



CarnegieMellon
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

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.

Unlimited distribution subject to copyright law.

The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

Copyright 1996 by Carnegie Mellon University.

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-CMMSM)¹ and is expected to become a key process area within the Software Capability Maturity Model (SW-CMMSM)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.

1. The SA-CMM is being published at the time of this writing.

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.

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).

2. CMM and Capability Maturity Model are service marks of Carnegie Mellon University.

Table of Contents

Preface		i
<hr/>		
Acknowledgments		iii
<hr/>		
Part 1	Introduction	1
<hr/>		
Chapter 1	Introduction to Continuous Risk Management	3
Chapter 2	How to Use This Guidebook	11
Part 2	What Is Continuous Risk Management?	17
<hr/>		
Chapter 3	Overview	19
Chapter 4	Identify	27
Chapter 5	Analyze	37
Chapter 6	Plan	53
Chapter 7	Track	73
Chapter 8	Control	91
Chapter 9	Communicate	103
Chapter 10	Summary	115
Part 3	Continuous Risk Management: Example Implementation	123
<hr/>		
Chapter 11	An Implemented Continuous Risk Management Practice	125
Chapter 12	Life-Cycle of a Risk	143
Part 4	How to Get Started in Continuous Risk Management	157
<hr/>		
Chapter 13	Overview	159
Chapter 14	Getting Started	167
Chapter 15	Install a Basic Risk Management Practice	183
Chapter 16	Improve and Expand Continuous Risk Management	197

Chapter 17	Transition Scenario	205
Chapter 18	Summary	217
Part 5	Summary and Conclusions	225
Chapter 19	Summary	227
Chapter 20	Conclusions	235
References		241
Glossary		245
Appendix A	Methods and Tools	251
Chapter A-1	Action Item List	255
Chapter A-2	Affinity Grouping	257
Chapter A-3	Bar Graph	263
Chapter A-4	Baseline Identification and Analysis	265
Chapter A-5	Baseline Planning	275
Chapter A-6	Binary Attribute Evaluation	285
Chapter A-7	Brainstorming	295
Chapter A-8	Cause and Effect Analysis	301
Chapter A-9	Closing a Risk	307
Chapter A-10	Comparison Risk Ranking	317
Chapter A-11	Cost-Benefit Analysis	325
Chapter A-12	Gantt Charts	333
Chapter A-13	Goal-Question-Measure	337
Chapter A-14	Interrelationship Digraph	345
Chapter A-15	List Reduction	355
Chapter A-16	Mitigation Status Report	361
Chapter A-17	Multivoting	383
Chapter A-18	Pareto Top N	391
Chapter A-19	Periodic Risk Reporting	399

Chapter A-20	PERT Charts	407
Chapter A-21	Planning Decision Flowchart	411
Chapter A-22	Planning Worksheet	413
Chapter A-23	Potential Top N	417
Chapter A-24	Problem-Solving Planning	423
Chapter A-25	Project Profile Questions	439
Chapter A-26	Risk Form	443
Chapter A-27	Risk Information Sheet	447
Chapter A-28	Risk Management Plan	451
Chapter A-29	Short Taxonomy-Based Questionnaire (Short TBQ)	457
Chapter A-30	Spreadsheet Risk Tracking	461
Chapter A-31	Stoplight Chart	469
Chapter A-32	Taxonomy-Based Questionnaire (TBQ)	471
Chapter A-33	Taxonomy-Based Questionnaire (TBQ) Interviews	495
Chapter A-34	Taxonomy Classification	503
Chapter A-35	Time Correlation Chart	511
Chapter A-36	Time Graph	513
Chapter A-37	Top 5	515
Chapter A-38	Tri-level Attribute Evaluation	521
Chapter A-39	Voluntary Risk Reporting	531
Chapter A-40	Work Breakdown Structure (WBS)	539
Index		543

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.

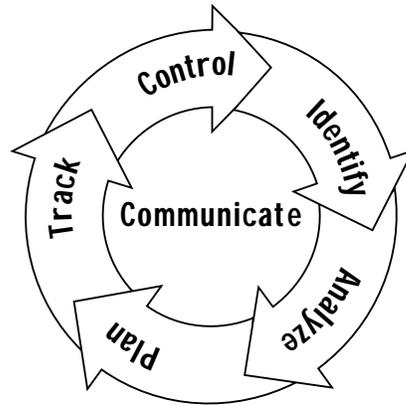
Part	Content	Purpose
Part 2	What is Continuous Risk Management?	Provide an overview of terminology, processes, and functions
Part 3	Continuous Risk Management: Example Implementation	Illustrate Continuous Risk Management as implemented in a typical project
Part 4	How to Get Started in Continuous Risk 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

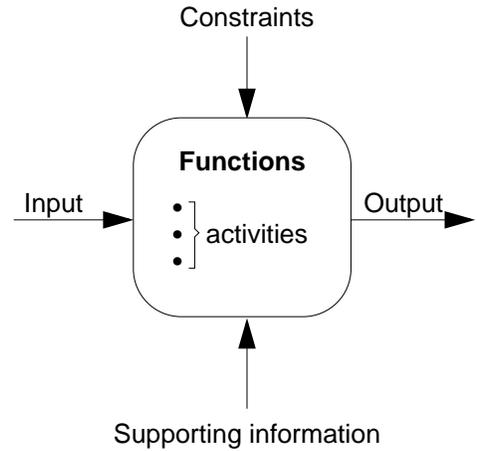
This document was structured and formatted based on the guidelines and formats provided by an Information Mapping® seminar given by Information Mapping, Inc. The most visible aspect of this format is the use of **labels** for each block of information to enable the reader to quickly scan the document 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.



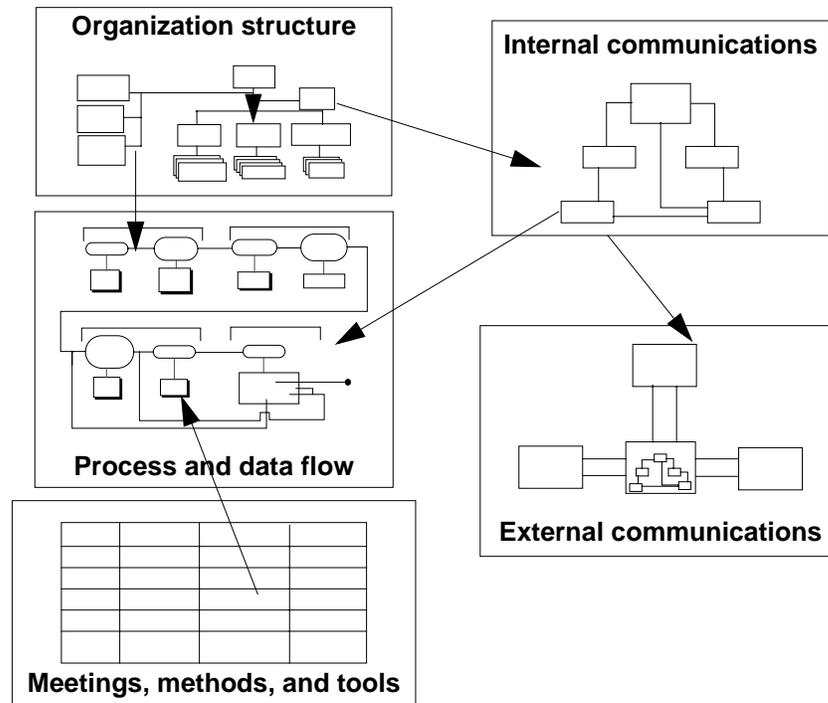
SEI Risk Management Paradigm



Function Diagram

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

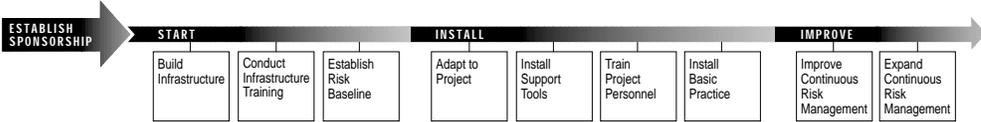
Part 3 provides one view of Continuous Risk Management implemented within a project. An example implementation (see diagram below) is used to provide a framework for showing how an organization might tailor the Continuous Risk Management practice to fit their environment. Internal and external risk communication 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 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 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]

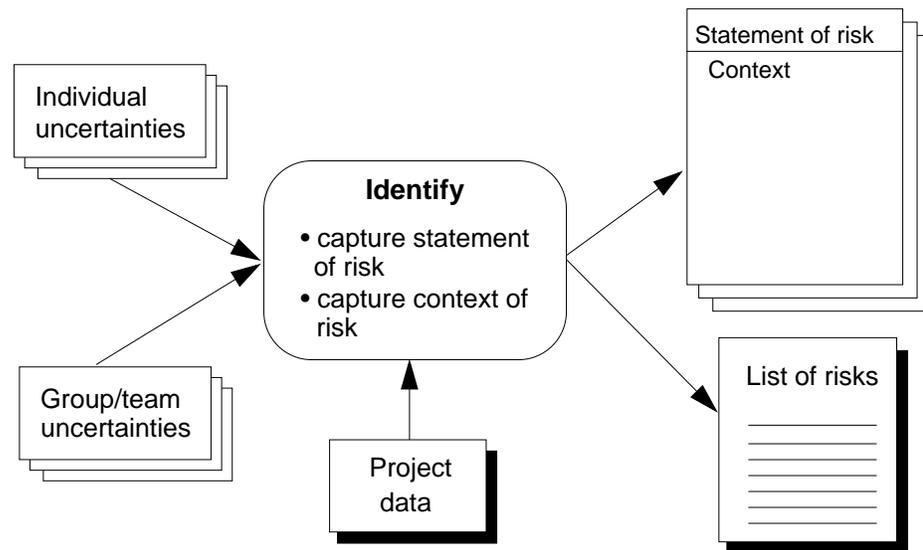
Note: Context provides additional information about the circumstances of the risk.

Objective

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

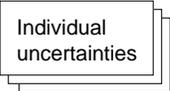
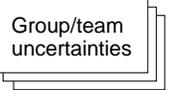
Diagram

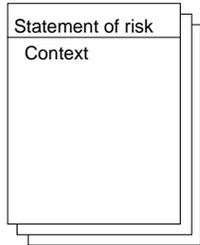
The following diagram shows the inputs and outputs of the **Identify** function.



Data Items

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

Data Item	Description
	Individuals have uncertainties and issues about the project and project progress which may or may not be risks.
	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
	<p>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).</p>
	<p>For each risk identified, a statement of risk is captured along with the associated context for the risk.</p>
	<p>This list contains all the statements of risk identified for the project.</p>

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.

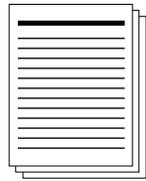
Methods and Tools

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	<ul style="list-style-type: none"> Brainstorming Periodic risk reporting Project profile questions Risk form Short TBQ Taxonomy-based questionnaire (TBQ) TBQ interviews Voluntary risk reporting

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.

