar with the form to be used and the process for submittal.

Section 2

When to Use

When to Use

Use this method
- to continuously identify risks
- to enable everyone in the project to contribute to the risk identification process
- to ensure anonymous identification of risks

Constraints

A central repository or collection person is required to collect and process risks.

Benefits

This method
- enables any individual to identify a risk (individual input)
- provides an opportunity for independent input at any time (continuously)
- is available to all personnel (project-wide involvement)
- enables any individual to identify a risk without attribution (anonymously). This is useful in a culture that does not have open communication or where there is little trust or rapport between managers and other personnel.

Section 3

Performing Voluntary Risk Reporting

Form Submittal

The steps for using and submitting forms for voluntary risk reporting are described in the following table.

Step	Action
1	**Complete the form**. The Risk Form [Chapter A-26] is one form that can be used for documenting and submitting risks voluntarily. Follow the directions for completing the form. Forms may be paper based or electronic. It is important to provide as much information as possible to support effective decision making about the risk.
2	**Submit form**. Turn in the form as appropriate for your organization. Options include • a central person designated as collector and processor • an electronic risk database • an anonymous drop box
3	**Clarify information, as appropriate**. Be prepared to clarify the risk information through the same anonymous channels if it is requested.

Form Processing

The steps for processing voluntarily reported risks are described in the following table.

Step	Action
1	**Distribute forms**. The forms should be widely distributed and made readily available to all personnel in the project. Distribution options include • forms provided to all personnel as part of a regular distribution of monthly meeting minutes • keeping forms at central locations with other forms used in the project (e.g., time reporting, engineering change forms, etc.) • providing the form electronically, linked with a risk database
2	**Encourage form submittals**. Encourage the submission of a form as soon as a risk is known. As part of regularly scheduled project meetings, project managers should remind project personnel of the forms and encourage them to watch for risks and to submit the risk forms as soon as a new risk is identified. *Note*: In some projects, particularly where risk is openly discussed, forms are submitted directly to management personnel without the need for anonymity.
3	**Collect forms**. Collect the forms on a pre-defined schedule. Paper-based forms may be collected from a designated drop-box. Electronically submitted forms can be printed or reviewed on screen. *Example*: Collect all forms from the four separate anonymous collection boxes every Friday afternoon.

Step	Action
4	**Process results**. Process the results and integrate the newly identified risks into the list of project risks.
	Examples: Processing can include • giving each risk a unique identifier • making sure the form was correctly filled in • adding the risk to the reports required for periodic review of new and existing risks • notifying the appropriate personnel for risks flagged as needing immediate management attention.

Clarifying Anonymous Data

It may be necessary to provide some means of gathering clarification or additional data on submitted risks. This can be difficult if submittals are anonymous. Management must decide on a means of notifying submitters that more information is needed and allowing them to provide it with the same degree of anonymity. Possibilities include

• notifying personnel during routine project meetings that a risk requires additional information. Anyone can provide the information during the meeting or afterwards.

• providing a supplementary form for additional information

• using electronic notification and collection of information

Section 4

Voluntary Risk Reporting Tools

Sample Risk Form

The risk form is one form that can be used to perform voluntary risk reporting. The format is not important, the availability of the form for use by personnel is. Below is a sample completed risk form.

Impact	Probability	Timeframe	Risk Form	ID#_____ (for internal use only)

Date: _4/5/96_

H	H	N	Statement of risk (with context)

The GUI must be coded using X Windows and we do not have expertise in X; the GUI code may not be completed on time and may be inefficient.

Context: The graphical user interface is an important part of the system and we do not have anyone trained in the X Window System. We all have been studying the language but it is complex and only one person in the group has any graphics experience and that is with Windows on the PC.

✓	**Requires immediate management attention**

Recommendation for dealing with the risk (optional):

Identify an expert in X to work with the team and begin a formal training project for the staff assigned to the GUI.

Classification:

Program Constraints, Resources, Staff (Risk Taxonomy)

Section 5

Guidelines and Tips

Anonymity

If anonymity is an objective, it is important that the entire organization has confidence in the integrity of the system.

**Use
Established
Processes**

It can be very effective to handle forms within established problem trouble reporting processes or within similar routine practices of the project.

**Monitor and
Improve**

Monitor the process; if it does not appear to be working, consider alternative methods, such as regular individual interviews or required risk reporting.

Chapter A-40

Work Breakdown Structure (WBS)

Description

A work breakdown structures (WBS) is a standard tool for project management. It provides a method for dividing a project into a number of small tasks and for assuring that all project activities are logically identified and related. It is commonly supported by project management software.

How to Use

For risk planning: A WBS defines a framework for the work to be accomplished in mitigating the risks and identifies who is responsible for accomplishing the work. It should be structured on tangible and deliverable items for both hardware and software, and there are no set rules on the level of detail required. Combined with other planning tools (e.g., a **Gantt Chart** [Chapter A-12] or a **PERT Chart** [Chapter A-20]), a WBS is a powerful tool for managing a complex mitigation strategy.

For mitigation resources: Since a project WBS provides a method for dividing the project into a number of small tasks and assures that all project activities are logically identified and related, it can be used to identify the project personnel who should be aware of a risk and involved in its mitigation.

For risk analysis: Finally, a project WBS can also be used during the **Analyze** function [Chapter 5] to provide a structure in which to classify risks.

Example Background

This example shows a risk statement and the mitigation goals as well as the key issues about the risk.

Risk statement
• The translation effort looks like it will slip; if it does, the whole test schedule will be in jeopardy.
Mitigation goals
• Modify the schedule with possible completion date further out.
• Do not increase cost.
• Identify a drop-dead date and include a buffer.
• Get to independent validation & verification with "quality" product (i.e., one that satisfies requirements).
Key issues
• software and firmware maturity
• test lab time
• system performance requirements
• repair priority
• spares

<div style="border:1px solid black; padding:10px;">

Task activities

- Produce aggressive test strategy for firmware-software (evaluate interface and performance).
- Develop test case and scenarios for areas of concern.
- Develop summary stress test.
- Clarify lab tasking and control.
- Establish priority for spares.
- Develop realistic serial-parallel schedules.

</div>

Example WBS for a Mitigation Task Plan

For risk planning: This WBS shows the tasks that were developed to deal with the key issues and mitigate the risk while achieving the mitigation goals. A Gantt chart for this example is shown in Chapter A-12.

```
                      ┌──────────────┐
                      │ Translation  │
                      │   effort     │
                      └──────────────┘
                 ┌───────────┴────────────────┐
        ┌──────────────┐              ┌──────────────┐
        │   Produce    │              │   Develop    │
        │  aggressive  │              │  realistic   │
        │    test      │              │  schedule    │
        │  strategy    │              └──────────────┘
        └──────────────┘
   ┌──────┬──────────┴───────┬──────────────┐
┌────────┐ ┌────────┐ ┌──────────┐ ┌──────────┐
│Develop │ │Develop │ │Establish │ │Clarify lab│
│ test   │ │ stress │ │ priority │ │tasking &  │
│ cases  │ │ test   │ │for spares│ │ control   │
└────────┘ └────────┘ └──────────┘ └──────────┘
```
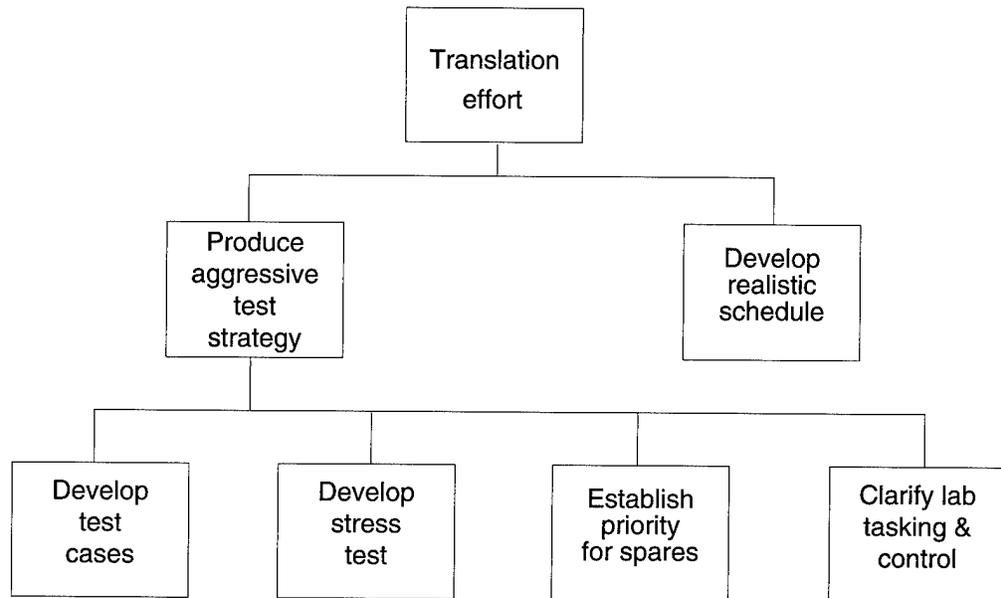
Examples Using a Project WBS

For mitigation resources: Since the above risk deals with testing issues, project personnel can go to the original project WBS to examine the testing-related tasks. By doing this, they can identify the people who should be aware of the risk and involved in its mitigation.

For risk analysis: When the above risk was first being analyzed during the risk identification and analysis process, project personnel used the project WBS to classify the risk and group it with other testing-related risks.

References

For more information about how to construct and use WBS, see the following:

[Bennatan 92]   Bennatan, E. M. *On Time, Within Budget - Software Project Management Practices and Techniques*. McGraw-Hill International (UK) Limited, 1992.

[Evans 83]   Evans, M. W.; Piazza, P.; & Dolkas, J. B. *Principles of Productive Software Management*. New York: John Wiley and Sons, 1983.

[Mayrhauser 90]   Mayrhauser, Anneliese von. *Software Engineering: Methods and Management*. San Diego Ca.: Academic Press, Inc., 1990.

[Meredith 89]   Meredith, Jack R. & Mantel, Samuel J. Jr. *Project Management: A Managerial Approach*, 2nd ed. New York: John Wiley and Sons, 1989.

[Pfleeger 91]   Pfleeger, Shari Lawrence. *Software Engineering: The Production of Quality Software*, 2nd ed. New York: MacMillan Publishing Co., 1991.

[Pressman 92]   Pressman, Roger S. *Software Engineering: A Practitioner's Approach*, 3rd ed. New York: MacGraw-Hill, Inc., 1992.

[Radice 88]   Radice, Ron A. & Phillips, Richard W. Chapter 6, "Planning The Project," 183-184. *Software Engineering: An Industrial Approach*, Volume 1. Englewood Cliffs, N.J.: Prentice Hall, 1988.

[Shere 88]   Shere, Kenneth D. *Software Engineering and Management*. Englewood Cliffs, N.J.: Prentice Hall, 1988.

[Thayer 88]   Thayer, Richard H. *Software Engineering Project Management Tutorial*. Washington D.C.: Computer Society Press of the Institute of Electrical and Electronics Engineers, Inc., 1988.

Index

S