Software Acquisition Risk Management Key Process Area (KPA)—A Guidebook Version 1.0

Brian P. Gallagher
Christopher J. Alberts
Richard E. Barbour
August 1997

HANDBOOK
CMU/SEI-97-HB-002

Handbook

CMU/SEI-97-HB-002
August 1997

Software Acquisition Risk Management Key Process Area (KPA)—A Guidebook Version 1.0

Brian P. Gallagher
Christopher J. Alberts
Richard E. Barbour

Risk Program

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213

This report was prepared for the

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

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

FOR THE COMMANDER

(signature on file)

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

This work is sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number F19628-95-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 52.227-7013.

This document is available through Asset Source for Software Engineering Technology (ASSET): 1350 Earl L. Core Road; PO Box 3305; Morgantown, West Virginia 26505 / Phone:—(304) 284-9000 / FAX—(304) 284-9001 World Wide Web: http://www.asset.com / e-mail: sei@asset.com

Copies of this document are available through the National Technical Information Service (NTIS). For information on ordering, please contact NTIS directly: National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. Phone—(703) 487-4600.

This document is also available through the Defense Technical Information Center (DTIC). DTIC provides access to and transfer of scientific and technical information for DoD personnel, DoD contractors and potential contractors, and other U.S. Government agency personnel and their contractors. To obtain a copy, please contact DTIC directly: Defense Technical Information Center / Attn: BRR / 8725 John J. Kingman Road / Suite 0944 / Ft. Belvoir, VA 22060-6218 / Phone—(703) 767-8274 or toll-free in the U.S.—1-800 225-3842.

Table of Contents

Acknowledgements

The authors wish to acknowledge the following individuals for their contributions to this document.

Jack Ferguson and Ron Higuera for providing vision and leadership.

Sandi Behrens, Jack Cooper, Ron Damer, Audrey Dorofee, Colleen Ellis, Suellen Eslinger, Matt Fisher, Sharon Hoting, Larry Jones, Linda Levine, John Marciniak, Jordan Matejceck, Ira Monarch, Dick Murphy, Jim Murrell, Mike Phillips, Tara Rumsey, Dave Smith, Bill Stone, Rob Sudakow, John Waclo, Julie Walker, and Ray Williams for reviewing early versions and providing valuable comments.

Robert Lang for his editorial efforts and his help structuring the document.

Our customers.

Preface

Goals of this Guidebook

In this guidebook, we hope to provide sponsors of acquisition improvement programs and their immediate staff with guidelines on how to implement a software acquisition risk management program satisfying the goals of the Acquisition Risk Management (ARM) Key Process Area (KPA) of the Software Acquisition Capability Maturity Model[SM] (SA-CMM[SM]). Brief overviews of software acquisition and the SA-CMM can be found in Appendix A, p. 63 and Appendix B, p. 67, respectively.

Guidebook Organization

The following table outlines the guidebook organization.

Component	Purpose
Chapter 1	Provide overviews of risk management and the ARM KPA, and list recommendations for each key practice of the ARM KPA.
Chapter 2	Provide detailed expansions of each key practice within the ARM KPA. Each key practice is described to help readers understand the objective of the practice and examples are provided to help readers apply the practice in various situations. The concept of teaming with other organizations to cooperatively manage project risks is also explored.
Appendix A - Software Acquisition Overview	Provide a short introduction to software acquisition.
Appendix B - The Software Acquisition CMM	Provide a short introduction to the SA-CMM.
Appendix C - Risk Management Methods and Tools	Describe select methods and tools used in risk management.
Appendix D - Selected Risk Management Forms	Provide select forms used in risk management.
Appendix E - The SA-CMM Appraisal Process	Describe the appraisal process used during an SA-CMM appraisal and provide sample questions.

How to Use this Guidebook

Depending on the individual's role or function in the organization, different components 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 Component
Acquisition organization management (e.g., manager above the project manager, sponsor)	Gain general understanding of Acquisition Risk Management	Appendices A & B Chapter 1
Project management (e.g., project manager, chief engineer, chief technical officer, division chiefs)	Learn what Acquisition Risk Management is	Appendices A& B Chapter 1 Chapter 2
Coordinator/developer of Acquisition Risk Management process (e.g., technical managers or leads, software acquisition process group members)	Learn what Acquisition Risk Management is, how to interpret the KPA, and select alternative methods and tools to use when defining a risk management process for a project	Appendices A & B Chapter 1 Chapter 2 Appendix C Appendix D Appendix E
Participant in Acquisition Risk Management (e.g., engineers, project officers, matrixed support, etc.)	Understand Acquisition Risk Management and how to participate in a project's defined risk management process	Chapter 1 Chapter 2 Appendices C & D

Guidebook Prerequisites

To fully understand the guidelines presented in this guidebook, readers should possess a general understanding of the structure and content of the SA-CMM and of basic risk management terminology and principles.

Major References

The following documents were used extensively to develop this guidebook.

[Dorofee 96] Dorofee, A.; Walker, J.; Alberts, C.; Higuera, R.; Murphy, R.; & Williams, R. *Continuous Risk Management Guidebook*. Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1996.

[Ferguson 96] Ferguson, J.; Cooper, J.; Falat, M.; Fisher, M.; Guido, A.; Marciniak, J.; Matejceck, J.; & Webster, R. *Software Acquisition Capability Maturity Model (SA-CMM^{SM}) Version 1.01* (CMU/SEI-96-TR-020). Software Engineering Institute, Carnegie Mellon University, 1996.

Chapter 1

Risk Management

Overview

This chapter introduces readers to risk management and the Acquisition Risk Management (ARM) Key Process Area (KPA) of the Software Acquisition Capability Maturity Model (SA-CMM). Recommendations from Chapter 2 are summarized here for easy reference.

Section

Section 1

Risk Management Overview

Overview

This section introduces risk management and provides an overview of the identify, analyze, plan, track, control, and communicate functions vital to successful implementation of an acquisition risk management process.

Section

Section 1.1

Risk Management Process

What Is Risk?

There are a number of definitions of the term risk, but none is universally accepted. However, all definitions of risk have two common characteristics [Kirkpatrick 92]:

- *uncertainty*: an event may or may not happen
- *loss*: an event has unwanted consequences

The SEI uses the following definition of risk: Risk is the possibility of suffering loss [Dorofee 96].

Risk vs. Opportunity

Risk and opportunity are related. Opportunity for advancement can't be realized without taking a risk. In this case, risk should not necessarily be viewed negatively, because it is essential to making progress. The key is to balance the potential negative consequences of risk against the potential benefits of opportunity [Kirkpatrick 92].

Example: A company that wants to increase its market share might decide to assume more risk in order to achieve its goal.

Risks vs. Problems

As defined above, risk is the possibility of suffering loss. Notice that uncertainty is associated with risk —an event may or may not happen. When a negative event or issue is a certainty, it is considered to be a problem, not a risk.

Risk Example

The software for a system being acquired must be developed using C++ and object-oriented (OO) technology. The contractor selected to develop the software has experience in the application domain, but has little experience with C++ and OO development. Personnel on the project team are concerned that the contractor's inexperience with C++ and OO technology will affect its ability to develop a system that meets the performance or functionality requirements within the defined schedule.

The risk is: The contractor does not have experience using C++ and OO technology; the system may not meet its performance or functionality requirements within the defined schedule.

There is uncertainty associated with whether the system will meet its performance or functionality requirements within the defined schedule—the contractor may or may not meet the requirements. Therefore, this is a risk.

Problem Example

An organization is acquiring a manufacturing process control system. The contractor informs the project team that during system integration and test, the process control system was found to crash periodically.

There is no uncertainty associated with the crashing of the process control system—it occurs periodically. Therefore, this is a problem.

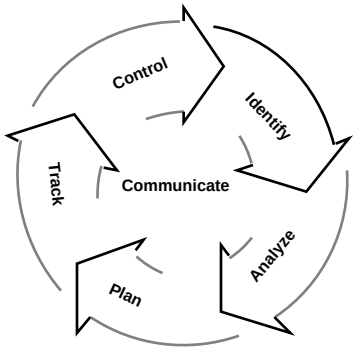
Overview of a General Process

There are many models for managing risk. A systematic risk management process must have a set of steps, or functions, that must be performed to manage project risks. In general, it must provide a way to identify project risks, to evaluate and prioritize risks, to develop plans designed to mitigate the most important project risks, to monitor the progress of the plans and their effectiveness in reducing risks, and to take additional corrective actions if necessary.

SEI Risk Management Paradigm

The SEI risk management paradigm, shown below [Van Scoy 92], defines a systematic process for managing a project's risks. The paradigm consists of a number of functions that are performed as continuous activities throughout a project's life cycle.

Note: The SEI risk management paradigm is one systematic process that can be used to manage risks. Other processes exist, but they are not described in this guidebook.



Paradigm Functions

The functions of the SEI risk management paradigm are outlined in the table below [Higuera 93] and expanded in the next section. Managers must rely on the experience and expertise of their personnel to effectively manage risks; the knowledge derived from participation in an activity as well as the unique skills of team members provide managers with additional information that they might not have had otherwise. All relevant risk data, including decisions made and actions taken, should be kept in a repository, because the data might be relevant to the present project or to other projects within the organization.

Paradigm Function	Purpose
Identify	To search for and find risks before they become problems
Analyze	To transform risk data into information that can be used to aid decision-making. The impacts, probabilities, and timeframes for risks are evaluated, and the risks are classified and prioritized.
Plan	To transform risk information into planning decisions and mitigation actions and to implement the mitigation actions
Track	To monitor risk metrics and mitigation actions to determine if the plan is on schedule as well as if the mitigation plan is effective in reducing the risk
Control	To make informed, timely, and effective decisions regarding risks and their mitigation plans

Paradigm Function	Purpose
Communicate	To provide information and feedback about the risk management process, mitigated or watched risks, and emerging risks. Sources for risk information may be either internal or external to the project Communication is an enabler of the other paradigm functions.

Continuous Process

A risk will typically progress through the paradigm functions sequentially, but the risk management functions are performed continually (i.e., risks are managed continuously throughout all phases of a project), concurrently (i.e., mitigation plans for risks are developed and tracked while new risks are being identified and analyzed), and iteratively (i.e., a mitigation plan for one risk may be used to identify another risk) throughout a project's life cycle [Dorofee 96]. Acquisition risk management requires sustaining constant vigilance and managing risks routinely throughout all phases of the project's life cycle.

Performing the Risk Management Functions

The risk management functions need further definition in order for a project to put these concepts into practice. The next section expands the definition of each function and provides components that can be used by a project to define a risk management process.

Section 1.2

Identify, Analyze, Plan, Track, Control, and Communicate

Identify

Risk identification is a process where uncertainties and issues about a project are transformed into tangible risks, which can be described and measured. Everyone on a project is responsible for identifying risks. The following table describes the components of risk identification [Dorofee 96]. Techniques used to identify risks include structured or unstructured brainstorming, peer-group interviews, and voluntary reporting. The methods and tools used to support identification are found in Appendix C, p. 71.

Component	Description
Capture statement of risk	Capturing a statement of risk includes considering and recording the conditions that are causing concern of a possible loss to the project. A brief description of the perceived consequences resulting from the conditions is also included in a statement of risk.
Capture context of risk	Capturing the context of a risk involves recording additional information regarding the circumstances, events, and interrelationships within the project that supplements the risk statement. Context provides more detail than is presented by the risk statement.

Analyze

Risk analysis is a process in which risks are examined in detail. The purpose is to determine the extent of the risks, how they relate to each other, and which ones are the most important. Personnel who have the appropriate knowledge, expertise, and background to effectively deal with risk information are responsible for evaluating, classifying, and prioritizing the risks.

Example: On one software acquisition project, when project personnel identify risks, they are responsible for estimating the risks' attribute values (see table below) as well as the risks' classification (see table below). The technical leads on the project examine the risks' attribute values and classifications and make any necessary changes. The technical leads are also responsible for prioritizing their teams' risks.

The following table describes the components of risk analysis [Dorofee 96]. The methods and tools used to support analysis are found in Appendix C, p. 71.

Component	Description
Evaluate	Evaluating the attributes of a risk involves establishing • impact: the loss or effect on the project if a risk occurs • probability: the likelihood that a risk will occur • timeframe: the time period during which action will be required to mitigate the risk

Component	Description
Classify	Classifying risks requires grouping risks based on their shared characteristics. The groups, which can also be called classes or sets, show the relationships among the risks. Risk classification can be used to help identify duplicate risks as well as to help simplify a list of risks.
Prioritize	Prioritizing risks involves the following: • partitioning risks or sets of risks based on the "vital few" sense [Juran 89] to separate those that are most important from the rest • ranking the most important risks or sets of risks based upon a criterion or set of criteria established by the project The product of risk prioritization is a ranking of the most important risks to the project, known as a "top N" list [Dorofee 96].

Plan

Planning is a process whereby decisions are made about what should be done with a risk. The results of planning are risk action plans for individual risks or sets of related risks. Personnel who have the knowledge, expertise, background, and resources to effectively deal with risks are responsible for developing their plans. In general, the goal of planning is to answer the following questions:

- Is it my risk? (responsibility)
- What can I do? (approach)
- How much and what should I do? (scope and actions)

The following table describes the components of risk planning [Dorofee 96]. The methods and tools used to support planning are found in Appendix C, p. 71.

Component	Description
Assign responsibility	Assigning responsibility for planning requires a project manager or a designated person(s) to review and understand the risks and to determine what to do with them. There are three choices in determining responsibility for risks: • Keep the risk. • Transfer the risk upward within the organization or to another organization. • Delegate the risk within the organization.

Component	Description
Determine approach	Determining an approach for planning a risk involves making a decision about the type of plan that will be required. • Is enough information known about the risk? If the answer is no, then develop a research plan to get the required information. • If the risk becomes a problem, can the impact of the consequences be accepted? Or can the risk be more efficiently addressed at a future time? If the answer is yes, then accept the risk, expend no further resources managing it, and document the reasons for accepting the risk (acceptance rationale). • If the risk can't be accepted, is it necessary to take immediate action? If the answer is yes, then mitigate the risk by developing and implementing a mitigation plan. • Is there a mitigation action that can or needs to be taken? Or can the risk be accepted? If the answer is no, then the risk must be watched and tracking requirements must be developed (e.g., metrics must be tracked). *Note*: The metrics required to track watched risks and mitigation plans are defined during planning.
Define scope and actions	Defining scope and actions involves answering the following questions when developing a mitigation plan: • How complex will the mitigation be? • How should it be documented? • What is the strategy? • What are the tasks? There are generally two types of mitigation plans, 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, including schedules and budgets for complex sets of actions

Track

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 metrics gathered during tracking are defined during planning and are presented to decision makers in tracking documents or presentations. The information is then used to make control decisions about watched risks and mitigation plans. The following table describes the components of risk tracking [Dorofee 96]. The methods and tools used to support tracking are found in Appendix C, p. 71.

Component	Description
Acquire	Acquiring risk data includes all of the steps associated with collecting information about and updating the values of risk metrics for watched and mitigated risks. The purpose of the information is to track the progress of watched risks and risk mitigation plans.
Compile	Compiling risk data involves analyzing, combining, calculating, and organizing data for a given risk to monitor the progress and effectiveness of a mitigation plan or to monitor changes in watched risks. *Note*: The reporting requirements determine how project personnel compile the data.
Report	Reporting involves communicating status information about risks and mitigation plans to decision makers and team members. Communicating risk information can be accomplished with written reports (using either paper or electronic media) or oral presentations. The delivered reports and presentations summarize the data that were analyzed and organized and are used by decision makers during control.

Control

Control is a process in which a decision maker analyzes the data contained in tracking reports, makes a decision, and implements the decision. The person who has accountability for a risk normally makes the control decision for that risk. The following table describes the components of risk control [Dorofee 96]. The methods and tools used to support control are found in Appendix C, p. 71.

Component	Description
Analyze	Analyzing risk data includes examining project data 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.
Decide	Making a decision requires using tracking data to determine how to proceed with project risks. Four basic decisions with respect to risks can be made: • replan • close the risk • invoke a contingency plan • continue tracking and executing the current plan
Execute	Executing a decision is the process where control decisions are implemented. Making changes to plans requires a return to planning, while taking predefined contingency actions and continuing to track risks requires a return to tracking.

Communicate

Risk communication deals with two subjects that people don't normally communicate well: probability and negative consequences. Managers need to establish a culture where risks are identified and addressed as a part of everyday business and where risk information is viewed positively and rewarded. Successful risk communication surfaces relevant issues and potential problems, allows information to be exchanged within and between all project levels, values the individual voice, and preserves non-attribution and trusted use of all risk information. Communication is an enabler of the other paradigm functions and ensures that

- risks and their mitigation plans are understood
- risk information is visible to all project members
- appropriate attention is applied to risk information
- an effective, ongoing dialog between the manager and the project team is established

Section 2

Acquisition Risk Management Overview

What Is Acquisition Risk Management (ARM)?

ARM is a process where risks are managed throughout the software acquisition life cycle (see Appendix A, p. 63). It is a two-part process [Marciniak 90].

- Early in the life cycle, the risks associated with the acquisition of the system are identified and analyzed, and an approach to mitigate the high-priority risks are incorporated into the software acquisition plan.
- A process to continually manage risks throughout the software acquisition life cycle is integrated into the project's defined software acquisition process.

When Does ARM Begin and End?

Acquisition risk management begins at the earliest phases of an acquisition and continues until the acquisition has been completed. Risk must be considered even in the earliest stages of system development, such as determining business objectives and developing alternative approaches to meet those objectives. Likewise, risk must be considered through user acceptance and transitioning maintenance of a system to a support organization. Acquisition risk management is a vital part of the entire software acquisition process.

Purpose of Acquisition Risk Management

The purpose of acquisition risk management is to identify risks at the earliest possible time, adjust the acquisition strategy to manage the high-priority risks, and implement a risk management process to manage risks throughout the acquisition life cycle [Marciniak 90].

Why Manage Risk?

Employing risk management can help managers identify potential problems and take action to prevent the problems from occurring. When managers continually manage risk, they can avoid disasters and prevent costly rework [Boehm 89].

Acquisition Risk Management Key Process Area

The goals and common features of the Acquisition Risk Management Key Process Area (see Appendix B, p. 67) are listed below [Ferguson 96]. Each of the goals and common features will be examined in more detail in Chapter 2 of this guidebook.

Goal	Description
Goal 1	Software acquisition risk management is an integral part of the project's defined software acquisition process.
Goal 2	The project identifies and deals with risk in a positive manner, such that identification is recognized and rewarded, and results in effective risk handling.

Common Feature	Description
Activity 1	Software acquisition risk management activities are integrated into software acquisition planning.
Activity 2	The Software Acquisition Risk Management Plan is developed in accordance with the project's defined software acquisition process.
Activity 3	The project team performs its software acquisition risk management activities in accordance with its documented plans.

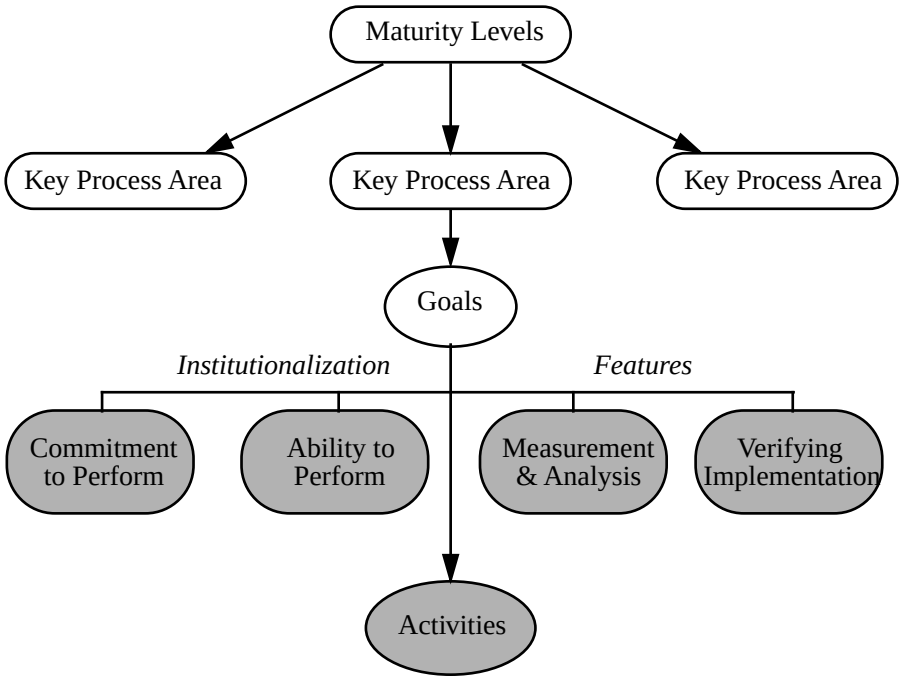
Common Feature	Description
Activity 4	Risk management is conducted as an integral part of the solicitation, project performance management, and contract performance management processes.
Activity 5	Software acquisition risk handling actions are tracked and controlled until the risks are mitigated.
Commitment 1	The acquisition organization has a written policy for the management of software acquisition risk.
Commitment 2	Responsibility for software acquisition risk management activities is designated.
Ability 1	A group that is responsible for coordinating software acquisition risk management activities exists.
Ability 2	Adequate resources are provided for software acquisition risk management activities.
Ability 3	Individuals performing software acquisition risk management activities have experience or receive required training.
Measurement 1	Measurements are made and used to determine the status of the acquisition risk management activities and resultant products.
Verification 1	Acquisition risk management activities are reviewed by acquisition organization management on a periodic basis.
Verification 2	Acquisition risk management activities are reviewed by the project manager on both a periodic and event-driven basis.

Section 3

Summary of Recommendations

Overview

This section provides a summary of the recommendations for the key practices of the ARM KPA. Refer to Chapter 2, p. 17 for a detailed discussion of each key practice. Refer to Appendix E, p. 91 for an overview of the SA-CMM appraisal process with typical questions directed at the key practices.



Activity 1

- Project teams should consider risk information when developing software acquisition strategies and plans.
- The output of risk identification should be tangible risk statements and supporting context information.
- Everyone on a project should be responsible for identifying risks.
- The output of risk analysis should be a prioritized list of the project's risks (i.e., a top N list).
- Personnel who have the appropriate knowledge, expertise, and background to effectively deal with risk information should be responsible for evaluating, classifying, and prioritizing the risks.
- The output of risk planning should be appropriate plans (i.e., research plan, acceptance rationale, tracking requirements, or mitigation plan) for the most important risks (i.e., the top N risks).
- Personnel who have the knowledge, expertise, background, and resources to effectively deal with risks should be responsible for developing their plans.
- Risk identification, analysis, and planning should be performed early in a project's life cycle to help the project team to develop its software acquisition strategy.

Activity 2

- A project team's Software Acquisition Risk Management Plan should define how the risk management process will be applied to the project.
- The Software Acquisition Risk Management Plan should be based on the project's defined acquisition process.
- The Software Acquisition Risk Management Plan should be tailored for the particular processes, methods, and tools used by the project team; it can be part of the system-level risk management plan, part of the project management plan, or a stand-alone plan.
- The minimal content for a risk management plan should include
  - introduction - defines the purpose and scope of the risk management plan
  - overview of processes - describes all risk management activities and their relations to other project management activities (see Activity 1, p. 22, and Activity 5, p. 33)
  - organization - defines project personnel responsibilities (see Commitment 2, p. 38) as well as customer, supplier, and co-developer responsibilities
  - process details - describes the processes and procedures for systematic risk management
  - resources and schedule - documents the resources (e.g., cost, staff effort, equipment, software) required for the risk management process (see Ability 2, p. 40)
  - risk documentation - defines project templates and forms, database tool specifications, and procedures and requirements for documentation
- The current list of risks and their mitigation plans should be maintained and updated separately from the risk management plan.

Activity 3

- The project team should follow the Software Acquisition Risk Management Plan.

Activity 4

- The project team should integrate acquisition risk management into all of its activities.
- The contract type should be chosen based on perceived risk.
- The project team should identify, analyze, plan, track, and control risks during Project Performance Management activities.
- The project team should identify the risks associated with the contractor's activities.
- The project team and contractor(s) should enter into a teaming relationship where risks are identified, analyzed, planned, tracked, controlled, and communicated in a shared environment.

Activity 5

- Project teams should determine whether plans are being executed properly and reducing risk by gathering and examining the risk metrics that are defined during risk planning.
- The output of risk tracking should be documents or presentations highlighting the relevant tracking data.
- Tracking should be performed by the person(s) responsible for tracking watched and mitigated risks.
- The output of risk control should be decisions (i.e., replan, close the risk, invoke a contingency plan, or continue tracking and executing the current plan) which are then implemented by project personnel.
- The person who has accountability for a risk should make the control decision for that risk.
- Risk reporting should be combined with routine project management activities (e.g., as part of a weekly or monthly project status update) to provide the project team with more information to use when making project decisions.

Commitment 1

- The acquisition organization should have a written policy on software acquisition risk management.
- The policy should include
  - a discussion of the importance of identifying risks throughout the acquisition
  - a discussion of inter-organizational risk management activities, including how the project team, contractor(s), and end user(s) are involved in risk management activities
  - how risk information is communicated
  - designation of responsibility at the acquisition organization level (see Commitment 2, p. 38)
  - a clear statement validating acquisition risk management as a positive and proactive part of software acquisition

Commitment 2

- Responsibility for software acquisition risk management activities should be formally designated at both the acquisition organization and project levels.
- Projects should document roles and responsibilities in the Software Acquisition Risk Management Plan (see Activity 2, p. 25).
- At the acquisition organization level, responsibility should be designated in the policy statement (see Commitment 1, p. 37).

Ability 1

- The acquisition organization should ensure that adequate personnel are available to each project to perform the acquisition risk management activities.

Ability 2

- The acquisition organization should ensure that projects have adequate funding, staff, equipment, and tools to perform acquisition risk management activities.
- Resources required to perform the software acquisition risk management functions should be documented in the Software Acquisition Risk Management Plan and should be updated as necessary throughout the project to reflect changing needs.

Ability 3

- The acquisition organization should provide knowledgeable personnel to project teams to perform acquisition risk management activities.
- A written plan (e.g., the project's Training Plan) should specify the risk management training required for project personnel and should specify the training schedule.

Measurement 1

- The project team should measure the process and work products to determine the status of the acquisition risk management activities.
- The project team should use the results of measurements as a basis for project management and acquisition organization management verifications (see Verification 1, p. 45, and Verification 2, p. 46)

Verification 1

- The project team should present the results of the acquisition risk management activities to acquisition organization management at periodic program reviews.
- The project team should present the status of the project's top risks and mitigation plans.
- The project team should present data that indicate the effectiveness of the acquisition risk management process (e.g., rate of identification versus rate of mitigation).

Verification 2

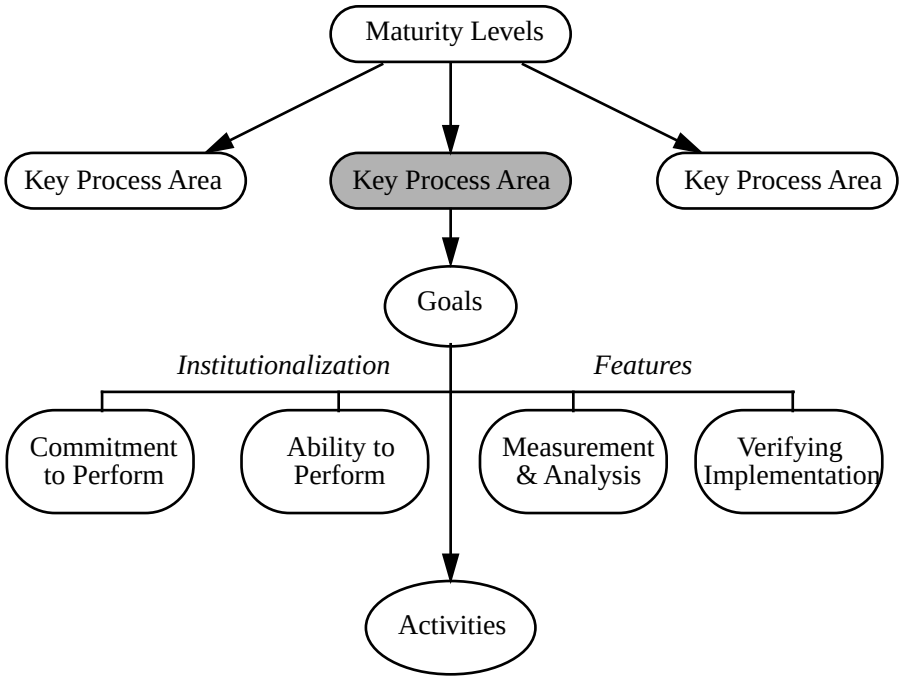
- The project manager should review and participate in the acquisition risk management activities.

Chapter 2

Acquisition Risk Management KPA

Overview

This chapter provides a detailed discussion of the Acquisition Risk Management KPA. Each component of the KPA is analyzed and expanded and includes examples and further definition. Finally, the concept of managing risk with other organizations is explored. The Acquisition Risk Management KPA identifies risk management issues which must be addressed by an acquisition organization to satisfy the defined maturity level of the SA-CMM. It includes the goals, institutionalization features, and activities required to implement risk management in an acquisition organization.



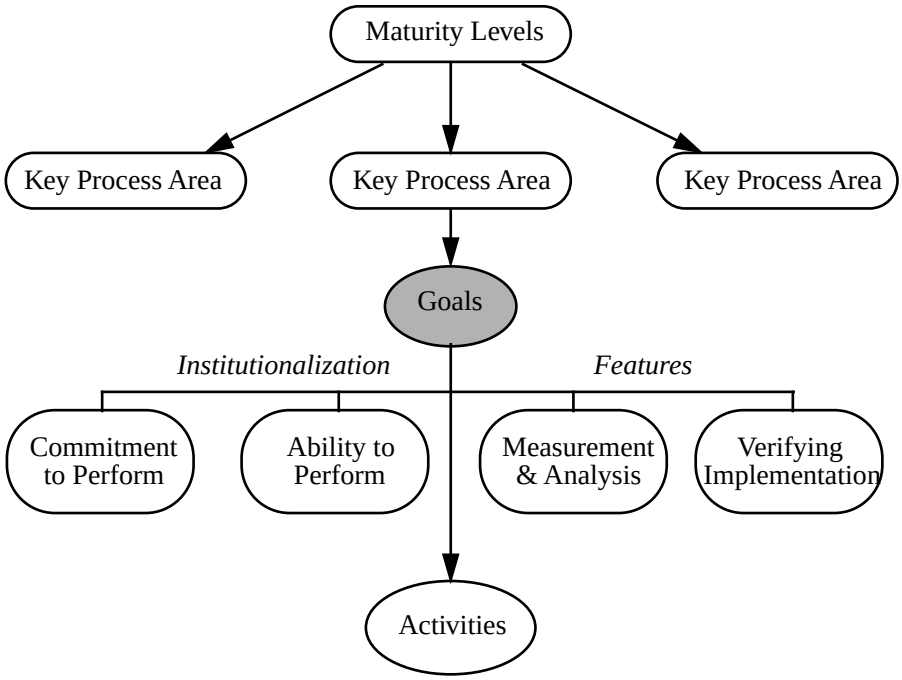
Section

Section 1

Goals

Definition

The acquisition risk management goals indicate the result that will be achieved by effective implementation of the institutionalization features and activities of a key process area. The goals highlight both the scope and the intent of the acquisition risk management key process area.



Section

Section 1.1

Goal 1

Goal 1

Software acquisition risk management is an integral part of the project's defined software acquisition process.

Description

In the defined maturity level of the SA-CMM (Level 3), the acquisition organization's software acquisition process is standardized. The process is then tailored and defined for each project in the organization. At Level 3, both project management and contract management activities are proactive in nature [Ferguson 96]; the objective is to address issues before they become problems. Risk management is a way to identify potential problems and take action to prevent the problems from occurring. It is a proactive process that is integral to a project's defined software acquisition process.

Objective

The objective of Goal 1 is for project personnel to proactively manage risk as part of the project's defined software acquisition process. Effective risk management requires a systematic process for managing risk, domain experience and expertise of the project personnel, a repository of risk data, and a risk-aware culture. When effective risk management is employed on a project, management of the project becomes proactive, and potential problems are identified and addressed early [Charette 89].

Managing Risk in the Acquisition Process

Risk must be managed from the earliest phases of an acquisition until the acquisition has been completed. This includes all pre-development activities, development activities, and post-development activities of a software acquisition. The project team should incorporate risk when developing the program plan, the acquisition strategy, the solicitation, and the source selection plan as well as when evaluating proposals and selecting a developer. After a contractor has been selected, the project team will normally manage the high-level or project risks, while the developer will manage the risks related to product development and the development process. In many cases, the project team and its developers can work together to cooperatively manage risk; this can be the most effective way to manage risk on a project [Gluch 95]. Finally, during post-development activities, such as transitioning a system to maintenance and support, the project team must also be sure to continuously manage risk while performing its tasks.

Section 1.2

Goal 2

Goal 2

The project identifies and deals with risk in a positive manner, such that identification is recognized and rewarded, and results in effective risk handling.

Description

Often, project management is not proactive about identifying and addressing potential problems. Consequently, managers do not encourage project members to identify risks. The assumption is that everything will progress according to plan, and there are no contingency plans available when things do go wrong [Charette 89]. Personnel on projects where risk is systematically managed do identify risks which could jeopardize those projects. The risks can then be proactively addressed and mitigated. Managers must deal with risk information in a positive manner and reward those who identify risks to sustain and reinforce this type of behavior in their organizations [Dorofee 96]. This is done by establishing a culture where risks are identified and addressed as a part of everyday business.

Objective

Effective risk management requires a systematic process for managing risk, domain experience and expertise of the project personnel, a repository of risk data, and a risk-aware culture. The objective of Goal 2 is to establish a culture in which risk information is openly shared and where risks are proactively addressed. This can involve modifying an organization's present culture to create and sustain an environment that enhances risk communication and removes the barriers to it.

Risk Communication

Risk communication deals with uncertainty and negative consequences, which are two subjects that most people have difficulty discussing. Communication is essential for managing risks within an organization. Risk communication must allow a free flow of information within and between all project levels, value the individual voice, and preserve non-attribution and trusted use of data. If done successfully, it will surface relevant issues and potential problems on a project, and as a result, project personnel will feel that they are informed [NRC 89].

Enablers of Risk Communication

Management is instrumental in establishing and sustaining an environment that encourages risk communication. The following list includes a few of the environmental and cultural traits that can help to enhance risk communication in an organization:

- establishing upper management sponsorship of risk management
- rewarding positive behavior
- making risk actions and decisions visible to project members
- setting an example by being a role model
- selecting a risk management advocate within the organization to help sustain the motivation for risk management

Barriers to Risk Communication

While management must establish an environment that enhances risk communication, it must also work to remove the barriers that discourage risk communication. The following list includes a few of the environmental and cultural traits that can help to inhibit risk communication in an organization:

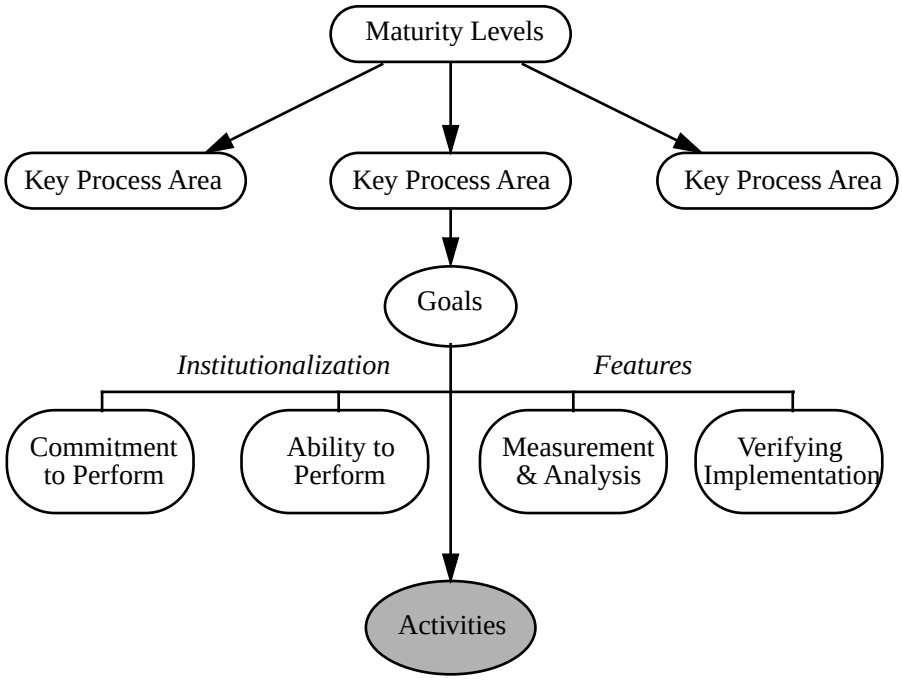
- failing to establish upper management sponsorship of risk management
- providing a solution before a problem is understood
- blaming project members who identify issues or problems
- executing "hidden agendas"
- lacking trust in other project members

Section 2

Activities Performed

Definition

The acquisition risk management activities are the steps taken or functions performed, either mental or physical, toward achieving the KPA goals. Activities include all of the work that the managers and technical staff do to perform the tasks of the project or organization.



Section

Section 2.1

Activity 1

Activity 1

Software acquisition risk management activities are integrated into software acquisition planning.

Description

The risk-related information generated by a project's risk management process is used when developing software acquisition strategies and plans. Software acquisition planning involves preparing the strategies and plans for the software-related areas of an acquisition project. After risks are identified, the project team can proactively incorporate the risk mitigation plans into its strategies and plans and can address the risks long before they become problems.

Objective

The objective of Activity 1 is for project teams to consider risk information when developing software acquisition strategies and plans. Effective risk management enables proactive project management, allowing a project team to identify and address potential problems early in the acquisition process. Potential problems can be addressed while a project team is formulating its acquisition strategy and generating its acquisition plan.

What is Software Acquisition Planning?

Software acquisition planning involves preparing the strategies and plans for the software-related areas in system-level planning (e.g., budgetary action, schedule determination, acquisition strategy, software requirements definition, and risk identification, analysis and mitigation planning) [Ferguson 96]. It ensures that a reasonable planning effort is performed for the software acquisition and that all elements of the project are considered when developing the plan. All planning activities are performed and documented, and participation in system-level planning activities is included as appropriate. Software acquisition planning begins when reasonable resources are assigned to form an acquisition project team, independent of whether the team is formally established as an organizational entity.

Relationship of Risk Management to Software Acquisition Planning

The SEI risk management paradigm is a process that can be used to manage risk on an acquisition project. It consists of the following functions: identify, analyze, plan, track, control, and communicate (see Appendix C, p. 71, for methods and tools). When a project team performs risk identification, analysis, and planning early in a project's life cycle, it can use the information as it develops the software acquisition strategy. After the need for the system has been established, the project team, users, and other appropriate personnel can identify risks, analyze and prioritize the risks, and develop mitigation plans for the most important risks. The project team can then incorporate the mitigation plans into its acquisition strategy and plan.

Note: Communication is a vital part of the risk management paradigm. Most of the methods and tools used in risk management require communication among project team members, users, and other personnel involved in the process

Acquisition Planning Example

A project team intends to acquire a system which pushes the envelope of current technical knowledge. A risk concerning the lack of foundational work in the technical area was identified. The mitigation plan for this risk calls for an incremental development approach, where the first stage is the development of a rapid prototype for proof of concept. The acquisition strategy is modified to the incremental approach because of the assessment that conventional approaches might fail.

Risk Identification, Analysis, and Planning

Activity 1 incorporates risk identification, analysis, and planning into a project's software acquisition strategy and plan. Identification produces tangible risk statements as well as supporting context information. Everyone on a project is responsible for identifying risks. Analysis produces a prioritized list of the project's risks (i.e., a top N list). Personnel who have the appropriate knowledge, expertise, and background to effectively deal with risk information are responsible for evaluating, classifying, and prioritizing the risks. Planning produces appropriate plans (i.e., research plan, acceptance rationale, tracking requirements, or mitigation plan) for the most important risks (i.e., the top N risks). Personnel who have the knowledge, expertise, background, and resources to effectively deal with risks are responsible for developing their plans.

Note: Detailed information about risk identification, analysis, and planning can be found in Chapter 1 p. 1, and information about the methods and tools that support identification, analysis, and planning can be found in Appendix C, p. 71.

Baseline Risk Identification and Analysis

Baseline risk identification and analysis is a process that establishes a baseline set of risks early in a project. It is a concentrated effort using many of the identification and analysis tools listed in Appendix C, p. 71, to capture and assess all of the risks that are presently known by project personnel. The selection of methods and tools used during this process is driven by the project's needs and goals. The output of baseline risk identification and analysis is multiple sets of related risks (also referred to as risk areas or mitigation areas). Baseline risk planning typically follows baseline risk identification and analysis.

Baseline Risk Planning

Baseline risk planning is a process that develops integrated mitigation plans for the multiple sets of related risks that are captured during baseline risk identification and analysis. It is a concentrated effort using many of the planning tools listed in Appendix C, p. 71, to develop mitigation plans for the most important risk sets. The priority of sets and individual risks, as determined by the project team, drives how much planning is done. Risks and risk sets that are not considered to be a priority are either accepted or watched. The selection of methods and tools used during this process is driven by the project's needs and goals.

Note: It is important to build baseline mitigation plans as soon as possible after performing baseline identification and analysis.

Relationship of Risk Baselines to Software Acquisition Planning

Performing baseline identification and analysis and baseline planning early in a project's life cycle can help the project team to develop its software acquisition strategy. After the need for the system has been established, a baseline can be generated with participation from the project team, users, and other appropriate personnel. The output of this process will be integrated mitigation plans for the highest priority risks and risk sets. The project team can then incorporate the mitigation plans into the project's acquisition strategy and plans.

Recommendations for Activity 1

- Project teams should consider risk information when developing software acquisition strategies and plans.
- The output of risk identification should be tangible risk statements and supporting context information.
- Everyone on a project should be responsible for identifying risks.
- The output of risk analysis should be a prioritized list of the project's risks (i.e., a top N list).

- Personnel who have the appropriate knowledge, expertise, and background to effectively deal with risk information should be responsible for evaluating, classifying, and prioritizing the risks.
- The output of risk planning should be appropriate plans (i.e., research plan, acceptance rationale, tracking requirements, or mitigation plan) for the most important risks (i.e., the top N risks).
- Personnel who have the knowledge, expertise, background, and resources to effectively deal with risks should be responsible for developing their plans.
- Risk identification, analysis, and planning should be performed early in a project's life cycle to help the project team to develop its software acquisition strategy.

Section 2.2

Activity 2

Activity 2

The Software Acquisition Risk Management Plan is developed in accordance with the project's defined software acquisition process.

Description

At the Defined Level of the SA-CMM (Level 3), the acquisition organization's standard software acquisition process is integrated into each project. The project's defined process is tailored from the acquisition organization's process, addressing specific characteristics of the project [Ferguson 96]. The management plans for a project are based on the project's defined acquisition process, and the risk management plan is one of the project's management plans. A project's Software Acquisition Risk Management Plan (also referred to as the risk management plan) documents how risks will be managed on the project. It includes the processes, activities, milestones, and responsibilities associated with risk management.

Objective

The objective of Activity 2 is for a project team to define how the risk management process (see Chapter 1, p. 1) will be applied to the project. This is achieved by developing the Software Acquisition Risk Management Plan [Charette 89], which is based on the project's defined acquisition process. The risk management plan documents the process that will be used to identify and address potential problems early in the acquisition.

Risk Management Plan

The Software Acquisition Risk Management Plan should be tailored for the particular processes, methods, and tools used by the project team. Managers have latitude to structure the document to suit their needs [DSMC 89]. The following table lists the minimal recommended content for a risk management plan [Dorofee 96]:

Part	Description
Introduction	The introduction defines the purpose and scope of the plan as well as the content that can be found in the Software Acquisition Risk Management Plan. Any assumptions, constraints, and policies for implementing the processes as well as any related plans, documents, and standards are also found here.
Overview of processes	The overview of processes describes the risk management activities and how they are related to each other; provides all process and data flows; and describes how the risk management activities are integrated with other project management activities.

Part	Description
Organization	The organization section of the Software Acquisition Risk Management Plan includes information about • project organization and responsibilities • customer responsibilities • supplier responsibilities • co-developer responsibilities This information includes: a description of the project organization; an organization chart that maps risk management activities to project roles and management responsibilities (see Commitment 2, p. 38); and a list of the risk management responsibilities, activities, and products expected from customers, suppliers, and co-developers.
Process details	The process details describe the processes and procedures required for systematic risk management (see Chapter 1, p.1, Activity 1, p. 22, and Activity 5, p. 33). This part of the Software Acquisition Risk Management Plan also includes • the methods and tools that are chosen to support each function as well as the criteria for selecting one method or tool over another • references to other plans, handbooks, and training materials for any method or tool that is documented elsewhere (e.g., in the project's, organization's, or customer's related materials) • all process improvement metrics that must be collected and reported (e.g., the number of risks open, the risks' classifications, the number of successful mitigations, the number of failed mitigations, etc., see Measurement 1, p. 43). • the process required to evaluate and improve the risk management process (e.g., a quarterly evaluation of the methods for their efficiency, a periodic review of customer reports assessing their usefulness, etc.)
Resources and schedule	The resources and schedule section documents the resources (e.g., cost, staff effort, equipment, software) required for the risk management process. The allocated budget as well as the source of mitigation funds are also specified (see Ability 2, p. 40). A mapping of risk management activities against the project schedule and milestones is included in this section of the risk management plan. All risk management-related deliverables, such as risk summary reports, baseline results, mitigation plans, etc., are also documented here.

Part	Description
Risk documentation	Risk documentation defines the database tool specifications, including access to, control of, and management of databases. Any templates or forms that are required should be either included in this part of the plan or referenced appropriately. All procedures and requirements for completing, processing, controlling, and retaining risk-related documents and forms should also be provided here.

Current List of Risks and Mitigation Plans

The current list of risks and their mitigation plans can be included in the Software Acquisition Risk Management Plan. If the project team continuously manages acquisition risks, then it could be faced with an administrative burden as it continually updates the risk management plan to reflect changes to the list. It is recommended that the current list of risks and their mitigation plans be maintained and updated separately from the risk management plan.

Tailoring a Risk Management Plan

The method used by a project team to document the Software Acquisition Risk Management Plan is ultimately determined by the project team and the acquisition organization. The risk management plan should be tailored for the processes, methods, and tools used by the project team; it can be part of the system-level risk management plan, part of the Project Management Plan (see the Project Performance Management KPA of the SA-CMM), or a stand-alone plan. The factors that can affect how a project team decides to construct the risk management plan include: the size of the project, how the acquisition organization does business, the complexity of the project, and the composition and size of the project team. The Software Acquisition Risk Management Plan does not have to be any more extensive than the risk management plans developed by well-managed software acquisition projects [Ferguson 96].

Recommendations for Activity 2

- A project team's Software Acquisition Risk Management Plan should define how the risk management process will be applied to the project.
- The Software Acquisition Risk Management Plan should be based on the project's defined acquisition process.
- The Software Acquisition Risk Management Plan should be tailored for the particular processes, methods, and tools used by the project team; it can be part of the system-level risk management plan, part of the Project Management Plan, or a stand-alone plan.
- The minimal content for a risk management plan should include
  - introduction - defines the purpose and scope of the risk management plan
  - overview of processes - describes all risk management activities and their relations to other project management activities (see Activity 1, p. 22, and Activity 5, p. 33)
  - organization - defines project personnel responsibilities (see Commitment 2, p. 38) as well as customer, supplier, and co-developer responsibilities
  - process details - describes the processes and procedures for systematic risk management
  - resources and schedule - documents the resources (e.g., cost, staff effort, equipment, software) required for the risk management process (see Ability 2, p. 40)
  - risk documentation - defines project templates and forms, database tool specifications, and procedures and requirements for documentation
- The current list of risks and their mitigation plans should be maintained and updated separately from the risk management plan.

Section 2.3

Activity 3

Activity 3

The project team performs its software acquisition risk management activities in accordance with its documented plans.

Description

The management plans for a project are based on the project's defined acquisition process. The Software Acquisition Risk Management Plan, which is one of the project's management plans, can be part of the system-level risk management plan, part of the Project Management Plan, or a stand-alone plan. The format of the plan is determined by the project team and the acquisition organization. Once the Software Acquisition Risk Management Plan has been formally documented, project personnel must perform their risk management activities (e.g., identifying risks, analyzing risks, etc.) as described in the plan.

Objective

The objective of Activity 3 is for a project team to follow the Software Acquisition Risk Management Plan. Following the risk management plan is important because it enables project personnel who are responsible for a task or activity to perform it in a repeatable way. Following the plan also helps other personnel who have general knowledge of the area to learn and perform the task or activity as outlined in the plan. In addition, people who depend on the consistency of the results can be satisfied. This is one aspect of institutionalizing a process [Paulk 95].

Example of Modifying a Risk Management Plan

A project team has developed a Software Acquisition Risk Management Plan and is following the plan as it manages project risks. Project team members learn about a new risk tracking tool that they would like to incorporate into the team's risk management process. They modify their risk management plan to reflect the use of the new tracking tool, and they also include the criteria that were used to select the tool in the risk management plan.

Recommendations for Activity 3

- The project team should follow the Software Acquisition Risk Management Plan.

Section 2.4

Activity 4

Activity 4

Risk management is conducted as an integral part of the solicitation, project performance management, and contract performance management processes.

Description

Software acquisition risk management is performed as an integral part of the project team's activities. The project team considers data collected from software acquisition risk management activities when making decisions. This focus on "what could go wrong" is the major factor in helping a project team shift from reacting to problems as they arise to anticipating and avoiding problems.

Objective

The objective of Activity 4 is to ensure that software acquisition risk management is integrated into the way a project team manages the project. Risk management isn't just conducted during "risk week" or during a concentrated effort to write a risk management plan. Software acquisition risk management has a role in all activities of the project team.

Solicitation

During solicitation, the project team prepares a solicitation package and selects a contractor who is best capable of satisfying the requirements of the contract. The contract type (e.g., fixed-price, cost-reimbursement) and the acquisition approach (e.g., incremental acquisition, prototyping) should be chosen based on the risk of not meeting the requirements of the acquisition within cost and schedule constraints. The project team may consider asking the contractor to submit a software risk management plan in response to the solicitation [Ferguson 96].

Solicitation Example

A project team is acquiring software to control a robot that will be used to explore hazardous terrain. Based on the operational requirements, the robot must be autonomous rather than controlled by teleoperation or remote control. The software to allow a robot to operate completely autonomously is extremely complicated and may even be beyond current technical capability. Given the uncertainty of the technical solution and the risk of failure, the project team selects a cost-plus incentive fee contract type and requires an incremental development approach as a part of their risk mitigation strategy.

Project Performance Management

At Level 3 of the SA-CMM, the project team manages the software acquisition project according to a defined software acquisition process. The Project Management Plan addresses all of the project team's management planning, including risk management planning (see Activity 2, p. 25, for a discussion of the Software Acquisition Risk Management Plan). The project team applies a systematic approach while they identify and analyze risks and plan risk handling (risk mitigation) actions (see Activity 1, p. 22 and Activity 5, p. 33) [Ferguson 96].

Contract Performance Management

During contract performance management, the project team uses a defined contract management process to ensure the acquired software products and services satisfy contract requirements. Risk analysis and management is performed by the project team as an integral part of contract performance management. The project team follows its plans, which include risk management. The project team appraises the contractor's risk management system and measures the risk analysis process [Ferguson 96]. The project team also ensures that the contractor is managing risk as outlined in the contract as well as in the contractor's risk management plan.

Managing Risk with Contractors

Contractors play an important role in managing software acquisition risks. Project teams can't simply transfer risk to the contractor after contract award. The project team

is ultimately responsible for the success of the project and is primarily responsible to ensure that risks are identified and mitigated. The project team and contractor(s) should enter into a teaming relationship where risks are identified, analyzed, planned, tracked, controlled, and communicated in a shared environment (see Section 4, Managing Risk with Others, p. 47). The effectiveness of joint mitigation strategies is greater than the sum of individual, potentially diverse, contractor and project team risk handling plans.

Risk Management at Level 2

Even though acquisition risk management isn't defined as a KPA until Level 3 of the SA-CMM, project teams begin to perform basic risk management as an integral part of Level 2 activities. The following chart shows where risk management is performed at Level 2.

Level 2 KPA	Key Practice	Risk-Related Function
Software Acquisition Planning	Commitment 1	Written policy typically includes a review process for resolving issues that focus on critical areas such as affordability and risk.
	Activity 2	Risk identification is a part of the software acquisition strategy development.
	Activity 3	Risk identification and tracking is documented in software acquisition planning.
Solicitation	Commitment 1	Contract type is chosen based on perceived risk.
	Activity 1	Offeror may be asked to submit a risk management plan with its response to the solicitation.
Requirements Development and Management	Activity 4	Changes are analyzed for risk.
Project Management	Activity 1	Risk identification and tracking are performed according to plans.
Contract Tracking and Oversight	Activity 2	Contractor's Software Acquisition Risk Management Plan is reviewed if applicable.
Evaluation	Commitment 1	Acquired software products and services are evaluated with intent of reducing acquisition risk.
	Activity 1	Plans describe the risks addressed by the evaluation.
	Activity 5	Independent evaluations may be performed to further reduce risk of failure.

Risk Management at Level 3

Acquisition risk management resides at Level 3 of the SA-CMM. It's the high-leverage KPA that helps a project change its focus from being reactionary to proactively managing the project. The following table identifies all areas of Level 3 where risk management is performed.

Level 3 KPA	Key Practice	Risk-Related Function
Project Performance Management	Activity 2	The Project Management Plan addresses risk management planning.
	Activity 10	The project team identifies and analyzes risks and identifies handling actions.
Contract Performance Management (CPM)	Commitment 1	Risk analysis and management is done as a part of CPM activities.
	Activity 1	CPM plans include risk management.
	Activity 2	The contractor's risk management system is appraised.
	Measurement 1	Risk analysis process is measured.
Acquisition Risk Management (ARM)	Commitment 1	Written policy for software ARM exists.
	Commitment 2	Responsibility for performing ARM activities is designated.
	Ability 1	A group exists to coordinate ARM.
	Ability 2	Adequate resources are provided to do ARM.
	Ability 3	Individuals doing ARM have experience or training.
	Activity 1	Software ARM is integrated into software acquisition planning.
	Activity 2	Software ARM Plan is developed.
	Activity 3	ARM Plan is followed.
	Activity 4	ARM is integrated with other KPAs.
	Activity 5	Risks are tracked and controlled until mitigated.
	Measurement 1	The statuses of ARM activities and products are measured.
	Verification 1	ARM activities are reviewed by acquisition organization management.
	Verification 2	ARM activities are reviewed by project manager.

Risk Management at Levels 4 and 5

At the higher maturity levels of the SA-CMM, the project team sets quantitative quality objectives for processes, products, and services. The acquisition organization is focused on continuous process improvement. The following tables show how the project team and acquisition organization integrate software acquisition risk management into their activities.

Level 4 KPA	Key Practice	Risk-Related Function
Quantitative Acquisition Management	Activity 1	Risk management practices are integrated with quantitative methods.
	Activity 2	Quantitative process and product measures are used to track risk management practices.

Level 5 KPA	Key Practice	Risk-Related Function
Acquisition Innovation Management	Commitment 1	Policy describes how new techniques and technologies are evaluated for risk.

Recommendations for Activity 4

- The project team should integrate acquisition risk management into all of its activities.
- The contract type should be chosen based on perceived risk.
- The project team should identify, analyze, plan, track, and control risks during Project Performance Management activities.
- The project team should identify the risks associated with the contractor's activities.
- The project team and contractor(s) should enter into a teaming relationship where risks are identified, analyzed, planned, tracked, controlled, and communicated in a shared environment.

Section 2.5

Activity 5

Activity 5

Software acquisition risk handling actions are tracked and controlled until the risks are mitigated.

Description

Mitigation plans (risk handling actions) are developed for the most important risks to the project. The project team must track both the progress of a plan and its effectiveness in reducing the risk to the project. As project personnel track data, they must make "control decisions." For example, if the mitigation is working as intended, then the decision would be to continue with the mitigation plan. If there is a problem with the mitigation plan, then a new plan might be required or a contingency plan might be implemented. If the mitigation plan is judged to be successful, then the risk can be closed. In general, risk tracking and control includes tracking the status of mitigation actions against the mitigation plan; tracking the effectiveness of the mitigation plan; reporting tracking data to the appropriate decision makers; replanning a mitigation plan or invoking a contingency plan when necessary; and periodically reviewing data about the statuses of risks and their plans.

Objective

The objective of Activity 5 is for project teams to know if a mitigation plan is being executed as it was designed and to understand whether a mitigation plan is effectively reducing risk to the project. By gathering and examining the metrics that are defined during risk planning, project personnel can determine whether a plan is being executed properly and reducing risk. They can then take appropriate actions based on the analysis of the data. This helps to ensure that risk mitigation plans effectively reduce risk to the acquisition.

Risk Tracking and Control

Activity 5 focuses on tracking and controlling mitigation plans until the risks are mitigated. Tracking produces reports (e.g., documents or presentations) highlighting the relevant tracking data. The person(s) who is assigned responsibility for tracking watched and mitigated risks prepares the reports. Control produces decisions (i.e., replan, close the risk, invoke a contingency plan, or continue tracking and executing the current plan) which are then implemented by project personnel. The person who has accountability for a risk should make the control decision for that risk.

Note: Detailed information about risk tracking and control can be found in Chapter 1 of this guidebook (see Section 1.2, Identify, Analyze, Plan, Track, Control, and Communicate, p. 6) and information about the methods and tools that support tracking and control can be found in the appendices (see Appendix C, p. 71).

Risk Reporting

Risk reporting should be combined with routine project management activities (e.g., as part of a weekly or monthly project status update). Risk data provides more information that decision makers can use when making decisions. The frequency of reporting can depend upon

- the reporting requirements for each risk or risk set as outlined during planning (e.g., weekly or bi-weekly)
- the manner in which the report will be used

Note: A critical event or condition might require that information be reported to a decision maker immediately rather than waiting for the next reporting period.

Control Decisions

The following table describes the control decisions that can be made for risks.

Component	Description
Replan	Replanning is required when analysis of the data shows that the mitigation plan is not working and a contingency plan is not available.
Close the risk	Closed risks are not tracked because the risks no longer exist or are not cost-effective to track. This occurs when • the probability or impact have been reduced below a defined threshold • the risk has become a problem and is now tracked as such *Note*: All closed risks should be documented along with the rationale for closure. Closure of a risk requires the agreement of all affected parties.
Invoke a contingency plan	Contingency plans are alternative plans developed ahead of time. They are invoked when the data indicates that a plan is not working. Risks as well as their mitigation plans continue to be tracked after the contingency plan has been executed.
Continue tracking and executing the current plan	When the analysis of the tracking data indicates that all is going as expected, the decision maker can decide to continue tracking the risk or mitigation plan as before.

Tracking and Control vs. Project Management

Risk tracking and control should be closely related to standard project management monitoring techniques used by the acquisition organization. One of the goals of risk tracking and control is to provide the project team with more information to use when making project decisions. Risk management activities should be integrated and coordinated with existing project management activities for the project team or acquisition organization.

Tracking and Control Example

A project team is acquiring software to use in a product it is developing. Completion of the product might be delayed because of the large number of change requests being submitted by the marketing group. Each change request requires a modification to the contract before it can be implemented, and this process is causing delays in processing and completing the changes. The company could miss its window of opportunity for this product if the release date is delayed. However, it is also important for them to incorporate the changes in order to develop a product that appeals to the marketplace.

The mitigation plan for this risk calls for the product team to negotiate a contract vehicle where a specified amount of resources will be set aside for future changes anticipated during the remainder of the project. As change requests are submitted, contract modifications will no longer be required and resources to implement the changes will be available. The project team chooses to track the resources remaining and the rate of resource consumption for this risk. As the project progresses, an analysis using the rate of resource consumption and the resources remaining indicates that the resources designated for processing and implementing changes will be consumed prior to the end of the project. The project manager decides to negotiate another contract vehicle to set aside additional resources for future changes.

Recommendations for Activity 5

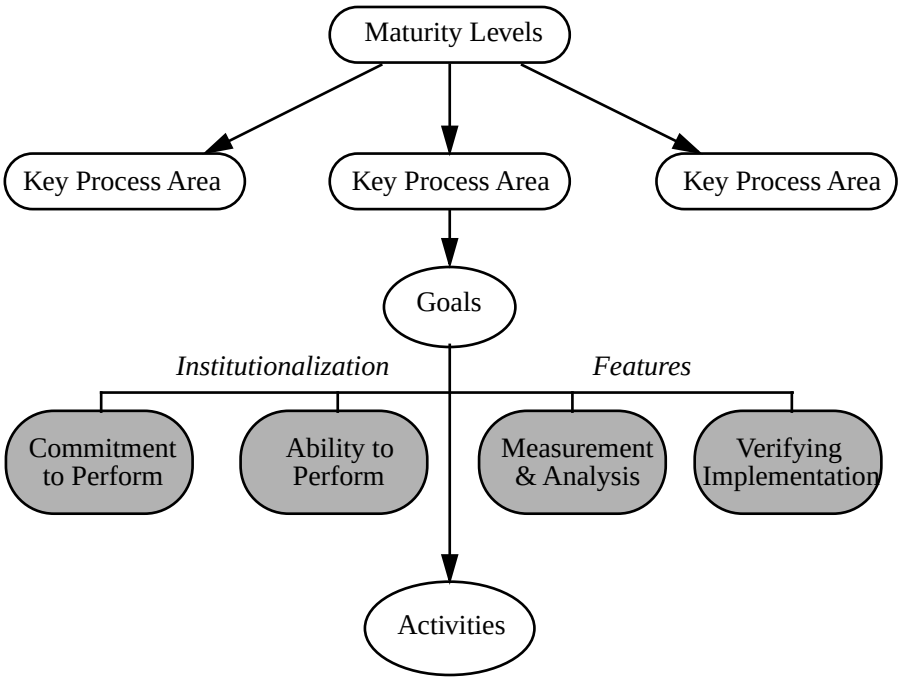
- Project teams should determine whether plans are being executed properly and reducing risk by gathering and examining the risk metrics and that are defined during risk planning.
- The output of risk tracking should be documents or presentations highlighting the relevant tracking data.
- Tracking should be performed by the person(s) responsible for tracking watched and mitigated risks.
- The output of risk control should be decisions (i.e., replan, close the risk, invoke a contingency plan, or continue tracking and executing the current plan) which are then implemented by project personnel.
- The person who has accountability for a risk should make the control decision for that risk.
- Risk reporting should be combined with routine project management activities (e.g., as part of a weekly or monthly project status update) to provide the project team with more information to use when making project decisions.

Section 3

Institutionalization Features

Definition

Institutionalization features are the building blocks for corporate culture and infrastructure. They are critical to successfully implementing the Acquisition Risk Management KPA. They help define common, corporate-wide methods, practices, and procedures that become the ongoing way of doing business. These are defined in such a way that they continue even after those who originally defined them are gone.



Section

Section 3.1

Commitment to Perform

Description

Commitment to Perform describes the actions that the organization must take to establish the process and ensure that it can endure. Commitment to Perform typically involves establishing organizational policies and management sponsorship.

Objective

The objective of the Commitment to Perform institutionalization feature is to visibly communicate a freely-assumed pact that is expected to be kept by all parties. A written policy statement emphasizes the connection between organizational commitment and the activities performed by a project. Management commitment and sponsorship is displayed by designating responsibility and accountability for actions.

Commitment 1

The acquisition organization has a written policy for the management of software acquisition risk.

Description

Commitment 1 requires a written policy at the acquisition organization level describing how projects will perform software acquisition risk management. This policy will apply to all projects and sets the stage for a standardized approach to risk management.

Objective

The objective of Commitment 1 is to communicate the acquisition organization's policy for software acquisition risk management clearly and unambiguously to all current and future members of the organization.

Policy Components

The policy should describe how projects are to identify and manage risks throughout the project life cycle in accordance with the project's defined software acquisition process and should reflect how business is actually conducted. It should include a discussion of how the project team, the end user, and the contractor interact to perform risk management activities. The policy should state that risk management is a proactive and positive part of software acquisition and should describe how risk information is communicated throughout the project team.

Example

The Department of Defense (DOD) recently revised and streamlined its acquisition regulations clarifying mandatory policy and decentralizing acquisition practice [Myers 96]. The resulting documentation is leaner and specifies only key activities that the project manager of a major defense or major information system acquisition must perform. The resulting written, highly-visible policy for acquisition risk management follows:

> *"The PM shall establish a risk management program for each acquisition program to identify and control performance, cost, and schedule risks. The risk management program shall identify and track risk drivers, define risk abatement plans, and provide for continuous risk assessment throughout each acquisition phase to determine how risks have changed. Risk reduction measures shall be included in cost-performance trade-offs, where applicable. The risk management program shall plan for back-ups in risk areas and identify design requirements where performance increase is small relative to cost, schedule, and performance risk. The acquisition strategy shall include identification of the risk areas of the program and a discussion of how the PM intends to manage those risks"* [DOD 96].

An acquisition organization needs a similar, highly-visible statement detailing its policy for software acquisition risk management.

Managing Risk with Others

Acquisition risks extend beyond the project team. The acquisition organization may have multiple projects which interact to mitigate risks of a global nature. A project team may share risk with its contractor(s) to increase the effectiveness of risk handling strategies. Users tend to be a major source of risks with evolving requirements and have an important voice in mitigation options. All of these external groups are vital to successful software acquisition risk management and the policy statement from the acquisition organization should validate their role in the identification, analysis, planning, tracking, control, and communication of risks (see Section 4, Managing Risk with Others, p. 47).

Recommendations for Commitment 1

- The acquisition organization should have a written policy on software acquisition risk management.
- The policy should include
  - a discussion of the importance of identifying risks throughout the acquisition
  - a discussion of inter-organizational risk management activities, including how the project team, contractor(s), and end user(s) are involved in risk management activities
  - how risk information is communicated
  - designation of responsibility at the acquisition organization level (see Commitment 2, p. 38)
  - a clear statement validating acquisition risk management as a positive and proactive part of software acquisition

Commitment 2

Responsibility for software acquisition risk management activities is designated.

Description

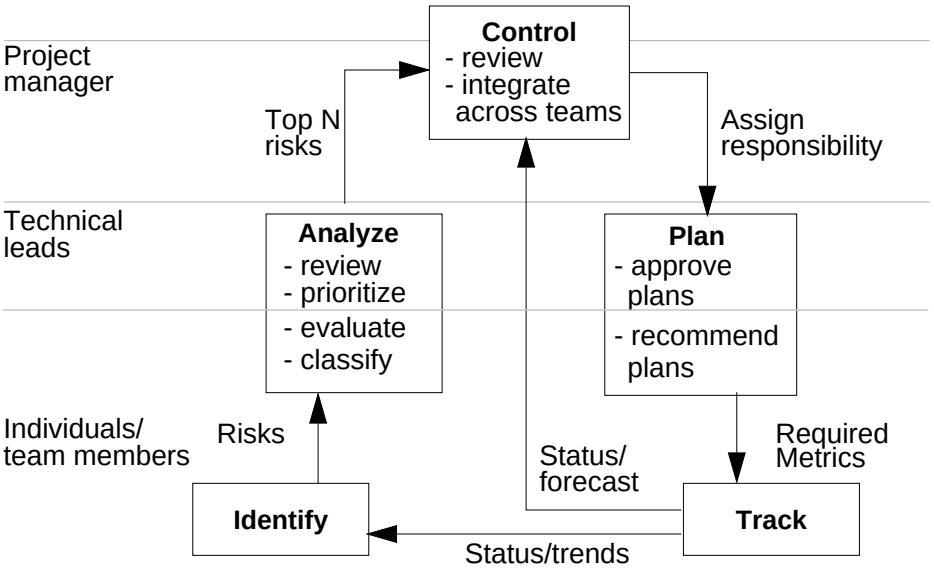
Commitment 2 clarifies the risk management functions by designating responsibility to acquisition organization and project team members.

Objective

The objective of Commitment 2 is to increase the visibility of the software acquisition risk management activities by formally designating responsibility for risk management functions. Each member of the organization should understand their responsibilities clearly and how their risk management activities support the entire process.

Designating Responsibility

Every member of the acquisition organization needs to understand their responsibilities for performing software acquisition risk management. There are many ways an acquisition organization can designate responsibilities and the approach should be based on the needs of the acquisition organization. Fundamental elements are that it should be in writing, all members of the organization should understand their responsibilities, and it needs to reflect how responsibility and accountability are actually designated. Roles and responsibilities are documented in the Software Acquisition Risk Management Plan (see Activity 2, p. 25). The following diagram depicts one way an organization can designate risk management responsibility [Dorofee 96]:



Individuals/ Team Members

In the above example, every individual in the organization is responsible for continuously identifying, evaluating and classifying risks, and recommending mitigation plans. An individual or group may be assigned the responsibility of tracking the status of risks for the project or organization.

Technical Leads

In the above example, in addition to their responsibilities as individuals and team members, technical leads evaluate and classify risks and approve risk mitigation plans.

Project Manager

In the above example, the project manager reviews and integrates risk information, assigns responsibility for risks and mitigation plans, and handles communications external to the project.

Small Projects

A small software acquisition project office may need to designate responsibility differently than the above example. The project manager may have only one level of staff members who double as technical leads and team members. Regardless of how the project designates responsibility for software acquisition risk management, it needs to be in writing.

Recommendations for Commitment 2

- Responsibility for software acquisition risk management activities should be formally designated at both the acquisition organization and project levels.
- Projects should document roles and responsibilities in the Software Acquisition Risk Management Plan (see Activity 2, p. 25).
- At the acquisition organization level, responsibility should be designated in the policy statement (see Commitment 1, p. 37).

Section 3.2

Ability to Perform

Description

Ability to Perform describes the preconditions that must exist in the project or organization to implement the software acquisition process competently. Ability to Perform typically involves resources, organizational structures, and training.

Objective

The objective of the Ability to Perform institutionalization feature is to ensure that the organization has all of the resources, organizational structures, and training required to acquire software. Resources include access to special skills, adequate funding, and tools. Organizational structures are described to ensure that capability exists to perform the KPA. Training can include both formal and informal methods of transferring knowledge to individuals in the organization. Training requirements are identified and provided through the Training Program KPA.

Ability 1

A group that is responsible for coordinating software acquisition risk management activities exists.

Description

Ability 1 ensures that adequate personnel are available to coordinate software acquisition risk management functions.

Objective

The objective of Ability 1 is to ensure that a collection of departments, managers, and individuals exists to perform the acquisition risk management tasks and activities. Clearly identifying a group responsible for coordinating these activities shows organizational commitment beyond a policy statement and communicates the importance of performing acquisition risk management.

What is Meant by Group?

In the SA-CMM, a group may vary from a single individual assigned part-time, to several part-time individuals matrixed from other organizations, to several individuals dedicated full-time. The acquisition organization should define “group” based on the needs of the individual projects. Candidate members of the group could come from the project team, the user community, and the contractor(s).

How to Implement

There are three basic approaches to ensure that a group to coordinate risk management activities exists. In a survey of DOD program management offices, one set of respondents allocated specific positions to coordinate risk management activities while a second set felt that risk management was so integral to project management that separate personnel were not identified [DSMC 89]. A third approach is to identify specific personnel for some of the administrative functions while recognizing that all project personnel must participate in risk management (see Commitment 2, p. 38). Whichever approach is selected, the acquisition organization needs to ensure that personnel accountability decisions are documented.

Recommendations for Ability 1

- The acquisition organization should ensure that adequate personnel are available to each project to perform the acquisition risk management activities.

Ability 2

Adequate resources are provided for software acquisition risk management activities.

Description

Ability 2 requires the acquisition organization to provide adequate resources to perform the software acquisition risk management functions. The required resources are documented in the Software Acquisition Risk Management Plan (see Activity 2, p. 25).

Objective

The objective of Ability 2 is to ensure that the funding, staff, equipment, and tools required to perform acquisition risk management are available to the project. This allows individual projects to successfully implement and maintain a healthy acquisition risk management program that continues throughout the life of the project.

Resources

The following table describes risk management resources:

Resource	Description	Example
Funding	Specific monies may be required to adequately perform acquisition risk management on the project. Funding should be set aside for resources that the project doesn't already have.	The project may want to use a relational database tool to store risk information. Funding should be allocated to procure and support the database tool and associated computer systems.
Staff	Project team members can perform all risk management functions as an integral part of their project duties (see Commitment 2, p. 38). If additional personnel are required to effectively perform the project's defined acquisition risk management process, people should be provided to the project.	A project may need a technical assistant to help coordinate the acquisition risk management activities (see Ability 1, p. 40).
Equipment	Equipment encompasses everything from pencil and paper, dry-erase boards, overheads, and adequate facilities, to computer systems to store and track risk data.	Project team members need to capture risks they identify (see Activity 1, p. 22). The acquisition organization needs to supply personnel with equipment which facilitates and encourages risk identification.
Tools	Tools include a defined process and any system, either manual or automated, allowing project members to perform the risk management functions (see Appendix C, p. 71).	The project may use a time chart or run graph to document the values of risk status metrics over time.

Example

One project actively solicited risk data from project members using a standard risk identification form. Due to inadequate resources, the project manager had no easy way to track the risks and placed them in her filing cabinet. During operational acceptance of the system, a real-time processor couldn't handle the amount of data encountered in the operational environment, requiring a major re-write of the software and an upgrade of the processor. This problem was encountered during operational testing but was identified as a risk early in system-level design. The re-work could have been avoided if the project manager had been given the resources to track and mitigate risks.

Recommendations for Ability 2

- The acquisition organization should ensure that projects have adequate funding, staff, equipment, and tools to perform acquisition risk management activities.
- Resources required to perform the software acquisition risk management functions should be documented in the Software Acquisition Risk Management Plan and should be updated as necessary throughout the project to reflect changing needs.

Ability 3

Individuals performing software acquisition risk management activities have experience or receive required training.

Description

Ability 3 requires that the acquisition organization and each project have individuals who know how to perform software acquisition risk management. At Level 3 of the SA-CMM, training needs of the acquisition organization and project are identified and satisfied by the Training Program KPA.

Objective

The objective of Ability 3 is to ensure that each project has team members performing software acquisition risk management who are competent in software acquisition, risk management, and the problem domain.

Required Knowledge

Team members assigned to perform acquisition risk management functions on a project need to understand the principles of software acquisition, how to perform the acquisition organization's risk management process, as well as the domain or problem space in which the application solution needs to operate. Individuals need to have knowledge in all three areas to successfully contribute to the project.

Obtaining Required Knowledge

The following table describes methods of obtaining required knowledge:

Method	Description
Experience	An individual has the experience required to perform software acquisition risk management if the following is true: the individual has participated in a software acquisition management role on at least one project, has applied risk management techniques on at least one project, and has experience in the domain of the application being acquired [Ferguson 96]. If the individual is lacking in any of the above, he or she should be afforded training in that area.
Formal Training	Formal classroom training is provided by the acquisition organization or a third party. This allows the project members to feel confident in performing their risk management activities.
Informal Training	Informal training may include self-paced courses or on-the-job training (OJT) through the use of a strong mentoring program. *Note:* OJT does not mean that an individual is assigned responsibility and expected to perform. A successful OJT program includes mentors who are responsible for results while trainees learn.

Recommendations for Ability 3

- The acquisition organization should provide knowledgeable personnel to project teams to perform acquisition risk management activities.
- A written plan (e.g., the project's Training Plan) should specify the risk management training required for project personnel and should specify the training schedule.

Section 3.3

Measurement and Analysis

Description

Measurement and Analysis describes the need to measure the process and analyze the measurements. Measurement and analysis typically includes examples of the measurements that could be taken to determine the status and effectiveness of the activities performed.

Objective

The objective of Measurement and Analysis is to collect data which is then used to control and improve the way the acquisition organization and its projects conduct business. The measurements taken should be based on the needs of the projects. Variability in project environments may lead to different measurement needs and approaches. There are currently no universally-accepted measures of software acquisition process or quality [Paulk 95].

Measurement 1

Measurements are made and used to determine the status of the acquisition risk management activities and resultant products.

Description

Measurement 1 requires the project to measure the software acquisition risk management process and the quality of the products produced by the process.

Objective

The objective of Measurement 1 is to focus management attention on the process that the acquisition organization and individual projects use to conduct software acquisition risk management. A process focus allows managers to identify weaknesses in the way they do business and helps them improve the quality of their products by improving the process that produces them.

Measuring the Process

Metrics to monitor the risk management process are defined early in the project's life cycle and are documented in the Software Acquisition Risk Management Plan (see Activity 2, p. 25). A project team may use a top N list to track the highest-priority risks associated with a given phase of the project. Collecting and using risk management process metrics allows the project team to identify weaknesses in how the top N list is developed and maintained and provides the opportunity to improve the way they handle this critical data. Other examples of measurements include [Dorofee 96]

- number of risks open
- number of risks by classification
- trends in risk processing from identification to closure
- number of successful mitigations versus failed mitigations

Note: See Activity 5, p. 33, for a discussion on how the risks themselves are tracked and measured.

Example

One project manager decided to measure which organizations were actively submitting risks for his project, because anecdotal data told him that important operational voices weren't being heard. The results showed that 60% of the risks were identified by the acquisition project team, 38% were identified by the contractor, and only 2% were identified by the operational user. This hard data helped the project manager focus resources on finding a root cause. After a review of the risk identification process, the project manager found that the operational users' organization had imposed a lengthy and stifling process that users had to navigate in order to voice potential problems. The users were so disgusted with the process that they quit formally identifying risks and were waiting to bring up their "issues" during system testing. The users' organization was

quickly trained on the project's defined software acquisition risk management process and encouraged to remove the barriers.

Recommendations for Measurement 1

- The project team should measure the process and work products to determine the status of the acquisition risk management activities.
- The project team should use the results of measurements as a basis for project management and acquisition organization management verifications (see Verification 1, p. 45, and Verification 2, p. 46)

Section 3.4

Verifying Implementation

Description

Verifying Implementation describes the steps to ensure that the activities are performed in compliance with the process that has been established. Verifying Implementation typically encompasses reviews by management.

Objective

The objective of Verifying Implementation is to provide senior management and project management insight into the activities performed by the project team to ensure compliance with the acquisition organization's standard software acquisition risk management process and the project's defined process. Review of these activities by management indicates the importance that the organization places on the acquisition risk management process.

Verification 1

Acquisition risk management activities are reviewed by acquisition organization management on a periodic basis.

Description

Verification 1 requires acquisition organization management (senior management above the project manager) to review acquisition risk management activities on a periodic basis.

Objective

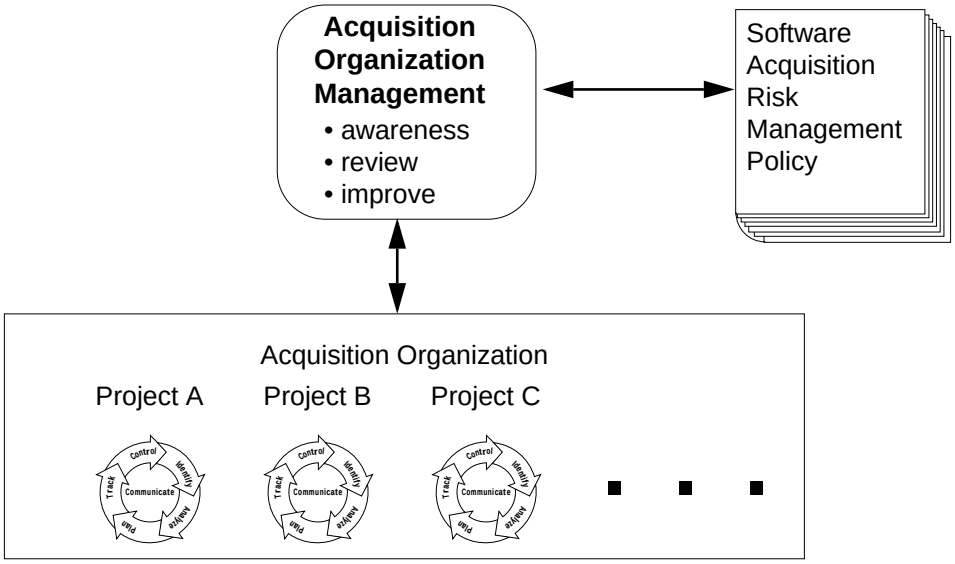
The objective of Verification 1 is to provide awareness of and insight into the software acquisition risk management process activities to senior managers. The information should be communicated at an appropriate level of abstraction and in a timely manner.

Risk Management at the Acquisition Organization Level

The time between reviews for acquisition organization management may be lengthy as long as adequate mechanisms are established for exception reporting. The scope and content may vary depending on what the acquisition organization management wants to see. Anticipate that acquisition organization management will expect different data than the project manager or the same data at a higher level of abstraction (e.g., the project's top risks, rate of risk identification versus mitigation, etc.).

Diagram

The following diagram shows the acquisition risk management process as seen at the acquisition organization level.



Recommendations for Verification 1

- The project team should present the results of the acquisition risk management activities to acquisition organization management at periodic program reviews.
- The project team should present the status of the project's top risks and mitigation plans.
- The project team should present data that indicate the effectiveness of the acquisition risk management process (e.g., rate of identification versus rate of mitigation).

Verification 2

Acquisition risk management activities are reviewed by the project manager on both a periodic and event-driven basis.

Description

Verification 2 requires the project manager to review software acquisition risk management activities both on a periodic and event-driven basis.

Objective

The objective of Verification 2 is to ensure that project managers maintain an ongoing awareness of the status of the software acquisition risk management efforts and receive information when significant events occur.

Risk Management at the Project Level

Oversight at the project manager level varies depending on the characteristics of the project and the needs of the project manager. The key is awareness which comes from participation in formal reviews, such as periodic project management reviews and staff meetings, as well as informal reviews such as real-time status reports and reviews of non-compliance issues. The reviews at the project manager level should be more detailed than those of the acquisition organization management because the project manager takes a more active role in the operational aspects of the project [Paulk 95].

Example

A project manager of a large, software-intensive project has integrated risk management into his project management activities and has replaced periodic program reviews with reviews of risk data. The project no longer spends days pouring over every aspect of the project. Rather, the results of the project's risk management process are reviewed in a proactive approach to project management.

Recommendations for Verification 2

- The project manager should review and participate in the acquisition risk management activities.

Section 4

Managing Risk with Others

Overview

A fundamental principle of acquisition risk management is that you can successfully manage risk only if you are proactive and forward thinking. The practices and goals of the ARM KPA provide mechanisms and techniques that foster this proactive principle. Software acquisition includes acquirer, developer, and user organizations, among others. In a traditional model, acquisition includes two organizations (i.e., an acquiring and a developing organization) or two divisions within the same organization informally contracting for products and services. The users of the acquired software could be part of a third organization. The relationship between the entities is the important aspect with regard to software acquisition risk management. In the simplest scenario, the development organization is usually "contracted" to do the development within certain cost, schedule, and performance parameters dictated by the contract. The acquisition organization traditionally manages the contract and ensures that the requirements for the development are being met. The users provide the requirements for the performance and functionality of the system. Risk management must be performed by all organizations on a continuous basis; it can be performed jointly when risks affect more than one party. When diverse organizations form a team to achieve common goals, the team's effectiveness can be greater than the sum of each organization's individual effectiveness.

Managing Risk with Other Organizations

Managing risk with other organizations depends on systematic and continuous risk management processes in the individual organizations. All organizations must work together to cooperatively manage risk throughout the project's life cycle [Gluch 95]. The result is a disciplined environment for proactive decision-making among two or more organizations. This is accomplished using a structure where personnel from multiple organizations work together to share information about risks that may affect the other organization(s). Creating such a structure requires a common work culture, a common set of motivators, and an emphasis on communication among the organizations.

Deciding to Manage Risk with Other Organizations

Teaming with external organizations to perform risk management activities might require a shift in paradigms. The project team and external groups must work together as a team and it might take time to build trust among personnel from different organizations. A strong and visible statement from a project's sponsor is often required to validate this approach and to encourage the formation of teams at the inter-organizational level (see Commitment 1, p. 37).

Identifying Risks with Other Organizations

Continuous identification of risks is generally left to the individual organizations through the use of their defined risk management process. Risks that are identified by an organization might be appropriately re-worded for an inter-organizational audience. It is also possible for inter-organizational teams to identify risks using techniques tailored from the parent organizations' standard practices.

Analyzing Risks with Other Organizations

Evaluation and classification of risks primarily depends on each organization's risk management process. The main task at the inter-organizational level is to prioritize risks, resulting in a joint list of risks that are most important to the program. A joint list of risks identifies the risks for which mitigation planning must be performed with input from multiple organizations.

Planning Risks with Other Organizations

To the extent possible, planning for all risks should be performed within an organization. In special cases, planning is performed at the inter-organizational level through joint action planning. For joint risks, the inter-organizational team should delegate planning to one of the organizations if possible.

Joint Action Planning

Joint action planning involves sharing data across organizations as well as using expertise and knowledge from all organizations effectively. Risks that are identified by an inter-organizational team require effort from all involved organizations for effective mitigation.

Note: Because joint action planning involves all parties, outside facilitation may be required.

Tracking and Controlling Risks with Other Organizations

The organization with primary responsibility for a risk acquires and compiles tracking data and reports risk and mitigation plan status. Control decisions are made by personnel within the organization responsible for the risk.

Integrated Product Development Teams (IPDTs) and Risk Management

Product development generally requires the specialization and division of activities required to make a product. Integrated product development (IPD) is a model for product development in which activities requiring multiple disciplines are integrated and adapted for the development task. Rapidly changing technology, short development cycles, and the need for various types of expertise required to develop a single product create a need for IPD [Andreasen 85]. As a result, IPD is common in today's product development environments. Applied to the acquisition process, integrated product development teams (IPDTs) comprise team members possessing skills from multiple disciplines who collaborate throughout the acquisition life cycle to develop a system or component of a system. Depending on circumstances, team members might represent a single organization or company, or they might be from different organizations or companies. In either case, an IPDT uses systematic and continuous risk management processes as part of the team's project activities. If an IPDT must interface with other IPDTs as part of a larger development, then all of the IPDTs must work together to cooperatively manage risk throughout the project's life cycle. The result is a disciplined environment for risk management among two or more IPDTs.

IPDT Example

An organization is acquiring engineering and manufacturing information systems as part of an initiative to update its design and production processes. An IPDT was chartered to develop the interface between the engineering and manufacturing systems. This cross-functional IPDT comprised members of the acquisition project team for each system and members of the system engineering and development organizations from each contractor organization. As part of the interface development, the IPDT continuously manages risk. Any risks that affect either the manufacturing or production system development or any other related system development are managed cooperatively with the IPDTs developing those systems.

Summary

Joint events to manage and discuss risks will bring together personnel from different organizations. The benefits of inter-organizational risk management are

- elevation of risks facing a project to a level which allows them to be handled by personnel from all of the involved organizations
- creation of a framework to implement integrated management and continuous process principles
- creation of long-term inter-organizational relationships based on trust

References

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

[Andreasen 85] Andreasen, M. M. & Hein, L. *Integrated Product Development*. Berlin, Germany: IFS (Publications) Ltd, 1985.

[Appleton 96] Appleton, E.L. "Divorce your Outsourcer?" *Datamation 42*, 14 (August 1996): 60-62

[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.

[Bennatan 92] Bennatan, E. M. *On Time, Within Budget - Software Project Management Practices and Techniques*. McGraw-Hill International (UK) Limited, 1992.

[Boehm 81] Boehm, Barry. *Software Engineering Economics*. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1981.

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

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

[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.

[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.

[DOD 96] Department of Defense. *DoD Regulation 5000.2-R Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) Acquisition Programs*. Washington, D.C.: Department of Defense, March 1996.

[Dorofee 96] Dorofee, A.; Walker, J.; Alberts, C.; Higuera, R.; Murphy, R.; & Williams, R. *Continuous Risk Management Guidebook*. Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1996.

[DSMC 89] Defense Systems Management College. *Risk Management: Concepts and Guidance*. Reading, Ma.: Analytic Sciences Corp., March, 1989.

[Ferguson 96] Ferguson, J.; Cooper, J.; Falat, M.; Fisher, M.; Guido, A.; Marciniak, J.; Matejceck, J.; & Webster, R. *Software Acquisition Capability Maturity Model (SA-CMM[SM]) Version 1.01* (CMU/SEI-96-TR-020). Software Engineering Institute, Carnegie Mellon University, 1996

[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.

[Gibbs 94] Gibbs, W. Wayt. "Software's Chronic Crisis." *Scientific American 271,* 3 (September 1994): 72-81.

[Gluch 95] Gluch, David P.; Dorofee, Audrey J.; Hubbard, Elizabeth A.; & Travalent, John J. *A Collaboration in Implementing Team Risk Management* (CMU/SEI-95-TR-016, ADA309157). Software Engineering Institute, Carnegie Mellon University, 1995.

[Grady 92] Grady, Robert B. *Practical Software Metrics for Project Management and Process Improvement*. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1992.

[Hays 88] Hays, William L. *Statistics*. New York: Holt, Rinehart and Winston, Inc., 1988.

[Herbsleb 94] Herbsleb, J.; Carleton, A.; Rozum, J.; Siegel, J.; & Zubrow, D. *Benefits of CMM-Based Software Process Improvement: Initial Results* (CMU/SEI-94-TR-13, ADA283848). 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.* Princeton, N.J.: 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.

[Kolinger 96] Kolinger, Joseph J. "Sustaining the Benefits of Software Project Management." *Proceedings of the Third Annual Conference on Software Acquisition Management,* October 7-8, 1996. Torrance, Ca.: Technology Training Corporation, 1996.

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

[Marciniak 90] Marciniak, John J. & Reifer, Donald J. *Software Acquisition Management*. New York: John Wiley & Sons, Inc., 1990.

[Masters 95] Masters, Steve & Bothwell, Carol. *CMM Appraisal Framework Version 1.0* (CMU/SEI-95-TR-001, ADA293300). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1995.

[Mayrhauser 90] Mayrhauser, Anneliese von. *Software Engineering: Methods and Management*. San Diego, Ca.: Academic Press, Inc., 1990.

[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 96] Meyers, Margaret. "The 5000 Series - Institutionalizing Fundamental Change." *Proceedings of the Third Annual Conference on Software Acquisition Management*, October 7-8, 1996. Torrance, Ca.: Technology Training Corporation, 1996.

[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 95] Paulk, M., et al. *The Capability Maturity Model: Guidelines for Improving the Software Process*. Reading, Ma.: Addison-Wesley, 1995.

[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.

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

[Sisti 94] Sisti, Frank J. & Joseph, Sujoe. *Software Risk Evaluation Method Version 1.0* (CMU/SEI-94-TR-19, ADA290597). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1994.

[STSC 96] Software Technology Support Center. *Guidelines for Successful Acquisition and Management of Software-Intensive Systems: Weapons Systems, Command and Control Systems, Management Information Systems version 2.0*. Hill AFB, Utah: Department of the Air Force, 1996.

[Van Scoy 92] Van Scoy, Roger L. *Software Development Risk: Opportunity, Not Problem* (CMU/SEI-92-TR-30, ADA258743). Pittsburgh, Pa.: Software Engineering Institute, 1992.

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

References

Glossary

accept - A *mitigation approach* 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.

acquisition - The process of obtaining through *contract*.

acquisition organization - That entity which has the oversight responsibility for the software acquisition project and which may have purview over the *acquisition* activities of a number of projects or *contract* actions.

acquisition organization's standard software acquisition process - (See *software acquisition process*.)

activity - Any step taken or function performed, either mental or physical, toward achieving some objective. Activities include all the work the *manager*s and technical staff do to perform the tasks of the *project* and organization.

Analyze - One of the six *function*s 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 domain - A bounded set of related systems (i.e., systems that address a particular type of problem). Development and maintenance in an application domain usually require special skills and/or resources. Examples include payroll and personnel systems, avionics, command and control systems, compilers, and expert systems.

attributes (of software) - Characteristics of software such as reliability, maintainability, portability, and complexity. These characteristics are sometimes referred to as quality attributes.

baseline - A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures.

capability maturity model - A description of the stages through which organizations evolve as they define, implement, *measure*, control, and improve their processes. The model provides a guide for selecting process improvement strategies by facilitating the determination of current process capabilities and the identification of the issues most critical to quality and process improvement.

commitment - A pact that is freely assumed, visible, and expected to be kept by all parties.

common features - The subdivision categories of the SA-CMM *key process area*s. The common features are attributes that indicate whether the implementation and *institutionalization* of a key process area can be *effective*, repeatable, and lasting. The SA-CMM's common features are the following: Commitment to Perform, Ability to Perform, Activities Performed, Measurement and Analysis, and Verifying Implementation.

Communicate - One of the six *function*s 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 *consequence*s. 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.

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.

consistency - The degree of uniformity, standardization, and freedom from contradiction among the documents or parts of a system or component.

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 Risk Management - Continuous Risk Management is an engineering practice with *process*es, *method*s, 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

contract - A binding agreement between two or more parties that establishes the requirements for the products and services to be acquired.

contract integrity - The adherence and compliance to contractual and legal policies, regulations, and other guidance.

contract terms and conditions - The stated legal, financial, and administrative aspects of a *contract*.

contractor - The entity delivering the product or performing the service being acquired, even if that entity is part of the acquiring organization.

Control - One of the six *function*s 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

defined level - (See *maturity level*.)

defined software acquisition process - (See *software acquisition process*.)

effective - Adequate to accomplish the intended purpose.

end user - The individual or *group* who will use the system for its intended operational use when it is deployed in its environment.

end user representatives - A selected sample of end users who represent the total population of end users.

evaluation - The use of reviews, inspections, and/or tests, to determine that a software product or service satisfies specified requirements.

event-driven basis - A review that is performed based on the occurrence of an event within the *project* (e.g., a formal review or the completion of a life cycle stage). (See *periodic review* for contrast.)

findings - The conclusions of an assessment, *evaluation*, audit, or review that identify the most important issues, problems, or opportunities within the area of investigation.

function - A set of related actions, undertaken by individuals or tools that are specifically assigned or fitted for their *role*s, to accomplish a set purpose or end.

goals - The aggregate result achieved by the *effective* implementation of the common features of a *key process area*. The goals signify the scope and intent of each key process area.

group - An assemblage of personnel organized to serve a specific purpose or accomplish a task. A group may vary from a single individual assigned part time, to several part-time individuals assigned from other organizations, to several individuals dedicated full-time.

Identify - One of the six *function*s 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.

infrastructure costs - Those costs associated with implementing risk management activities and supporting risk management *process*es, *method*s, and tools within the organization. These costs may be spread out across multiple *project*s. See also *mitigation costs* and *risk management costs*.

initial level - (See *maturity level*.)

institutionalization - The building of infrastructure and corporate culture that supports *method*s, practices, and *procedure*s so that they are the ongoing way of doing business, even after those who originally defined them are gone.

key process area - A cluster of related activities in an area of software *acquisition* that, when performed collectively, achieve a set of *goals* considered important for establishing *process capability* in that area. The key process areas have been defined to reside at a single *maturity level*. These are the principal building blocks to help determine the *software acquisition process* capability of an organization and understand the improvements needed to advance to higher maturity levels.

life cycle - (See *software life cycle*.)

managed and controlled - Implies that the version of the work product in use at a given time (past or present) is known (i.e., version control), and changes are incorporated in a controlled manner (i.e., change control).

manager - A *role* that encompasses providing technical and administrative direction and control to individuals performing tasks or activities within the manager's area of responsibility. The traditional functions of a manager include planning, resourcing, organizing, directing, and controlling work within an area of responsibility.

maturity level - A well-defined evolutionary plateau toward achieving a mature *software acquisition process*. The five maturity levels in the SA-CMM are Initial, Repeatable, Defined, Quantitative, and Optimizing.

measure - To ascertain the characteristics or features (extent, dimension, quantity, capacity, and capability) of something, especially by comparing with a *standard*.

measurement - The dimension, capacity, quantity, or amount of something (e.g., 300 source lines of code or seven document pages of design).

method - A reasonably complete set of rules and criteria that establishes a precise and repeatable way of performing a task and arriving at a desired result.

methodology - A collection of *method*s, *procedure*s, and *standard*s that defines an integrated synthesis of approaches.

metric - A standard way of measuring some attribute of the risk management process. Risk and *mitigation plan* metrics can be qualitative or quantitative.

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.

offeror - A *contractor* who submits a proposal in response to a *solicitation package*.

optimizing level - (See *maturity level*.)

organization - The parent organization of the *acquisition organization*.

organization's measurement program - The set of related elements for addressing an organization's *measurement* needs. It includes the definition of organization-wide measurements, *method*s and practices for collecting organizational measurements and analyzing data, and measurement *goals* for the organization.

orientation - An overview or introduction to a topic.

periodic review - A review that occurs at specified regular time intervals. (See *event-driven basis* for contrast.)

Plan - One of the six *function*s 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.

policy - A guiding principle, typically established by senior management, that is adopted by an organization or *project* to influence decisions.

prime contractor - An individual, partnership, corporation, or association that administers a subcontract to design, develop, and/or manufacture one or more products.

procedure - A written description of a course of action to be taken to perform a given task.

process - A set of activities performed for a given purpose (e.g., the *software acquisition process*).

process capability - The range of expected results that can be achieved by following a process. (See *process performance* for contrast.)

process capability baseline - A documented characterization of the range of expected results that would normally be achieved by following a specific process under typical circumstances. A process capability baseline is typically established at an organizational level. (See *process performance baseline* for contrast.)

process descriptions - Documentation that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a process. It may also include the *procedure*s for determining whether these provisions have been satisfied.

process measurement - The set of definitions, *method*s, and activities used to take *measurement*s of a process and its resulting products for the purpose of characterizing and understanding the process.

process performance - A measure of the actual results achieved by following a process. (See *process capability* for contrast.)

process performance baseline - A documented characterization of the actual results achieved by following a process. A process performance baseline is typically established at the *project* level, although the initial process performance baseline will usually be derived from the process capability baseline. (See *process capability baseline* for contrast.)

project - An undertaking that is focused on acquiring a specific product. The product may include hardware, software, and services. Typically, a project has its own funding, cost accounting, and delivery schedule.

project manager - The *role* with total business responsibility for an entire *project*; the individual who directs, controls, administers, and regulates a project acquiring software, a hardware/software system, or services. The project manager is the individual ultimately responsible to the *end user.*

project office - The aggregate of individuals assigned the primary responsibility for software *acquisition* in the contracted effort. A project office may vary in size from a single individual assigned part time to a large organization assigned full time.

project team - All individuals that have an assigned software *acquisition* responsibility in the contracted effort. A project team may vary in size from a single individual assigned part time to a large organization assigned full time.

project's defined software acquisition process - (See *software acquisition process*.)

quantitative control - Any quantitative or statistically-based technique appropriate to analyze a *software acquisition process*, identify special causes of variations in the performance of the *software acquisition process*, and bring the performance of the software acquisition process within well-defined limits.

quantitative level - (See *maturity level*.)

repeatable level - (See *maturity level*.)

required training - Training required by the *acquisition organization.* (See *training* for contrast.)

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.

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 management - The *process* associated with identifying, analyzing, planning, tracking, and controlling *project* risks.

risk management costs - The costs associated with performing risk management activities—e.g., identifying risks, building status reports, and developing *mitigation plan*s. This should not be confused with *mitigation costs* or *infrastructure costs*.

role - A unit of defined responsibilities that may be assumed by one or more individuals.

software acquisition management personnel - Those individuals who are trained, educated, or experienced in software *acquisition* management and who are either assigned to or support the *project team* in the performance of software acquisition activities.

software acquisition plans - The collection of plans, both formal and informal, used to express how software *acquisition* activities will be performed; for example, the *Software Acquisition Risk Management Plan* or Project Management Plan.

software acquisition process - A set of activities, *method*s, practices, and transformations that people use to acquire software and the associated products.

- **acquisition organization's standard software acquisition process** - The *acquisition organization*'s fundamental software acquisition process which guides the establishment of each *project*'s defined software acquisition process.
- **project's defined software acquisition process** - The project's tailored version of the acquisition organization's standard software acquisition process.

software acquisition process assets - A collection of entities, maintained by an *organization*, for use by *project*s in developing, tailoring, maintaining, and implementing their *software acquisition process*.

Some examples of these software acquisition process assets include

- the *acquisition organization*'s standard *software acquisition process*
- descriptions of the *software life cycle*s approved for use
- the guidelines and criteria for tailoring the acquisition organization's standard software acquisition process
- the organization's software acquisition process database
- a library of *software acquisition process-related documentation*

Any entity that the organization considers useful in performing the activities of process definition and maintenance could be included as a process asset.

software acquisition process group - This *group* is responsible for the definition, improvement, and maintenance of the *acquisition organization*'s standard *software acquisition process* and related process assets, including guidelines for all *project*s to *tailor* the standard software acquisition process to their specific situations. It coordinates process activities with the software projects and related elements of the organization.

software acquisition process-related documentation - Documents and document fragments that may be of use to future *project team*s when tailoring the *acquisition organization*'s standard *software acquisition process*. The examples may cover subjects such as a *project's defined software acquisition process*, *standard*s, *procedure*s, *software acquisition risk management plan*s, and training materials.

software acquisition process repository - A collection of *software acquisition process* information (e.g., estimated and actual data on software *project* size, effort, and cost; and *project team* productivity and quality data) gathered from the software acquisition projects that is maintained by the *acquisition organization* to support its software acquisition definition and improvement activities.

software acquisition project - An undertaking that is focused on acquiring the software components and associated documentation of a system. A software *project* may be part of a project building a hardware/software system.

software acquisition-related group - A collection of individuals (both *manager*s and technical staff) representing a software discipline that supports, but is not directly responsible for, software *acquisition*. Examples of software disciplines include software configuration management and software quality assurance.

software acquisition risk management plan - A formal plan or documentation of the risk management practice (*process*es, *method*s, and tools) to be used for a specific *project*. This directs and manages the activities used to perform risk management within that project.

software life cycle - The period of time that begins when a software product is conceived and ends when the software is no longer available for use. The software life cycle typically includes a concept phase, requirements phase, design phase, implementation phase, test phase, installation and checkout phase, operation and maintenance phase, and, sometimes, retirement phase.

solicitation package - When seeking suppliers for a particular *acquisition*, it is the information distributed which tells the interested bidders what the requirements are, how to prepare their proposals, how proposals will be evaluated, and when to submit their proposals. Sometimes called request for proposals (RFP).

standard - Mandatory requirements employed and enforced to prescribe a disciplined, uniform approach to software development or *acquisition*.

standard software acquisition process - (See *software acquisition process*.)

tailor - To modify a *process*, standard, or *procedure* to better match process or product requirements.

technology - The application of science and/or engineering in accomplishing a particular result.

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 *function*s 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

training - *Project team* training. (See *required training* for contrast.)

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.

Appendix A

Software Acquisition Overview

Definition

Software acquisition is the process of buying software and software services. Buying software has become a common event in our society and can be done without even leaving the home or workplace. Software vendors use the Internet to allow users to download their products immediately, install them, and enjoy enhanced computing capability within minutes of purchase. This simplistic view of software acquisition doesn't hold when acquiring complex or custom systems dependent on software. Consider the F-22 fighter. Eighty percent of the functionality allowing it to fly and perform the fighter mission is dependent on software [STSC 96]. You can't simply connect an F-22 to the Internet and download commercially available navigation control, weapon system, electronic warfare, and other complex software systems and expect to maintain dominance over the enemy. Marciniak and Reifer have helped narrow the definition of software acquisition as follows:

> *software acquisition is...the process of managing the acquisition of custom software systems. The key discriminators of custom software are that it cannot be developed by a small group of people (say, fewer than 10) and that it involves a set of users with direct interest in and impact on system requirements"* [Marciniak 90].

The State of Software Acquisition Practice

Seventy-five percent of all large-scale, custom software-intensive systems fail [Gibbs 94]. The primary cause of failure is poor management on the part of the developer and the acquirer [STSC 96], not lack of technical performance. Even with this track record, the demand for software-intensive systems has been growing consistently and steadily. More and more, software costs dominate these systems. The Department of Defense (DOD) estimated in 1995 that software accounted for $35.7 billion of new systems while hardware accounted for $6.8 billion [STSC 96]. On the commercial side, outsourcing is estimated to reach $121 billion by the year 2000 [Appleton 96].

An Example

In 1987, California's Department of Motor Vehicles (DMV) decided it needed to merge its driver license and vehicle registration systems. Seven years and $44.3 million later, the DMV cancelled the project after facing a 4 year schedule slip and a projected increase in cost 6.5 times over what was originally expected [Gibbs 94].

The Software Development Life Cycle

The software development life cycle can be depicted as a series of events performed sequentially, concurrently, or cyclically. Whichever approach is selected, the following steps are usually performed when developing a software-intensive system and they provide a template for understanding software development and its application in more sophisticated development models such as the incremental model [Pressman 92].

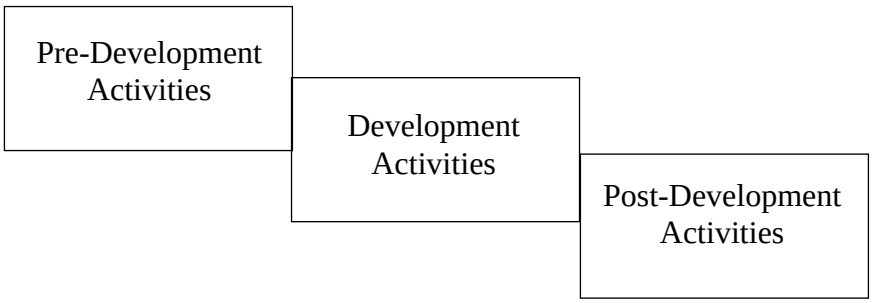
- system requirements analysis
- software requirements analysis
- preliminary design
- detailed design
- code and unit test
- software test and integration
- subsystem test and integration
- system test and integration

The Software Acquisition Life Cycle

The software acquisition life cycle encompasses the software development life cycle with additional activities performed on either end. The Department of Defense defines four acquisition phases [DOD 96]:

- Phase 0: Concept Exploration
- Phase 1: Program Definition and Risk Reduction
- Phase 2: Engineering and Manufacturing Development
- Phase 3: Production, Fielding/Deployment, and Operational Support

For clarity, the life cycle is simplified into three phases: pre-development activities, development activities (the software development process fits in here), and post-development activities as depicted in the figure below. Each of these phases contain critical activities performed by the acquisition organization which can lead to a project's success or failure.



Pre-Development Activities

The pre-development activities can include determining strategic business objectives based on market, needs, or threat analysis, developing proposed alternatives to meet those objectives, performing feasibility studies, capturing system requirements, estimating project costs, capturing and continuously managing risks, selecting one or more projects to fund, deciding to make or buy the new capability, staffing a project office, developing a solicitation package, selecting a contractor, and teaming with the winner to start the project. While the list is by no means exhaustive, each of these activities is critical to the project's eventual success.

Development Activities

During development, the acquirer tracks and oversees the contracted effort, maintains the health of the project team, approves design decisions, and is the liaison between the user and the developer. Many custom, software-intensive systems take years to develop. This presents the acquirer with two major problems; knowing the real status of the project at any given time and struggling with the need to freeze requirements in a changing environment.

Post-Development Activities

Post-development activities can include user acceptance, installation of the new capability in the operational environment, and transitioning maintenance to the software support organization. User rejection is a very real possibility. Finding out that users have rejected the system during this phase is a major failure on the part of the acquisition organization. This risk can be mitigated "...with intimate user involvement, and often with periodic prototype or early version field tests" [STSC 96].

Contracting for enhancements, defect removal, and adaptation can be seen as mini-acquisitions requiring another cycle starting with the pre-development activities.

Making it Successful

Given the activities performed by the acquisition organization and the potential for project disaster based on mismanagement, the need for software acquisition improvement becomes obvious. Appendix B, p. 67 introduces the Software Acquisition Capability Maturity Model (SA-CMM), which can be used to help an organization baseline software acquisition capability and define an improvement path with the goal of standardizing the way the organization does business, increasing predictability, and reducing risk.

Appendix A

Appendix B

The Software Acquisition CMM

How the Acquirer and Developer Differ

During the acquisition of a custom software system, the acquirer and the developer have distinct responsibilities. The acquirer acts as an agent for an end user while the developer responds to the acquirer's requirements and delivers a specified capability [Marciniak 90]. Each have an important role to play in acquiring a software-intensive system. The following table contains examples of the types of responsibilities each may have when acquiring a software system and is not meant to be comprehensive.

Role	Responsibilities
Acquirer	Describe functional requirements
	Manage the user's needs
	Allocate resources
	Contract with developer
	Staff project team
	Monitor development (cost, schedule, performance)
	Determine support requirements
Developer	Decide to bid
	Staff a proposal team
	Estimate resources
	Develop detailed proposal
	Respond to acquirer post-contract award
	Analyze and allocate requirements
	Design solution
	Develop software
	Test and install capability
	Hand maintenance over to support agency

Process Capability

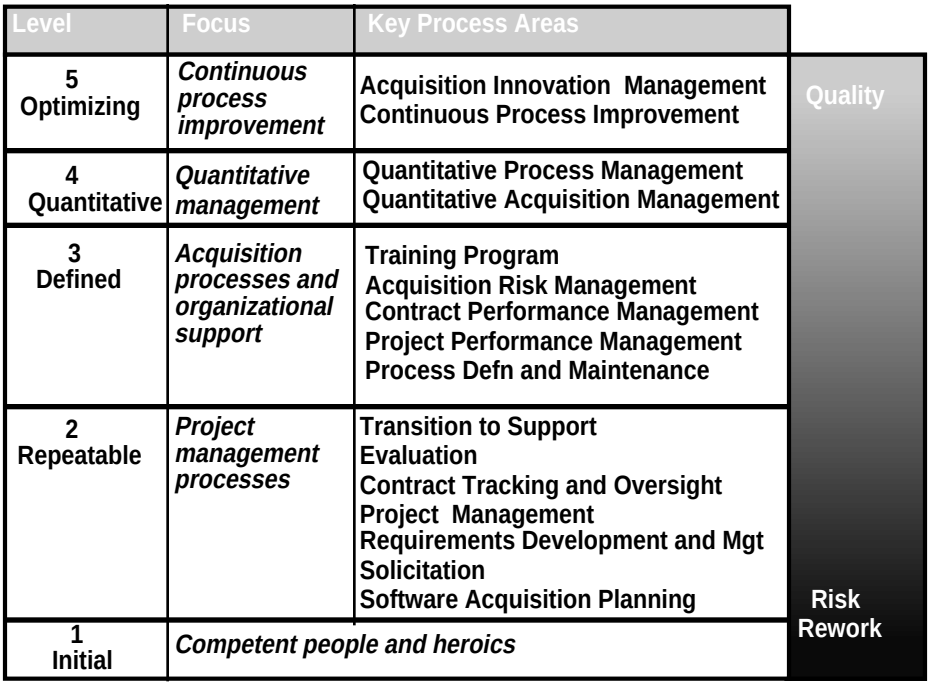
Software acquisition process capability is the ability of an organization's acquisition process to produce predictable and consistent, planned results. The Capability Maturity Model for Software (SW-CMM) has been used for several years to help software developers increase their software process capability [Paulk 95]. By using the SW-CMM to help define and improve process capability, software development organizations have seen as much as an 8:1 return on investment [Herbsleb 94]. The intangible benefits of using a CMM-based improvement program can be even more impressive. Pacific Bell's benefits from using the SW-CMM are listed below [Kolinger 96].

Pacific Bell's Benefits from Using the SW-CMM
A repeatable process for commitment management is established.
Consistent program office practices, understood by all, reduce the PM's workload.

Pacific Bell's Benefits from Using the SW-CMM
Project managers can focus on critical project issues.
Helps in understanding and forecasting capability.
New project managers become productive more quickly.
A consistent set of values is communicated.
Developers experience far fewer interruptions.
Project managers feel valued, supported, and empowered.
Gives clients and users confidence as it improves credibility.
Allows normalization of project metrics.

A Collection of Key Practices

The SW-CMM is a collection of key practices that developers can use to baseline and improve their software development process capability. Acquirers have a similar need to assess the maturity of their software acquisition process with the goal of identifying areas needing improvement. The Software Acquisition Capability Maturity Model (SA-CMM) was developed by a group of software acquisition experts from government and industry to address this need [Ferguson 96]. The SA-CMM is a collection of key practices formed into an improvement framework depicting organizational maturity. The model has five maturity levels with key process areas (KPAs) grouped at each level. As an organization masters the KPAs at a given level and progresses from an ad hoc acquisition organization to an organization embracing continuous improvement, risk and rework are reduced.



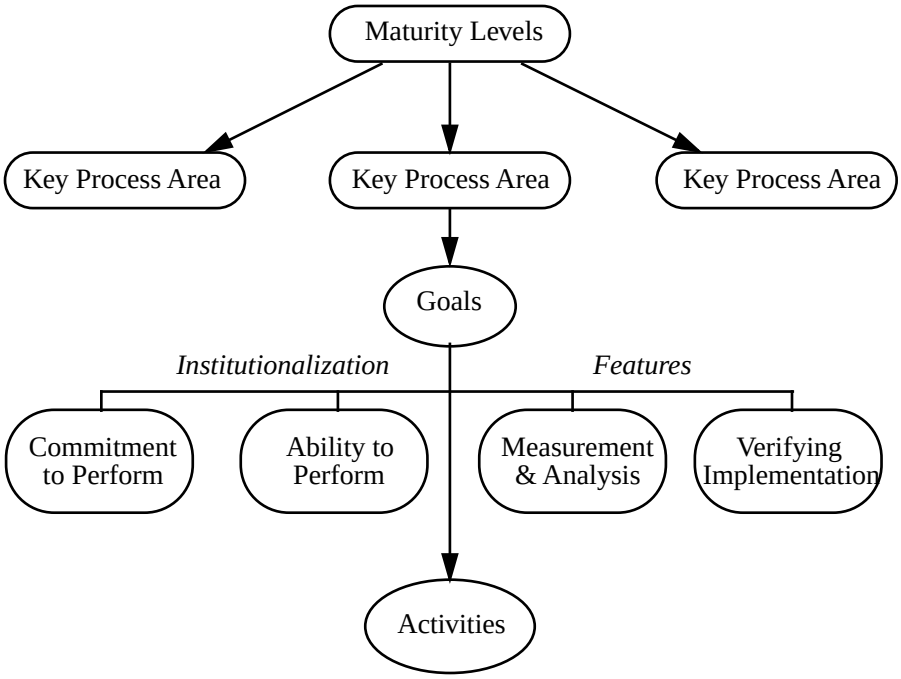
Organizational Maturity

Organizations at Level 1 of the SA-CMM are immature. As an organization progresses through the model, its software acquisition process capability matures. Organizations at lower levels of maturity are reactionary. Managers and practitioners make up processes on the fly and usually in response to a major problem. There is no common understanding of how to conduct business, and project members have to re-invent the wheel at every turn. Project managers have little insight into the activities of the project team and are usually caught by surprise when the contractor or project team encounters problems.

A mature software acquisition organization, by contrast, is proactive. It has the ability to capture, maintain, and improve software acquisition processes. These processes are communicated to existing staff and new employees. The organization's processes are documented, usable, and reflect how work actually gets done. Roles and responsibilities are defined within the process and are clear across the project and entire organization. Managers monitor and evaluate the quality of the software acquisition products and the process that produces them. Cost and schedule estimates are developed based on historical data and the project achieves realistic expectations [Paulk 95].

KPA Structure

KPAs are grouped at maturity levels within the SA-CMM. A KPA is a cluster of related practices in an area of software acquisition. When these practices are performed collectively, they achieve the goals that establish process capability in that area [Ferguson 96]. To master a KPA, its goals must be achieved. Supporting those goals are the institutionalization features which help install the KPA as a common business practice and the activities which are performed by the acquisition organization to accomplish the goals.



Reducing Risk Through Process Improvement

A mature organization with well-defined processes can expect improvement in predictability, control, and effectiveness [Paulk 95]. Improvements in these three areas will reduce the risks associated with acquiring software. See Appendix E, p. 91 for a discussion of the appraisal process used to determine an acquisition organization's software acquisition capability using the SA-CMM.

Appendix B

Appendix C

Risk Management Methods and Tools

Overview

This appendix provides a summary of the methods and tools that can be used to perform the risk management paradigm functions. Methods are systematic approaches to performing risk management processes while tools are templates or forms. More detailed information for all of the methods and tools in this section are featured in the *Continuous Risk Management Guidebook* [Dorofee 96]. The project team may select these or other methods and tools to perform acquisition risk management.

Identification Methods and Tools

The following table provides a summary of some of the methods and tools that can be used to support the components of risk identification. Additional references are provided for some of the methods and tools. Any identification method or tool which is not listed in the table below, but which a project team feels is appropriate for its needs, can be selected by a project team as needed.

Component	Method or Tool	Description
All components	Risk information sheet	A form that documents information about a risk, similar to a software trouble or problem report. As information is acquired or collected, it is added to the risk information sheet [see Appendix D, p. 85].
Capture statement of risk	Brainstorming	A method where project personnel verbally identify risks as they think of the risks. This method provides the opportunity for participants to build on each others' ideas. [Lumsdaine 90], [Osborn 53], and [Xerox 92].
	Periodic risk reporting	A method requiring mandatory and scheduled reporting of risks by project personnel.
	Project profile questions	A tool used to tailor the taxonomy-based questionnaire (TBQ) based on project characteristics.
	Risk form	A form used to document new risks as they are identified. [see Appendix D, p. 85]
	Short TBQ	A shortened version of the TBQ which can be used in conjunction with voluntary or periodic risk reporting. It can also be used during meetings and one-on-one interviews to help identify risks.
	Taxonomy-based questionnaire (TBQ)	A listing of interview questions which are organized according to the software development risk taxonomy. [Carr 93]
	TBQ interviews	A method where structured peer group interviews are conducted using the TBQ.
	Voluntary risk reporting	A method where project personnel voluntarily submit risk forms whenever new risks are identified.
Capture context of risk	All above methods and tools	All of the above methods and tools are applicable to capturing the context of a risk because context is required any time a risk is identified.

Analysis Methods and Tools

The following table provides a summary of some of the methods and tools that can be used to support the components of risk analysis. Additional references are provided for some of the methods and tools. Any analysis method or tool which is not listed in the table below, but which a project team feels is appropriate for its needs, can be selected by a project team as needed.

Component	Method or Tool	Description
All components	Risk information sheet	A form that documents information about a risk, similar to a software trouble or problem report. As information is acquired or collected, it is added to the risk information sheet [see Appendix D, p. 85].
Evaluate	Binary attribute evaluation	A method where each risk is evaluated with respect to • *impact* (significant, insignificant) • *probability* (likely, unlikely) • *timeframe* (near-term, far-term) *Note*: Each attribute only has two possible values.
	Risk form	A form that can be used to capture the results of the binary attribute evaluation or tri-level attribute evaluation methods for a risk [see Appendix D, p. 85].
	Tri-level attribute evaluation	A method where each risk is evaluated with respect to • *impact* (catastrophic, critical, marginal) • *probability* (very likely, probable, improbable) • *timeframe* (imminent, near-term, far-term) *Note*: Each attribute only has three possible values [Air Force 88] and [Sisti 94].
Classify	Affinity grouping	A method where risks that are naturally related are grouped together. The concept that ties together the risks in the group is also identified [Brassard 89] and [Brassard 94].
	Bar graph	A tool that presents a graphical summary of the number of risks in each classification category [Brassard 89], [Hays 88], and [Moran 90].
	Risk form	A form used to capture the results of the affinity grouping or taxonomy classification methods for a risk [see Appendix D, p. 85].
	Taxonomy classification	A method that groups risks according to software development areas using the software development risk taxonomy's class/element/attribute structure [Carr 93].

Component	Method or Tool	Description
Prioritize	Comparison risk ranking	A method where risks are ranked. The method is conducted by comparing two risks to each other, based on an established criterion or set of criteria. The comparisons continue until every risk has been compared to all of the other risks [Fitzgerald 90a], [Fitzgerald 90b], and [Xerox 92].
	Multivoting	The multivoting method is a general voting technique to select the most important items on a list. For a large list, a series of votes is used to reduce the list to a workable number. Each participant is given a number of votes to be distributed across the items on the list. Participants vote individually, and the votes are tallied by one of the group members [Scholtes 88] and [Xerox 92].
	Pareto top N	A method where the most important risks to the project are selected based on the results of the tri-level attribute evaluation [Juran 89].
	Potential top N	A method where the most important risks to the project are selected based on individual opinions, which are surfaced using the top 5 method. All of the participants' number one risks are grouped together; then, all of the number two risks are grouped together. This continues until all of the risks in the participants' top 5 lists are placed in a group. If a risk appears in more than one group, it is eliminated from all but the highest ranking group. The result is a non-ordered list of important risks to the project.
	Top 5	A method where individuals choose the top 5 risks to the project as part of a group analysis effort, such as the potential top N method. The intent is to collect individual perspectives on which risks are important to the project.

Planning Methods and Tools

The following table provides a summary of some of the methods and tools that can be used to support the components of planning. Additional references are provided for some of the methods and tools. Any planning method or tool which is not listed in the table below, but which a project team feels is appropriate for its needs, can be selected by a project team as needed.

Component	Method or Tool	Description
All components	Planning decision flowchart	A tool that can be used to remind planners of possible planning approaches as well as the criteria for selecting those approaches [see Appendix D, p. 85].
	Risk information sheet	A form that is used to document the chosen mitigation strategy and actions as well as who has responsibility for developing the plan [see Appendix D, p. 85].
Assign responsibility	No specific method or tool	Assigning responsibility is a management or team decision.
Determine approach	Goal-question-metric	A method where metrics are identified to track the progress of a mitigation strategy and the changes in the status of a risk. A list of questions is developed and used to structure a brainstorming session to identify appropriate metrics [Basili 84], [Pulford 96], and [Grady 92].
Define scope and actions	Action item list	A document that lists one or more simple actions required to mitigate a risk. The status of the mitigation effort is tracked and reported when using this tool.
	Planning worksheet	A form that is used to identify, analyze, and document alternative mitigation actions and decisions. It also serves as a historical record of the alternatives that were considered before the mitigation plan was chosen [see Appendix D, p. 85].

Component	Method or Tool	Description
Define scope and actions (cont.)	Problem-solving planning	A method where task plans are developed to mitigate a risk or risk set. This method is used for a complex risk or set of related risks where dependencies are high and mitigation may be costly. Management approval is likely required to implement the task plan. Often, group expertise is required to develop the detailed plans and schedules, and this method is designed for groups. Problem-solving planning includes the following methods and tools: • affinity grouping • brainstorming • cause and effect analysis • cost-benefit analysis • Gantt charts • goal-question-metric • list reduction • multivoting • PERT charts • work breakdown structure [Kepner 81], [Lumsdaine 90], [Scholtes 88], and [Xerox 92]
	Risk form	A form that provides a field to document the recommended mitigation action [see Appendix D, p. 85].

Tracking 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 provides a summary of some of the approaches that can be used to support the components of risk tracking. Details on specific methods and tools that support some of the approaches are provided in Tracking Methods and Tools, p. 79. Any tracking approach which is not listed in the table below, but which a project team feels is appropriate for its needs, can be selected by a project team as needed.

Component	Approach	Description
Acquire	Re-evaluate risk attributes	With this approach, the individual who is responsible for the risk should periodically re-evaluate the risk attributes to determine changes in probability, impact, and timeframe. Access to knowledgeable individuals or other data may be required. This approach provides status information for watched risks and mitigation plans. The following methods are used to evaluate risk attributes: • binary attribute evaluation • tri-level attribute evaluation
	Direct communication	This approach consists of 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 risk or plan actions are interviewed. In some cases, the individual who is interviewed may be the manager responsible for the risk or mitigation plan.
	Review documents and reports	This approach involves looking at the technical aspects of the development effort's progress. Reviewing reports and documents can be useful for technical risks but can also provide insight into general project issues. This approach can also be used to look for new risk information.
	Review status reports	This approach involves reviewing documentation that is available from the routine project status meetings. These reviews can provide insight into general project issues as well as status information for watched risks and mitigation plans.
	Automated data collection	This approach involves using commercially-available tools to track and collect progress and quality metrics from the project's products and reports, providing consistent, often quantitative risk data. The data collected can be used to track risks and the progress of mitigation efforts.
Compile	Mitigation plan summaries	This approach uses summaries or reports that show mitigation plan progress. Mitigation status summaries are used to support decisions. The following method is designed to convey information about the status of a mitigation plan: • mitigation status report

Component	Approach	Description
Compile (cont.)	Risk status summaries	This approach uses summary tables, which are concise tabular compilations of key data items. The following methods and tools are designed to produce and use tabular formats: • risk information sheet • spreadsheet risk tracking • stoplight chart The analysis of current status data can identify both changes in priority or the need for outside help as well as new risks to the project.
	Trend summaries	This approach utilizes graphical representations of compiled risk data. The following are used to present risk data on graphs or charts: • bar graph • time correlation chart • time graph
Report	Verbal reporting	This approach uses informal means of communication to disseminate risk data. The people responsible for risks give verbal reports on the general status of their risks. This forum can also be used 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 as well as immediate notification of critical issues or changes.
	Written reporting	This approach can use either formal or informal memoranda or documents (e.g., electronic mail, reports, etc.). The reports should be integrated into the normal status reporting mechanisms used by the organization. The following methods can be used to support this activity: • mitigation status report • risk information sheet • spreadsheet risk tracking • stoplight chart
	Formal presentations	This approach requires a medium and format that are appropriate for the organization. Formal presentations are often supported by written reports and contain additional material that might not be included in written reports.

Tracking Methods and Tools

The following table provides a summary of some of the methods and tools used to support the tracking approaches described above. Additional references are provided for some of the methods and tools. Any tracking method or tool which is not listed in the table below, but which a project team feels is appropriate for its needs, can be selected by a project team as needed.

Component	Method or Tool	Description
Acquire	Binary attribute evaluation	A method where each risk is evaluated with respect to • *impact* (significant, insignificant) • *probability* (likely, unlikely) • *timeframe* (near-term, far-term) *Note*: Each attribute only has two possible values.
	Tri-level attribute evaluation	A method where each risk is evaluated with respect to • *impact* (catastrophic, critical, marginal) • *probability* (very likely, probable, improbable) • *timeframe* (imminent, near-term, far-term) *Note*: Each attribute only has three possible values [Air Force 88] and [Sisti 94].
Compile and Report	Mitigation status report	This method requires compiling data using textual information and graphics (e.g., time graphs, bar graphs, etc.) to document detailed information about specific risk mitigation plans. Mitigation status reports are used to support decisions. The format of the report and the information included in the report should be tailored to the needs of an organization [Clark 95].
	Risk information sheet	This form documents information about a risk, similar to a software trouble or problem report. It is used to document detailed information on specific risks and to support decisions [see Appendix D, p. 85].
	Spreadsheet risk tracking	This method uses spreadsheets to summarize the current statuses of all risks and provides a way to monitor project risks. The basic process involves a periodic (e.g., weekly or monthly) update and review of the risks. Spreadsheet risk tracking reports are normally included as read-ahead material for project meetings, where the reports are reviewed and updated as appropriate [see Appendix D, p. 85].
	Stoplight chart	This is a tool that is used to summarize the statuses of important risks and their mitigation efforts. The charts are effective tools for reporting risk information to senior management. Each mitigation plan is assigned one of three conditions: • *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, although no management action is required • *red*—indicates that the plan is not working and that management action is required [see Appendix D, p. 85]

Component	Method or Tool	Description
Compile and Report (cont.)	Bar graph	This type of graph depicts data across distinct categories. Bar graphs highlight changes in the number of risks in individual categories and can be used to identify trends [Brassard 89], [Hays 88], and [Moran 90].
	Time correlation chart	This type of graph shows the relationship of one metric with respect to another over time. Time correlation charts are useful for identifying the trend over time in the relationship of two metrics [Brassard 89], [Hays 88], and [Moran 90].
	Time graph	This type of graph illustrates data variations over time. Time graphs are useful for identifying the trend over time of a risk metric [Brassard 89], [Hays 88], and [Moran 90].

Control Methods and Tools

The following table provides a summary of some of the methods and tools that can be used to support the components of risk control. Additional references are provided for some of the methods and tools. Any control method or tool which is not listed in the table below, but which a project team feels is appropriate for its needs, can be selected by a project team as needed.

Note: The 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 projects have an established suite of effective methods for these activities. If such methods and tools do exist within an organization, then they should also be applied to risk data.

Component	Method or Tool	Description
Analyze	Cause and effect analysis	This method analyzes the relationships and interrelationships between a risk and it associated causes. Analyzing the causes and effects of risks and actions may provide additional insight into their dependencies and relationships to support decisions [Lumsdaine 90], [Scholtes 88], and [Xerox 92].
	Cost-benefit analysis	This method re-evaluates the costs and benefits of a particular mitigation strategy if the strategy is not having the expected results. Cost-benefit analysis provides the information needed by decision makers to determine whether to continue as planned or to replan [Arrow 88], [Boehm 81], and [Xerox 92].
	Mitigation status report	This method requires compiling data using textual information and graphics (e.g., time graphs, bar graphs, etc.) to document detailed information about specific risk mitigation plans. Mitigation status reports provide decision makers with the data required to determine the appropriate control actions (e.g., invoke contingency plan, replan, etc.). The format of the report and the information included in the report should be tailored to the needs of an organization [Clark 95].
	PERT Chart	This tool is a commonly-used management tool for managing time and cost. PERT (program evaluation and review technique) charts are dependency and probability schedules that can be used to analyze the impacts of changes in risk status and mitigation plans [Bennatan 92], [Mayrhauser 90], [Pressman 92], and [Xerox 92].
	Spreadsheet risk tracking	This method uses spreadsheets to summarize the current statuses of all risks and provides a way to monitor project risks. The basic process involves a periodic (e.g., weekly or monthly) update and review of the risks. Spreadsheet risk tracking reports are normally included as read-ahead material for project meetings, where the reports are reviewed and updated as appropriate [see Appendix D, p. 85].

Component	Method or Tool	Description
Analyze (cont.)	Stoplight chart	This is a tool that is used to summarize the statuses of important risks and their mitigation efforts. The charts are effective tools for reporting risk information to senior management. Each mitigation plan is assigned one of three conditions: • *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, although no management action is required • *red*—indicates that the plan is not working and that management action is required [see Appendix D, p. 85]
Decide	Closing a risk	This method formally documents information about a risk that has been successfully mitigated, has been accepted, or has become a problem. Any lessons learned from watching or mitigating the risk or set as well as the rationale for closing the risk or set should be captured upon closure.
	List reduction	This method is used with a large number of risks, strategies, or other ideas. It is especially useful when dealing with the results of a brainstorming session (see Identification Methods and Tools, p. 72). The participants vote on each item to determine whether or not to keep it on the list. A majority of votes generally keeps the item on the list [Xerox 92].
	Multivoting	The multivoting method is a general voting technique to select the most important items on a list. For a large list, a series of votes is used to reduce the list to a workable number. Each participant is given a number of votes to be distributed across the items on the list. Participants vote individually, and the votes are tallied by one of the group members [Scholtes 88] and [Xerox 92].
Execute	Closing a risk	This method formally documents information about a risk that has been successfully mitigated, has been accepted, or has become a problem. See closing a risk in the Decide component methods and tools above.
	Mitigation status report	This method requires compiling data using textual information and graphics to document detailed information about specific risk mitigation plans. See mitigation status report in the Analyze component methods and tools above.
	Risk information sheet	A form that documents information about a risk, similar to a software trouble or problem report. As information is acquired or collected, it is added to the risk information sheet [see Appendix D, p. 85].

Component	Method or Tool	Description
Execute (cont.)	Spreadsheet risk tracking	This method uses spreadsheets to summarize the current statuses of all risks and provides a way to monitor project risks. Documentation of the action being executed as well as other relevant information (e.g., the scheduled completion date) is added to the spreadsheet. See spreadsheet risk tracking in the Analyze component methods and tools above.
	Stoplight chart	This is a tool that is used to summarize the statuses of important risks and their mitigation efforts. The action being executed, its current state of success, and other relevant information (e.g., the scheduled completion date) is added to the chart. See stoplight chart in the Analyze component methods and tools above.

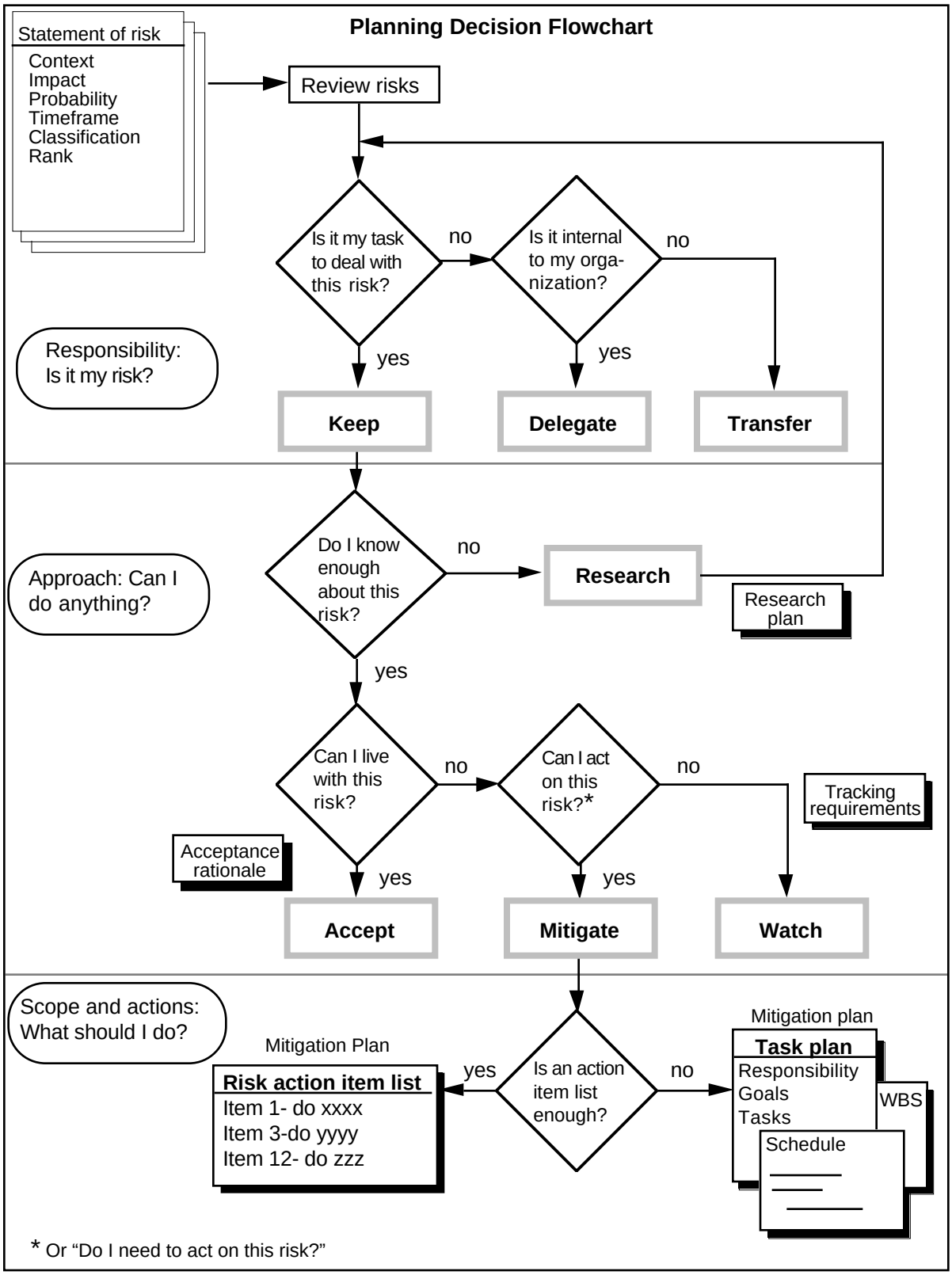
Appendix D

Selected Risk Management Forms

Overview

This appendix contains examples of selected risk management tools. All of the tools highlighted in this section are featured in the *Continuous Risk Management Guidebook* [Dorofee 96]. Examples of the following forms, flowcharts, and spreadsheets can be found in this section:

- planning decision flowchart
- planning worksheet
- risk form
- risk information sheet
- spreadsheet risk tracking
- stoplight chart


Planning Decision Flowchart
Statement of risk
Context
Impact
Probability
Timeframe
Classification
Rank
Review risks
Is it my task to deal with this risk?
no
Is it internal to my organization?
no
yes
yes
Responsibility: Is it my risk?
Keep
Delegate
Transfer
Do I know enough about this risk?
no
Research
Research plan
Approach: Can I do anything?
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
Risk action item list
Item 1- do xxxx
Item 3-do yyyy
Item 12- do zzz
yes
Is an action item list enough?
no
Mitigation plan
Task plan
Responsibility
Goals
Tasks
WBS
Schedule
* Or "Do I need to act on this risk?"

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**

Risk Form

Impact

Probability

Timeframe

ID#_____

(for internal use only)

Date:_____

Statement of risk (with context)

Requires immediate management attention

Recommendation for dealing with the risk (optional):

Classification:

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**	

.

Risk Spreadsheet						6/10/94
Risk ID	**Priority**	**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.

.

Stoplight Chart						
Status	**Risk ID**	**Risk Statement**	**Assigned To**	**Action Plan**	**Key Mile-stones**	**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

Appendix E

The SA-CMM Appraisal Process

Overview

This appendix provides a summary of the appraisal process used by the SEI when performing appraisals of an acquisition organization's acquisition capability using the SA-CMM. Assessments and evaluations are discussed and a list of typical appraisal questions for the ARM KPA are provided.

Appraisal Methods

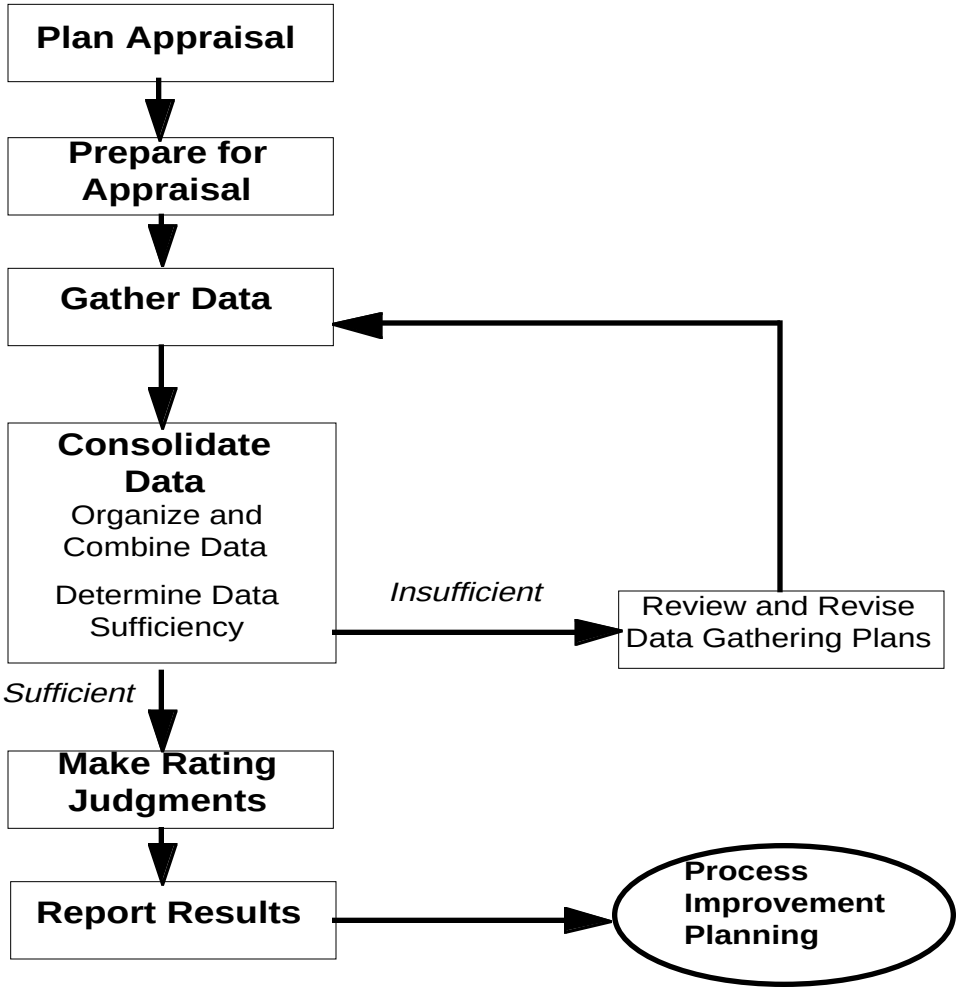
The SA-CMM uses the SEI-defined CMM appraisal methods. The term "appraisal" in this context is used to address both assessments and evaluations. For assessments, the CMM-Based Appraisal for Internal Process Improvement (CBA-IPI) method is used, and for evaluations the Software Capability Evaluation (SCE) V3.0 is used. Both methods are CMM Appraisal Framework (CAF) compliant [Masters 95] and have been approved and used extensively by the SW-CMM community the past two years.

Appraiser Qualifications

As with the SW-CMM, SA-CMM appraisers must be trained and qualified prior to executing appraisals. The qualifications for SA-CMM appraisers are similar to that for the Lead Assessors and Lead Evaluators for the SW-CMM, with acquisition experience being the primary discriminator.

Appraisal Diagram

The following diagram shows the generic appraisal activities that occur with SEI CAF-compliant methods.



ARM and the Appraisal Process

With respect to the ARM KPA, the activities and institutionalization features will be appraised through interviews and documentation reviews. Results are ultimately reported in the form of findings in the context of the specific KPA they address. These

results form the basis for acquisition process improvement planning and execution.

Maturity Questionnaire

Normally an SA-CMM maturity questionnaire will be administered in advance of the onsite appraisal. This data is used to provide the appraisal team its first set of organization-specific data and may provide insight into appropriate tailoring of the onsite document requests and interview questions (i.e., the data gathering plan).

Typical ARM Questions

The following are typical questions that an appraiser may ask when assessing or evaluating an organization's acquisition capability:

Key Practice	Question
Commitment 1	What organizational policy prescribes acquisition risk management?
Commitment 2 Ability 1	Who on this project is responsible for coordinating acquisition risk management activities?
Ability 3	How were the individuals who perform acquisition risk management activities chosen?
Activity 1	How does the project ensure risk identification, analysis, and mitigation activities are integrated into the software acquisition planning?
Activity 2 Activity 3	Does a Software Acquisition Risk Management Plan exist?
Activity 4	How does the project ensure that risk identification, analysis, and mitigation are conducted as an integral part of the solicitation, project performance management, and contract performance management processes?
Activity 5	How does the project team track and control risks?
Ability 2 Measurement 1 Verification1 Verification 2	Describe how resources expended for acquisition risk management activities are recorded and tracked?
Verification 1 Verification 2	How often does the project manager and acquisition organization management review the acquisition risk management activities?

Results of Appraisals

The appraisal final briefing and delivery of the final report become the basis for acquisition process improvement activities. Regardless of the determination of a maturity level rating, the appraisal findings provide a rich source of information upon which to initiate and establish overall acquisition process improvement as well as acquisition risk management.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. **AGENCY USE ONLY** (leave blank)	2. **REPORT DATE** August 1997	3. **REPORT TYPE AND DATES COVERED** Final
4. **TITLE AND SUBTITLE** Software Acquisition Risk Management Key Process Area (KPA)—A Guidebook		5. **FUNDING NUMBERS** C — F19628-95-C-0003
6. **AUTHOR(S)** Brian P. Gallagher, Christopher J. Alberts, Richard E. Barbour		
7. **PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. **PERFORMING ORGANIZATION REPORT NUMBER** CMU/SEI-97-HB-002
9. **SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)** HQ ESC/AXS 5 Eglin Street Hanscom AFB, MA 01731-2116		10. **SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. **SUPPLEMENTARY NOTES**		
12.a **DISTRIBUTION/AVAILABILITY STATEMENT** Unclassified/Unlimited, DTIC, NTIS		12.b **DISTRIBUTION CODE**

13. **ABSTRACT** (maximum 200 words)

In this guidebook, we hope to provide sponsors of acquisition improvement programs and their immediate staff with guidelines on how to implement a software acquisition risk management program satisfying the goals of the Acquisition Risk Management (ARM) Key Process Area (KPA) of the Software Acquisition Capability Maturity Model[SM] (SA-CMM[SM]). Brief overviews of software acquisition and the SA-CMM are included.

14. **SUBJECT TERMS** risk management, software acquisition, software acquisition capability maturity model (SA-CMM)			15. **NUMBER OF PAGES** 93 pp. 16. **PRICE CODE**
17. **SECURITY CLASSIFICATION OF REPORT** UNCLASSIFIED	18. **SECURITY CLASSIFICATION OF THIS PAGE** UNCLASSIFIED	19. **SECURITY CLASSIFICATION OF ABSTRACT** UNCLASSIFIED	20. **LIMITATION OF ABSTRACT** UL