Software Engineering Institute

Risk Management Framework

Christopher J. Alberts
Audrey J. Dorofee

August 2010

TECHNICAL REPORT
CMU/SEI-2010-TR-017
ESC-TR-2010-017

Acquisition Support Program

http://www.sei.cmu.edu

Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

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.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number FA8721-05-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 252.227-7013.

For information about SEI publications, please visit the library on the SEI website (www.sei.cmu.edu/library).

Table of Contents

List of Figures

Acknowledgments

The authors would like to thank the Army Strategic Software Improvement Program (ASSIP) for piloting a workshop that resulted in significant improvements to the framework. The authors also wish to acknowledge the contributions of the reviewers, Carol Woody, Julie Cohen, and Tricia Oberndorf, and the editor of this technical report, Barbara White.

Abstract

Although most programs and organizations use risk management when developing and operating software-reliant systems, preventable failures continue to occur at an alarming rate. In many instances, the root causes of these preventable failures can be traced to weaknesses in the risk management practices employed by those programs and organizations. To help improve existing risk management practices, Carnegie Mellon University Software Engineering Institute (SEI) researchers undertook a project to define what constitutes best practice for risk management. The SEI has conducted research and development in the area of risk management since the early 1990s. Past SEI research has applied risk management methods, tools, and techniques across the life cycle (including acquisition, development, and operations) and has examined various types of risk, including software development risk, system acquisition risk, operational risk, mission risk, and information security risk, among others.

In this technical report, SEI researchers have codified this experience and expertise by specifying (1) a Risk Management Framework that documents accepted best practice for risk management and (2) an approach for evaluating a program's or organization's risk management practice in relation to the framework.

1 Introduction

Occurrence of Preventable Failures

Although most programs and organizations use risk management when developing and operating software-reliant systems, preventable failures continue to occur at an alarming rate. Several reasons contribute to the occurrence of these failures, including

- significant gaps in the risk management practices employed by programs and organizations
- uneven and inconsistent application of risk management practices within and across organizations
- ineffective integration of risk management with program and organizational management
- increasingly complex management environment

To help improve existing risk management practices, Carnegie Mellon® Software Engineering Institute (SEI) researchers undertook a project to define what constitutes best practice for risk management. This technical report provides the results of that research project by specifying the following:

- a Risk Management Framework that documents accepted best practice for risk management
- an approach for evaluating a program's or organization's risk management practice in relation to the requirements specified in the framework

SEI Background in Risk Management

Since the early 1990s, the SEI has conducted research and development in the area of risk management and has applied risk management methods, tools, and techniques across the life cycle (including acquisition, development, and operations). In addition, past SEI research examined various types of risk, including software development risk [Dorofee 1996, Williams 1999, Alberts 2009], system acquisition risk [Gallagher 1999], operational risk [Gallagher 2005], mission risk [Alberts 2009] and information security risk [Alberts 2002], among others. In this technical report, SEI researchers have codified this experience in the form of a Risk Management Framework.

® Carnegie Mellon is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Risk Management Framework

The Risk Management Framework specifies accepted best practice for the discipline of risk management. The framework is implementation independent—it defines key risk management activities, but does not specify how to perform those activities. In particular, the framework helps provide a

- foundation for a comprehensive risk management methodology
- basis for evaluating and improving a program's risk management practice

The Risk Management Framework can be applied in all phases of the system development life cycle (e.g., acquisition, development, operations). In addition, the framework can be used to guide the management of many different types of risk (e.g., acquisition program risk, software development risk, operational risk, information security risk).

Purpose of this Document

The purpose of this technical report is to present the Risk Management Framework, which defines the core set of activities and outputs required to manage risk effectively. However, this document does not provide step-by-step procedures for conducting the risk management activities. Other SEI documents and courses provide specific methods, tools, and techniques for managing different types of risk.

Intended Audience

The primary audience for this technical report is people who are responsible for assessing and managing risk in development and operational settings. People who are interested in the following topics might also find this document useful:

- learning about what constitutes best practice in risk management
- evaluating and improving an existing risk management practice

Structure of This Document

This technical report is divided into the following parts:

- **Section 1: Introduction**—provides a brief overview of the motivation for developing the Risk Management Framework and defines the audience for this document
- **Section 2: Risk Management Concepts**—presents background information about risk management
- **Section 3: Framework Overview**—describes how the Risk Management Framework is structured
- **Section 4: Prepare for Risk Management (Phase 1)**—presents activities that are required to prepare for risk management
- **Section 5: Perform Risk Management Activities (Phase 2)**—describes activities that are required to manage risk effectively
- **Section 6: Sustain and Improve Risk Management (Phase 3)**—presents activities that are required to sustain and improve a risk management practice over time
- **Section 7: Framework Requirements**—defines the criteria that are used to establish conformance with the Risk Management Framework
- **Appendix: Evaluating a Risk Management Practice**—presents a set of worksheets that can be used to evaluate a program's or organization's risk management practice and establish consistency with the Risk Management Framework

2 Risk Management Concepts

Multiple Contexts of Risk Management

The term *risk* is used universally, but different audiences often attach different meanings to it [Kloman 1990]. In fact, the details about risk and how it supports decision making depend upon the context in which it is applied [Charette 1990]. For example, safety professionals view risk management in terms of reducing the number of accidents and injuries. A hospital administrator views risk as part of the organization's quality assurance program, while the insurance industry relies on risk management techniques when setting insurance rates. Each industry thus uses a definition that is uniquely tailored to its context. No universally accepted definition of risk exists.

Three Conditions of Risk

Whereas specific definitions of risk might vary, a few characteristics are common to all definitions. For risk to exist in any circumstance, the following three conditions must be satisfied [Charette 1990]:

1. The potential for loss must exist.
2. Uncertainty with respect to the eventual outcome must be present.[1]
3. Some choice or decision is required to deal with the uncertainty and potential for loss.

Basic Definition of Risk

These three characteristics can be used to forge a very basic definition of the word *risk*. Most definitions focus on the first two conditions—loss and uncertainty—because they are the two measurable aspects of risk. Thus, the essence of risk, no matter what the domain, can be succinctly captured by the following definition: *Risk is the possibility of suffering loss* [Dorofee 1996].

[1] Some researchers separate the concepts of certainty (the absence of doubt), risk (where the probabilities of alternative outcomes are known), and uncertainty (where the probabilities of possible outcomes are unknown). However, because uncertainty is a fundamental attribute of risk, we do not differentiate between decision making under risk and decision making under uncertainty in this technical report.

Components of Risk

As illustrated in Figure 1, a risk can be thought of as a cause-and-effect pair, where the threat is the cause and the resulting consequence is the effect. In this context, a *threat* is defined as a circumstance with the potential to produce loss, while a *consequence* is defined as the loss that will occur when a threat is realized [Alberts 2009].

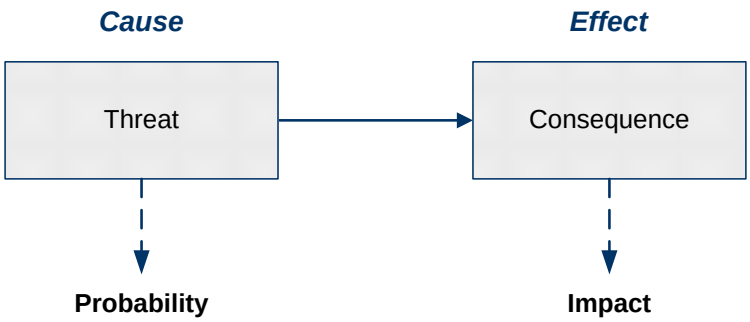

Figure 1: Components of Risk

Risk Measures

Three measures are associated with a risk: (1) probability, (2) impact, and (3) risk exposure. The relationships between probability and impact and the components of risk are shown in Figure 1. In this context, *probability* is defined as a measure of the likelihood that a threat will occur, while *impact* is defined as a measure of the loss that will occur if the threat is realized. *Risk exposure* provides a measure of the magnitude of a risk based on current values of probability and impact.

Risk Management

Risk management is a systematic approach for minimizing exposure to potential losses. It provides a disciplined environment for

- continuously assessing what could go wrong (i.e., assessing risks)
- determining which risks to address (i.e., setting mitigation priorities)
- implementing actions to address high-priority risks and bring those risks within tolerance

Risk Management Activities

Figure 2 illustrates the three core risk management activities:

- **assess risk**—transform the concerns people have into distinct, tangible risks that are explicitly documented and analyzed
- **plan for risk mitigation**—determine an approach for addressing or mitigating each risk; produce a plan for implementing the approach[2]
- **mitigate risk**—deal with each risk by implementing its defined mitigation plan and tracking the plan to completion

These three activities form the foundation of the Risk Management Framework.

Figure 2: Risk Management Activities

[2] No universal definition for the term *mitigation* exits. In fact, various risk management standards and guidelines use this term quite differently. In this report, we define *mitigation* broadly as any action taken to address a risk.

Issue/Problem

One of the fundamental conditions of risk is uncertainty regarding its occurrence. A risk, by definition, might or might not occur. In contrast, an *issue*[3] (also referred to as a *problem* in many contexts) is a loss or adverse consequence that has occurred or is certain to occur. With an issue, no uncertainty exists—the loss or adverse consequence has taken place or is certain to take place.[4] Issues can also lead to (or contribute to) other risks by

- creating a circumstance that produces a new threat
- making an existing threat more likely to occur
- aggravating the consequences of existing risks

Opportunity

Risk is focused on the potential for loss; it does not address the potential for gain. The concept of opportunity is used to address the potential for gain. An *opportunity* is the likelihood of realizing a gain from an allocation or reallocation of resources. Opportunity defines a set of circumstances that provides the potential for a desired gain and requires an investment or action to realize that gain (i.e., to take advantage of the opportunity). Pursuit of an opportunity can produce new risks or issues, and it can also change existing risks or issues.

Focus of the Risk Management Framework

The Risk Management Framework (hereafter also referred to as "the framework") defines activities that are required to manage risk effectively. *Activities for managing issues and opportunities are not explicitly specified in the Risk Management Framework.* While risk management can be integrated with issue and opportunity management [Alberts 2009], the details for achieving an integrated approach for managing risks, issues, and opportunities is beyond the scope of this report.

---

[3] People do not always find it easy to distinguish between an issue and the future risk posed by that issue (if left uncorrected). This confusion can result in issues being documented in a risk database and being treated like risks (and vice versa). Management must take great care to ensure that their approaches for managing issues and risks are integrated appropriately and understood by both management and staff.

[4] Many of the same tools and techniques can be applied to both issue and risk management.

3 Framework Overview

Introduction

This section presents an overview of the Risk Management Framework. Figure 3 shows the three phases of the framework. The main goal of the framework is to specify the core sequence of activities that must be executed when performing risk management (Phase 2). However, because risk management must be conducted within a broader context or environment, the framework also specifies activities to prepare for risk management (Phase 1) as well as to sustain and improve the risk management practice over time (Phase 3).

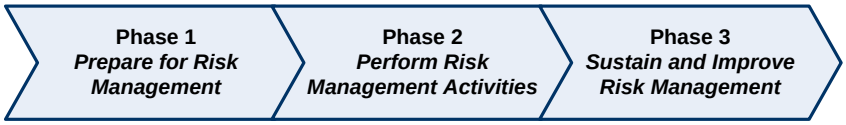

Figure 3: Framework Structure

Risk Management Framework: Three Phases

Phase 1 ("Prepare for Risk Management") is used to get ready for the other two phases. Phase 1 activities should be complete before activities in the other phases are executed. Phase 2 ("Perform Risk Management Activities") defines a set of activities for managing risk. Phase 2 activities are continually performed to ensure that the overall risk to key objectives is effectively managed over time. The activities of Phase 3 ("Sustain and Improve Risk Management") are normally performed on a periodic basis to ensure that the risk management practice remains effective over time. Phase 3 activities are used to identify improvements to a risk management practice. While Phase 1 is generally completed prior to beginning the other two, Phases 2 and 3 are typically executed concurrently.

Specifying Framework Phases

The following common elements are used to specify each phase of the framework:

- description of the phase
- key questions answered by the phase
- dataflow for the phase that highlights the phase's inputs, constraints, resources, and outputs
- description of each input required by the activities performed in the phase
- description of each constraint affecting activities performed in the phase
- description of each resource required by activities performed in the phase
- description of each output produced by the activities performed in the phase
- description of each activity that must be performed in the phase

Specifying Phase 2 Activities

Phase 2 is described in more detail than the other phases because it specifies the distinct sequence of activities that uniquely defines a risk management practice. Phase 2 of the framework comprises the following three activities:

- Activity 2.1: Assess Risk
- Activity 2.2: Plan for Risk Mitigation
- Activity 2.3: Mitigate Risk

The following common elements are used to specify each Phase 2 activity:

- description of the activity
- key questions answered by the activity
- dataflow of inputs and outputs for the activity
- descriptions of each input to the activity
- descriptions of each output produced by the activity
- circumstances that trigger execution of the activity
- description of each sub-activity that must be performed when conducting the activity

Dataflow Diagrams

Dataflow diagrams are used to document phases and activities in the Risk Management Framework. Figure 4 shows the structures of the dataflow diagrams for a phase and an activity.

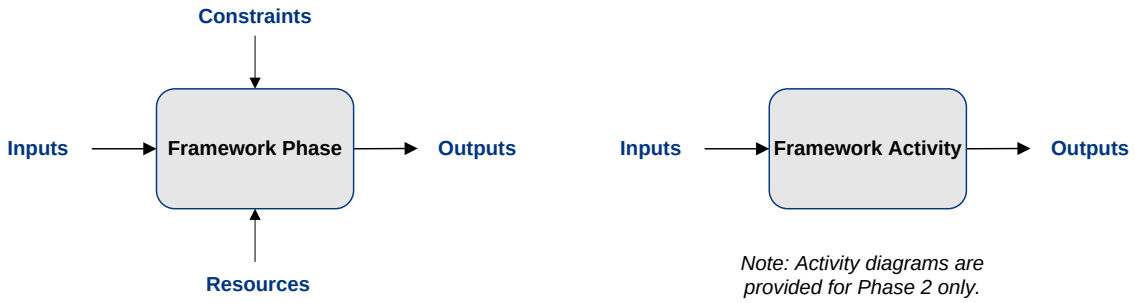

Figure 4: Structure of Dataflow Diagrams

Note that dataflow diagrams include the following four elements:

- inputs—items that are used by a phase or activity to produce an output or result
- outputs—the results that are produced by a phase or activity
- constraints—items that restrict the execution of a phase and its activities
- resources—items that can be used during the execution of a phase and its activities

In the Risk Management Framework, dataflow diagrams for activities are documented only for Phase 2. Because Phase 2 defines the core risk management activities, additional details are provided for that phase of the framework. Dataflow diagrams are not provided for the activities of Phases 1 and 3.

Notice that the dataflow structure for a Phase 2 activity does not include constraints and resources. (Refer to Figure 4.) Phase 2 constraints and resources influence all activities that are performed during that phase. For simplicity, Phase 2 constraints and resources are documented in the Phase 2 diagram only; they are not replicated in each activity diagram for Phase 2.

Dataflow Identifiers

Each input, output, constraint, and resource included in a dataflow is represented by an identifier, which includes a prefix and a number. The prefix is based on the type of data and the number represents a specific data element of that type. For example:

- C1 is the first risk management constraint (affects all phases).
- R3 is the third risk management resource (affects Phases 1 and 3).
- PI1 is the first input to Phase 1 (preparation).
- O4 is the fourth output of Phase 2 (conduct risk management).
- SO2 is the second output of Phase 3 (sustainment and improvement).

The prefixes used in the dataflow diagrams are listed in Table 1.

Table 1: Prefixes Used in the Dataflow Diagrams

Assessment Phase	Prefixes
Phase 1	*PI* is an input to ***p***reparation activities.
	PO is an output that is produced when ***p***reparation activities are performed.
	C is a constraint.
	R is a resource.
Phase 2	*I* is an input to the core risk management activities of Phase 2.
	O is an output produced when the core risk management activities of Phase 2 are performed.
	C is a constraint.
	PO is an output of Phase 1 that either acts as a constraint or is used as a resource during Phase 2.
Phase 3	*SI* is an input to ***s***ustainment and improvement activities.
	SO is an output that is produced when ***s***ustainment and improvement activities are performed.
	C is a constraint.
	R is a resource.

Specifying Framework Requirements

One of the objectives of the framework is to provide a basis for evaluating and improving risk management practice for a program or organization. Requirements have been specified for each output in the framework. These requirements provide the basis for evaluating a risk management practice. Requirements are presented for the following phases and activities:

- Phase 1: Prepare for Risk Management
- Phase 2: Perform Risk Management Activities, Activity 2.1: Assess Risk
- Phase 2: Perform Risk Management Activities, Activity 2.2: Plan for Risk Mitigation
- Phase 2: Perform Risk Management Activities, Activity 2.3: Mitigate Risk
- Phase 3: Sustain and Improve Risk Management

A set of worksheets that can be used to evaluate a risk management practice and establish conformance with the Risk Management Framework is provided in the appendix of this report.

Framework Specification: Structure

The basic structure of the Risk Management Framework is defined as:

- Phase 1: Prepare for Risk Management
- Phase 2: Perform Risk Management Activities
  - Activity 2.1: Assess Risk
  - Activity 2.2: Plan for Risk Mitigation
  - Activity 2.3: Mitigate Risk
- Phase 3: Sustain and Improve Risk Management
- Framework Requirements

This structure forms the basis for the remainder of this report.

4 Prepare for Risk Management (Phase 1)

Description

In this phase, preparation activities for risk management are performed.

Key Questions

This phase answers the following questions:

- Who is sponsoring risk management?
- How can stakeholder sponsorship be attained?
- What is the plan for conducting risk management?
- What resources are required to effectively conduct risk management?

Dataflow

The following dataflow describes the inputs and outputs of this phase.

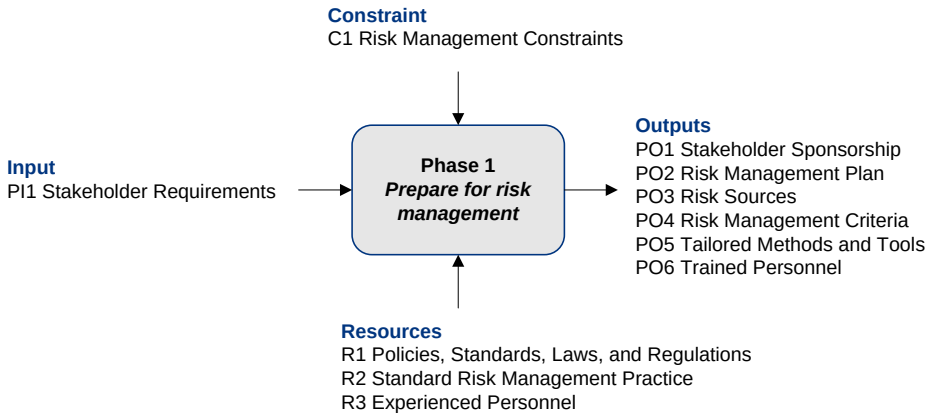

Figure 5: Dataflow for Phase 1

Input

The following is the input to this phase.

Input	Description
PI1 Stakeholder Requirements	The needs of the key stakeholders regarding risk management

Constraint

The following is the constraint for this phase.

Constraint	Description
C1 Risk Management Constraints	Any circumstances, including logistics, standards, laws, regulations, personnel, schedule, and cost issues that could affect risk management activities

Resources

The following are the resources required by this phase.

Resource	Description
R1 Policies, Standards, Laws, and Regulations	Any informative policies, standards, laws, and regulations that guide the implementation of the risk management practice
R2 Standard Risk Management Practice	The accepted practice for implementing risk management, including methods, tools, procedures, criteria, worksheets, automated support tools, and databases. The standard risk management practice must be tailored for each specific application of risk management (e.g., program, organization, technology).
R3 Experienced Personnel[5]	A core group of people who are collectively experienced in all phases of risk management. Risk management roles and responsibilities for these people are defined, and they have received training that is appropriate for their roles and responsibilities.

[5] This core group of experienced personnel is responsible for setting up and sustaining an effective risk management practice. Other personnel who will also be performing risk management activities will be trained as needed.

Outputs

The following are the outputs of this phase.

Output	Description
PO1 Stakeholder Sponsorship	Active and visible support of risk management by key stakeholders and decision makers
PO2 Risk Management Plan	The activities a program intends to perform when conducting risk management. Examples of items commonly found in a risk management plan include ▪ the objectives of the risk management effort ▪ the scope of the risk management effort (e.g., actively participating groups and teams, support groups, interfaces) ▪ resources (e.g., personnel, funding, technology, facilities, and equipment) needed to conduct risk management ▪ roles and responsibilities for conducting risk management ▪ description of the risk management method being employed ▪ relationships and dependencies with other management practices (e.g., project, problem/issue, or opportunity management) ▪ pointers to the procedures, artifacts, and tools used in each risk management activity ▪ the sources of risk being assessed ▪ all relevant criteria for conducting risk management activities, including the criteria for probability, impact, and risk exposure ▪ a communication framework that describes formal paths for sharing risk information among key stakeholders ▪ time intervals and other triggers for establishing risk baselines ▪ effectiveness measures used to evaluate the risk management practice
PO3 Risk Sources	The causes of risk that will be assessed (this should be kept current)
PO4 Risk Management Criteria	The parameters used when managing risks, including ▪ probability, impact, and risk exposure criteria ▪ decision-making criteria (e.g., for prioritizing risks during mitigation or deciding when to escalate risks within a program or organization) ▪ criteria that establish risk tolerance ▪ criteria for communicating with collaborators and partners as well as with senior management
PO5 Tailored Methods and Tools	The methods and tools that will be used when conducting risk management, including procedures, criteria, worksheets, automated support tools, and databases. Methods and tools are usually tailored from a standard set for a specific application of risk management (e.g., program, organization, technology).
PO6 Trained Personnel[6]	The people who are tasked with performing risk management activities and are prepared to conduct them

[6] The majority of personnel in a program typically receive awareness training to enable them to effectively identify risks or bring them to the attention of those responsible for risk management activities. Other people can receive more specialized training based on their roles in the risk management process.

Activities

The following activities are performed in this phase.

Activity	Description
1.1 Develop stakeholder sponsorship	Meet with key stakeholders and decision makers to foster their active, visible, and continuous support of risk management and gather their requirements.
1.2 Develop risk management plan	Create the plan for conducting risk management based on requirements and constraints (e.g., schedule, funding, logistics, and contractual restrictions). *Note*: The risk management plan needs to be consistent with applicable policies, standards, laws, and regulations.
1.3 Tailor methods and tools	Adapt the risk management methods and tools (e.g., procedures, criteria, worksheets, automated support tools, databases) for the specific application of risk management (e.g., program, organization, technology).
1.4 Train personnel	Ensure that all of the people who will participate in risk management are able to effectively perform their assigned roles and responsibilities.

5 Perform Risk Management Activities (Phase 2)

Description

In this phase, risk management activities are performed as planned.

Key Questions

This phase answers the following questions:

- What risks could affect the achievement of key program objectives?
- How will each risk be addressed?
- What needs to be done to ensure that each risk is maintained within an acceptable tolerance over time?
- Is each mitigation plan having its intended effect?

Dataflow

The following dataflow describes the inputs and outputs of this phase.

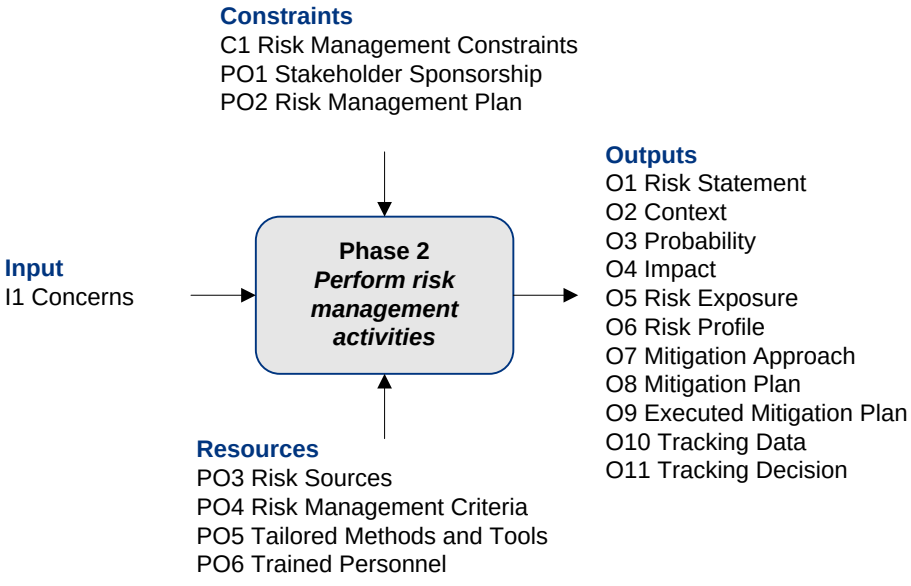

Figure 6: Dataflow for Phase 2

Input

The following is the input to this phase.

Input	Description
I1 Concerns	Doubts, worries, and unease about how current conditions and potential events might adversely affect the ability to achieve key objectives

Constraints

The following are the constraints for this phase.[7]

Constraint	Description
C1 Risk Management Constraints	Any circumstances, including logistics, standards, laws, regulations, personnel, schedule, and cost issues that could affect risk management activities
PO1 Stakeholder Sponsorship	Active and visible support of risk management by key stakeholders and decision makers.
PO2 Risk Management Plan	The activities a program intends to perform when conducting risk management. Examples of items commonly found in a risk management plan include ▪ the objectives of the risk management effort ▪ the scope of the risk management effort (e.g., actively participating groups and teams, support groups, interfaces) ▪ resources (e.g., personnel, funding, technology, facilities, and equipment) needed to conduct risk management ▪ roles and responsibilities for conducting risk management ▪ description of the risk management method being employed ▪ relationships and dependencies with other management practices (e.g., project, problem/issue, or opportunity management) ▪ pointers to the procedures, artifacts, and tools used in each risk management activity ▪ the sources of risk being assessed ▪ all relevant criteria for conducting risk management activities, including the criteria for probability, impact, and risk exposure ▪ a communication framework that describes formal paths for sharing risk information among key stakeholders ▪ time intervals and other triggers for establishing risk baselines ▪ effectiveness measures used to evaluate the risk management practice

[7] Constraints affect all activities performed during Phase 2. Similarly, resources are used to aid the completion of all activities performed during Phase 2. The definitions for all Phase 2 constraints and resources are provided in this section only. They are not replicated in the sections for individual Phase 2 activities.

Resources

The following are the resources required by this phase.

Resource	Description
PO3 Risk Sources	The causes of risk that will be assessed (this should be kept current)
PO4 Risk Management Criteria	The parameters used when managing risks, including ▪ probability, impact, and risk exposure criteria ▪ decision-making criteria (e.g., for prioritizing risks during mitigation or deciding when to escalate risks within a program or organization) ▪ criteria that establish risk tolerance ▪ criteria for communicating with collaborators and partners as well as with senior management
PO5 Tailored Methods and Tools	The methods and tools that will be used when conducting risk management, including procedures, criteria, worksheets, automated support tools, and databases. Methods and tools are usually tailored from a standard set for a specific application of risk management (e.g., program, organization, technology).
PO6 Trained Personnel	The people who are tasked with performing risk management activities and are prepared to conduct them

Outputs

The following are the outputs of this phase.[8]

Output	Description
O1 Risk Statement	A succinct and unique description of a risk. Risk statements typically describe (1) a circumstance with the potential to produce loss (i.e., threat) and (2) the loss that will occur if that circumstance is realized (i.e., consequence). *Note*: A risk statement does not have to be documented using text. For example, a graphical expression or model can also be used to provide a succinct and unique description of a risk.
O2 Context	Additional information essential for characterizing a risk, including any relevant background information about the risk, elaborations about the threat and consequence, any aggravating or mitigating conditions, and relationships and dependencies with other risks
O3 Probability	A measure of the likelihood that a risk will occur
O4 Impact	A measure of the severity of a risk's consequence if the risk were to occur
O5 Risk Exposure	A measure of the magnitude of a risk based on current values of probability and impact

[8] Outputs O1 through O5 will exist for each risk that is identified. Output O6 provides a snapshot of all risks that are identified. Output O7 will exist for each risk that is identified. Finally, outputs O8 through O11 will exit for each risk that is being actively mitigated.

Output	Description
06 Risk Profile	A snapshot or summary of all risks relevant to the specific application of risk management (e.g., program, organization, technology)
O7 Mitigation Approach	A strategy for addressing a risk. Examples of common mitigation approaches include ▪ accept—If a risk occurs, its consequences will be tolerated; no proactive action to address the risk will be taken. When a risk is accepted, the rationale for doing so is documented. ▪ transfer—A risk is shifted to another party (e.g., through insurance or outsourcing). ▪ avoid—Activities are restructured to eliminate the possibility of a risk occurring. ▪ control—Actions are implemented in an attempt to reduce or contain a risk.
O8 Mitigation Plan	A set of actions for implementing the selected mitigation approach. Examples of items commonly found in a mitigation plan include ▪ objectives of the plan ▪ resources allocated to the plan ▪ responsibility for completing each action in the plan ▪ a schedule for completing all actions in the plan ▪ the funding allocated to performing the plan's actions ▪ measures for tracking the execution of the plan (in relation to the schedule and cost) and the effectiveness of the plan ▪ a contingency plan and triggers when appropriate *Note*: Changes in probability, impact, and risk exposure (i.e., residual risk) are often used to track a plan's effectiveness.
O9 Executed Mitigation Plan	A set of completed actions (as outlined in a mitigation plan)
O10 Tracking Data	Specific data that are gathered when monitoring the progress of a mitigation plan
O11 Tracking Decision	Reaching a conclusion or determination about what action(s) to take related to a mitigation plan. Examples of common tracking decisions include ▪ continue implementing the mitigation plan as intended ▪ modify the mitigation approach and develop a new plan as appropriate ▪ modify the mitigation plan ▪ implement the contingency plan (if one exists) ▪ close the risk

Importance of Open Communication

Effective communication among all stakeholders ensures that information, plans, actions, concerns, and progress are known. Risk communication is not a separate activity; it is embedded in all other risk management activities. The importance of communication is highlighted by its emphasis in the risk management plan, where a communication framework for sharing risk information among key stakeholders is documented.

Success cannot be achieved if risk information is not communicated to and understood by the organization's decision makers and stakeholders. Open communication requires

- risk management activities that are built upon collaborative approaches
- encouraging exchanges of risk information among all levels of an organization
- using consensus-based processes that value the individual voice

Activities

The following activities are performed in this phase.

Activity	Description
2.1 Assess risk	Transform concerns into distinct, tangible risks that are explicitly documented and measured
2.2 Plan for risk mitigation	Determine an approach for addressing or mitigating each risk, and produce a plan for implementing the approach
2.3 Mitigate risk	Deal with each risk by implementing its defined mitigation plan and tracking it to completion

5.1 Assess Risk (Activity 2.1)

Description

This activity transforms concerns into distinct, tangible risks that are explicitly documented and measured. *Assessing risk is an activity that is performed continually*.

Key Questions

This activity answers the following questions:

- What is the statement of risk?
- What additional information is important for understanding this risk?
  - What are the root causes of the risk?
  - What conditions aggravate or mitigate the risk?
  - What are the relationships and dependencies with other risks?
- What is the likelihood that the risk will occur?
- What is the severity of the impact if the risk were to occur?
- What is the magnitude of a risk exposure based on current values of probability and impact?
- What is the current snapshot or profile of all risks?

Dataflow

The following dataflow describes the inputs and outputs of this activity.

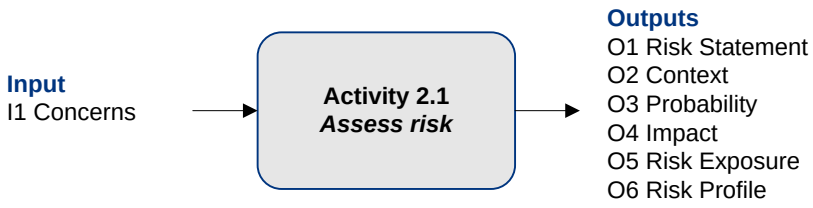

Figure 7: Dataflow for Activity 2.1

Input

The following is the input to this activity.

Input	Description
I1 Concerns	Doubts, worries, and unease about how current conditions and potential events might adversely affect the ability to achieve key objectives

Outputs

The following are the outputs of this activity.

Output	Description
O1 Risk Statement	A succinct and unique description of a risk. Risk statements typically describe (1) a circumstance with the potential to produce loss (i.e., threat) and (2) the loss that will occur if that circumstance is realized (i.e., consequence). *Note*: A risk statement does not have to be documented using text. For example, a graphical expression or model can also be used to provide a succinct and unique description of a risk.
O2 Context	Additional information essential for characterizing a risk, including any relevant background information about the risk, elaborations about the threat and consequence, any aggravating or mitigating conditions, and relationships and dependencies with other risks
O3 Probability	A measure of the likelihood that a risk will occur
O4 Impact	A measure of the severity of a risk's consequence if the risk were to occur
O5 Risk Exposure	A measure of the magnitude of a risk based on current values of probability and impact
06 Risk Profile	A snapshot or summary of all risks relevant to the specific application of risk management (e.g., program, organization, technology)

Activity Triggers

The following situations will trigger this activity:

- A risk evaluation, appraisal, or audit is scheduled to be performed.
- Someone raises a new concern that could affect the ability to achieve key objectives.
- Conditions indicate a potential change in the current risk profile.
- A tracking decision requires a risk to be reassessed.

Sub-Activities

The following table describes the sub-activities performed when conducting this activity.

Sub-Activity	Description	Outputs
2.1.1 Identify risk	A concern is transformed into a distinct, tangible risk that can be described and measured. *Note*: Risks that are related can be grouped to provide an aggregate view of risk to objectives. A risk statement for the group is documented, and the statement for the group is carried forward in the rest of the risk management activities.[9] Aggregating risks in this manner helps keep the total number of risks to a manageable level without losing the broader view.	O1 Risk Statement O2 Context
2.1.2 Analyze risk	The risk is evaluated in relation to predefined criteria to determine its probability, impact, and risk exposure. *Note*: Measures for existing risks must be re-evaluated on a periodic basis. *Note*: Some risk management methods include *timeframe* as a risk measure. Timeframe is the period when action is required in order to mitigate a risk. However, timeframe is not a standard risk measure; many methods do not use it. For this reason, it is not included as a standard output in the framework.	O3 Probability O4 Impact O5 Risk Exposure
2.1.3 Develop risk profile	A snapshot or summary of all risks relevant to the specific application of risk management (e.g., program, organization, or technology) is developed and documented. The risk profile should be shared with all relevant stakeholders as appropriate.	O6 Risk Profile

[9] When multiple risks are grouped into an aggregate risk, a new risk statement is documented for the aggregate risk. The aggregate risk is handled the same as other risks from this point forward in the process.

5.2 Plan for Risk Mitigation (Activity 2.2)

Description

This activity determines an approach for addressing or mitigating a risk, and produces a plan for implementing the approach.

Key Questions

This activity answers the following questions for each risk:

- How will the risk be addressed?
- What is the plan for mitigating the risk?
  - What are the objectives of the mitigation plan?
  - Who is responsible for completing each action in the plan?
  - When will each action be completed?
  - How much funding is allocated to executing the plan?
  - What are the requirements for tracking the risk mitigating plan's execution and effectiveness?
  - Is a contingency plan needed for the risk? If so, what it the contingency plan?

Dataflow

The following dataflow describes the inputs and outputs of this activity.

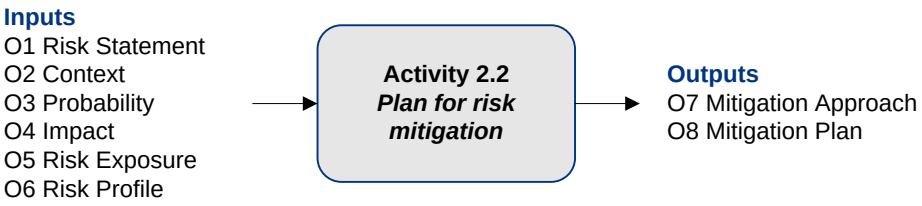

Figure 8: Dataflow for Activity 2.2

Inputs

The following are the inputs to this activity.

Input	Description
O1 Risk Statement	A succinct and unique description of a risk. Risk statements typically describe (1) a circumstance with the potential to produce loss (i.e., threat) and (2) the loss that will occur if that circumstance is realized (i.e., consequence). *Note*: A risk statement does not have to be documented using text. For example, a graphical expression or model can also be used to provide a succinct and unique description of a risk.
O2 Context	Additional information essential for characterizing a risk, including any relevant background information about the risk, elaborations about the threat and consequence, any aggravating or mitigating conditions, and relationships and dependencies with other risks
O3 Probability	A measure of the likelihood that a risk will occur
O4 Impact	A measure of the severity of a risk's consequence if the risk were to occur
O5 Risk Exposure	A measure of the magnitude of a risk based on current values of probability and impact
06 Risk Profile	A snapshot or summary of all risks relevant to the specific application of risk management (e.g., program, organization, technology)

Outputs

The following are the outputs of this activity.

Output	Description
O7 Mitigation Approach	A strategy for addressing a risk. Examples of common mitigation approaches include ▪ accept—If a risk occurs, its consequences will be tolerated; no proactive action to address the risk will be taken. When a risk is accepted, the rationale for doing so is documented. ▪ transfer—A risk is shifted to another party (e.g., through insurance or outsourcing). ▪ avoid—Activities are restructured to eliminate the possibility of a risk occurring. ▪ control—Actions are implemented in an attempt to reduce or contain a risk.

Output	Description
O8 Mitigation Plan	A set of actions for implementing the selected mitigation approach. Examples of items commonly found in a mitigation plan include ▪ objectives of the plan ▪ resources allocated to the plan ▪ responsibility for completing each action in the plan ▪ a schedule for completing all actions in the plan ▪ the funding allocated to performing the plan's actions ▪ measures for tracking the execution of the plan (in relation to the schedule and cost) and the effectiveness of the plan ▪ a contingency plan and triggers when appropriate *Note*: Changes in probability, impact, and risk exposure (i.e., residual risk) are often used to track a plan's effectiveness.

Activity Triggers

The following situations will trigger this activity:

- A risk has been assessed (or reassessed).
- A tracking decision
  - changes the mitigation approach
  - calls for a new or modified mitigation plan

Sub-Activities

The following table describes the sub-activities performed when conducting this activity.

Sub-Activity	Description	Outputs
2.2.1 Determine mitigation approach	The strategy for addressing a risk is based on the current measures for the risk (i.e., probability, impact, and risk exposure). Decision-making criteria (e.g., for prioritizing risks during mitigation or deciding when to escalate risks within a program or organization) may also be used to help determine the appropriate strategy for addressing a risk. Common mitigation approaches include ▪ accept—If a risk occurs, its consequences will be tolerated; no proactive action to address the risk will be taken. When a risk is accepted, the rationale for doing so is documented. ▪ transfer—A risk is shifted to another party (e.g., through insurance or outsourcing). ▪ avoid—Activities are restructured to eliminate the possibility of a risk occurring. ▪ control—Actions are implemented in an attempt to reduce or contain a risk. Mitigation approaches should be shared with all relevant stakeholders as appropriate.	O7 Mitigation Approach

Sub-Activity	Description	Outputs
2.2.2 Develop mitigation plan	A mitigation plan is defined and documented. Mitigation plans should be shared with all relevant stakeholders as appropriate. *Note*: More than one risk might share a common root cause. Relationships between risks (including those within an aggregate risk or between the smaller risks in different aggregate groups) can point to more effective mitigation actions. Mitigation actions should maximize the return on investment for resources.	O8 Mitigation Plan

5.3 Mitigate Risk (Activity 2.3)

Description

This activity deals with the risk by implementing the defined mitigation plan and tracking it to completion.

Key Questions

This activity answers the following questions for each mitigation plan:

- Is the mitigation plan being implemented as planned?
- Is the mitigation plan having its intended effect?
- Based on tracking data, do any corrective actions need to be taken?

Dataflow

The following dataflow describes the inputs and outputs of this activity.

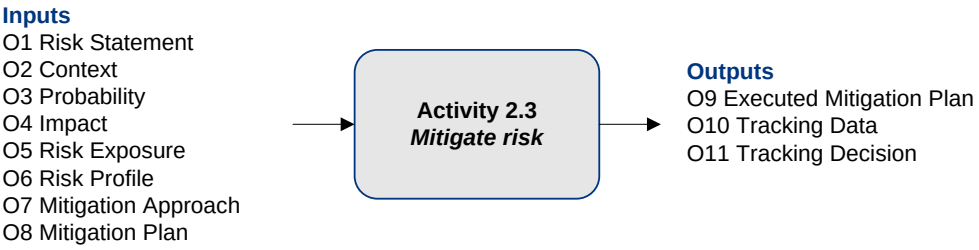

Figure 9: Dataflow for Activity 2.3

Inputs

The following are the inputs to this activity.

Input	Description
O1 Risk Statement	A succinct and unique description of a risk. Risk statements typically describe (1) a circumstance with the potential to produce loss (i.e., threat) and (2) the loss that will occur if that circumstance is realized (i.e., consequence). *Note*: A risk statement does not have to be documented using text. For example, a graphical expression or model can also be used to provide a succinct and unique description of a risk.
O2 Context	Additional information essential for characterizing a risk, including any relevant background information about the risk, elaborations about the threat and consequence, any aggravating or mitigating conditions, and relationships and dependencies with other risks
O3 Probability	A measure of the likelihood that a risk will occur

Input	Description
O4 Impact	A measure of the severity of a risk's consequence if the risk were to occur
O5 Risk Exposure	A measure of the magnitude of a risk based on current values of probability and impact
06 Risk Profile	A snapshot or summary of all risks relevant to the specific application of risk management (e.g., program, organization, technology)
O7 Mitigation Approach	A strategy for addressing a risk. Examples of common mitigation approaches include ▪ accept—If a risk occurs, its consequences will be tolerated; no proactive action to address the risk will be taken. When a risk is accepted, the rationale for doing so is documented. ▪ transfer—A risk is shifted to another party (e.g., through insurance or outsourcing). ▪ avoid—Activities are restructured to eliminate the possibility of a risk occurring. ▪ control—Actions are implemented in an attempt to reduce or contain a risk.
O8 Mitigation Plan	A set of actions for implementing the selected mitigation approach. Examples of items commonly found in a mitigation plan include ▪ objectives of the plan ▪ resources allocated to the plan ▪ responsibility for completing each action in the plan ▪ a schedule for completing all actions in the plan ▪ the funding allocated to performing the plan's actions ▪ measures for tracking the execution of the plan (in relation to the schedule and cost) and the effectiveness of the plan ▪ a contingency plan and triggers when appropriate *Note*: Changes in probability, impact, and risk exposure (i.e., residual risk) are often used to track a plan's effectiveness.

Outputs

The following are the outputs of this activity.

Output	Description
O9 Executed Mitigation Plan	A set of completed actions (as outlined in a mitigation plan)
O10 Tracking Data	Specific data that are gathered when monitoring the progress of a mitigation plan
O11 Tracking Decision	Reaching a conclusion or determination about what action(s) to take related to a mitigation plan. Examples of common tracking decisions include ▪ continue implementing the mitigation plan as intended ▪ modify the mitigation approach and develop a new plan as appropriate ▪ modify the mitigation plan ▪ implement the contingency plan (if one exists) ▪ close the risk

Activity Trigger

The following situation will trigger this activity: a mitigation plan has been developed or modified.

Sub-Activities

The following table describes the sub-activities performed when conducting this activity.

Sub-Activity	Description	Outputs
2.3.1 Implement mitigation plan	The mitigation plan (or the contingency plan) is executed as intended.	O9 Executed Mitigation Plan
2.3.2 Track mitigation plan	The measures for tracking the action plan's execution are collected and analyzed as specified in the mitigation plan. Tracking data should be shared with all relevant stakeholders as appropriate.	O10 Tracking Data
2.3.3 Make tracking decision	A decision about whether to take corrective action(s) related to a risk or it's mitigation plan is made. Tracking decisions should be shared with all relevant stakeholders as appropriate.	O11 Tracking Decisions

6 Sustain and Improve Risk Management (Phase 3)

Description

In this phase, activities are performed to sustain and improve risk management effort over time.

Key Questions

This phase answers the following questions:

- Which risk management assets (e.g., methods, tools) and work products (e.g., risk profile, mitigation plans) need to be under configuration control?
- What lessons were learned when preparing for risk management?
- What lessons were learned when conducting risk management?
- How does the risk management practice (e.g., plan, methods, tools, resources, training) need to be updated or improved?

Dataflow

The following dataflow describes the inputs and outputs of this phase.

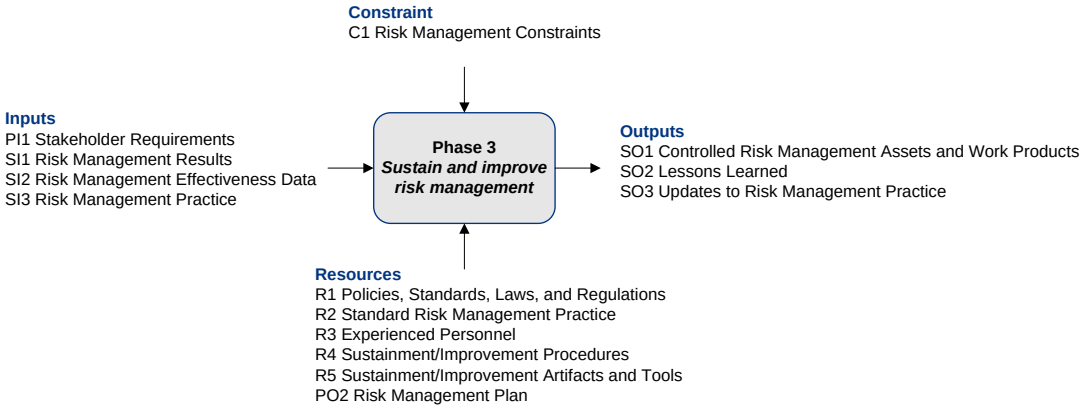

Figure 10: Dataflow for Phase 3

Inputs

The following are the inputs to this phase.

Input	Description
PI1 Stakeholder Requirements	The needs of the key stakeholders regarding risk management
SI1 Risk Management Results	All outputs and data produced when preparing for and conducting risk management, including the risk management plan, risks, mitigation plans, and risk tracking data
SI2 Risk Management Effectiveness Data	Specific data that are gathered to evaluate the effectiveness of the risk management practice
SI3 Risk Management Practice	The accepted approach for performing risk management activities, including the risk management plan, methods, tools, resources, and training

Constraint

The following is the constraint for this phase.

Constraint	Description
C1 Risk Management Constraints	Any circumstances, including logistics, standards, laws, regulations, personnel, schedule, and cost issues that could affect risk management activities

Resources

The following are the resources required by this phase.

Resource	Description
R1 Policies, Standards, Laws, and Regulations	Any informative policies, standards, laws, and regulations that guide the implementation of the risk management practice
R2 Standard Risk Management Practice	The accepted practice for implementing risk management, including methods, tools, procedures, criteria, worksheets, automated support tools, and databases. The standard risk management practice must be tailored for each specific application of risk management (e.g., program, organization, technology).
R3 Experienced Personnel	A core group of people who are collectively experienced in all phases of risk management. Risk management roles and responsibilities for these people are defined, and they have received training that is appropriate for their roles and responsibilities.
R4 Sustainment/ Improvement Procedures	Documentation that describes how to conduct sustainment and improvement activities
R5 Sustainment/ Improvement Artifacts and Tools	Basic items that can be used when conducting sustainment and improvement activities, including templates, worksheets, standard presentations, automated tools, and databases

Resource	Description
PO2 Risk Management Plan	The activities a program intends to perform when conducting risk management. Examples of items commonly found in a risk management plan include ▪ the objectives of the risk management effort ▪ the scope of the risk management effort (e.g., actively participating groups and teams, support groups, interfaces) ▪ resources (e.g., personnel, funding, technology, facilities, and equipment) needed to conduct risk management ▪ roles and responsibilities for conducting risk management ▪ description of the risk management method being employed ▪ relationships and dependencies with other management practices (e.g., project, problem/issue, or opportunity management) ▪ pointers to the procedures, artifacts, and tools used in each risk management activity ▪ the sources of risk being assessed ▪ all relevant criteria for conducting risk management activities, including the criteria for probability, impact, and risk exposure ▪ a communication framework that describes formal paths for sharing risk information among key stakeholders ▪ time intervals and other triggers for establishing risk baselines ▪ effectiveness measures used to evaluate the risk management practice

Outputs

The following are the outputs of this phase.

Output	Description
SO1 Controlled Risk Management Assets and Work Products	Selected risk management assets (e.g., methods, tools) and work products (e.g., risk profile, mitigation plans) that are under configuration control
SO2 Lessons Learned	Knowledge gained by preparing for and conducting risk management activities that can be used to modify and improve the risk management practice
SO3 Updates to Risk Management Practice	Any changes to the risk management practice (e.g., changes to the risk management plan, methods, tools, resources, training) to improve the efficiency and effectiveness of its application

Activities

The following activities are performed in this phase.

Activity	Description
3.1 Manage risk management assets and work products	Place designated assets (e.g., methods, tools) and work products (e.g., risk profile, mitigation plans) of the risk management practice under appropriate levels of control.
3.2 Evaluate effectiveness of risk management practice	Analyze risk management results and effectiveness measures (as specified in the risk management plan) to identify and document lessons learned regarding the strengths and weaknesses of the risk management practice (e.g., risk management plan, methods, tools, resources, training).
3.3 Implement improvements to risk management practice	Make identified changes to the risk management practice (e.g., changes to the risk management plan, methods, tools, resources, training) based on lessons learned.

7 Framework Requirements

Framework Requirements

Framework requirements define criteria that are used to establish conformance with the Risk Management Framework. A requirement is specified for each output in the framework. Requirements are presented for the following phases and activities:

- Phase 1: Prepare for Risk Management
- Phase 2: Perform Risk Management Activities, Activity 2.1: Assess Risk
- Phase 2: Perform Risk Management Activities, Activity 2.2: Plan for Risk Mitigation
- Phase 2: Perform Risk Management Activities, Activity 2.3: Mitigate Risk
- Phase 3: Sustain and Improve Risk Management

The appendix of this document provides a set of worksheets for evaluating a risk management practice against the framework requirements.

Phase 1 Requirements

The following are the framework requirements for *Phase 1: Prepare for Risk Management*.

Requirement		Related Output	
REQ 1	Support of risk management by key stakeholders is tangible, active, and visible. *Examples of sponsorship* Organizational policies; memos from senior management; resources; funding; risks discussed at management meetings	PO1	Stakeholder Sponsorship
REQ 2	A risk management plan is defined, documented, and approved. *Examples of plan content* Objectives; scope; resources; descriptions of methods and tools; sources of risk; risk management criteria; communication framework; schedule and triggers for conducting evaluations; effectiveness measures	PO2	Risk Management Plan

Requirement		Related Output	
REQ 3	Risk sources are defined, documented, and kept current. *Examples of documents containing risk sources* Publicly available lists and taxonomies; domain-specific lists and taxonomies; organizational lists and taxonomies *Examples of risk categories* Program management, technical, organizational, infrastructure, support services, and product	PO3	Risk Sources
REQ 4	Risk management criteria are defined and documented. *Examples of risk management criteria* Probability, impact, and risk exposure criteria; decision-making criteria (e.g., for escalation or prioritization); criteria that establish risk tolerance; criteria for communicating with collaborators, partners, subcontractors, suppliers, customers, and other stakeholders	PO4	Risk Management Criteria
REQ 5	Methods and tools used to support risk management activities have been appropriately tailored for use. *Examples of methods and tools* Procedures for conducting risk management activities; risk management criteria; risk sources; worksheets; automated support tools; report generators; databases	PO5	Tailored Methods and Tools
REQ 6	People who perform risk management activities are prepared to conduct them. *Examples of people who need training* Managers, technical leads, and staff who participate in risk management activities; risk manager; risk database administrator *Examples of types of training* Awareness training; method training; tool training	PO6	Trained Personnel

Phase 2, Activity 2.1 Requirements

The following are the framework requirements for *Phase 2: Perform Risk Management Activities, Activity 2.1: Assess Risk.*

Requirement		Related Output	
REQ 7	A risk statement is documented for each risk using a standard format. *Examples of items that influence the format and use of risk statements* Organizational guidance for communicating, documenting, and updating risks; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders	O1	Risk Statement

Requirement		Related Output	
REQ 8	Context is documented for each risk. *Examples of items that influence the format and use of context* Organizational guidance for communicating, documenting, and updating risks; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders *Examples of context* Root causes; aggravating conditions; mitigating conditions; relationships and dependencies with other risks	O2	Context
REQ 9	Probability is evaluated and documented for each risk. *Examples of items that influence the use of probability* Probability criteria; organizational guidance for assessing probability; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders	O3	Probability
REQ 10	Impact is evaluated and documented for each risk. *Examples of items that influence the use of impact* Impact criteria; organizational guidance for assessing impact; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders	O4	Impact
REQ 11	Risk exposure is evaluated and documented for each risk. *Examples of items that influence the use of risk exposure* Risk exposure criteria; organizational guidance for assessing risk exposure; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders	O5	Risk Exposure
REQ 12	A profile of all risks is developed, documented, and kept current. *Examples of items that influence the development of a risk profile* Organizational guidance for communicating, documenting, and updating the risk profile; requirements of methods and tools; format of risk statements; risk profile format; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders	O6	Risk Profile

Phase 2, Activity 2.2 Requirements

The following are the framework requirements for *Phase 2: Perform Risk Management Activities, Activity 2.2: Plan for Risk Mitigation*.

Requirement		Related Output	
REQ 13	A mitigation approach is established and documented for each risk. *Examples of items that influence selection of a mitigation approach* Organizational guidance for communicating, documenting, and updating a mitigation approach; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders; risk tolerance; decision-making criteria *Examples of common mitigation approaches* Accept a risk and take no action; transfer a risk to another party; restructure activities to avoid a risk by eliminating the possibility of it occurring; take action to reduce or contain a risk	O7	Mitigation Approach
REQ 14	A mitigation plan is defined and documented for each risk that is actively being addressed. *Examples of items that influence development of a mitigation plan* Organizational guidance for communicating, documenting, and updating a mitigation plan; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders; risk tolerance *Examples of a mitigation plan's content* Objectives for the plan; resources responsible for completing each action; schedule for completing all actions; funding allocated to performing the plan's actions; measures for tracking the execution of the plan (in relation to the schedule and cost); measures for tracking the effectiveness of the plan; a contingency plan and triggers when appropriate	O8	Mitigation Plan

Phase 2, Activity 2.3 Requirements

The following are the framework requirements for *Phase 2: Perform Risk Management Activities, Activity 2.3: Mitigate Risk*.

Requirement		Related Output	
REQ 15	Mitigation plans are implemented as intended (unless circumstances force a change in direction). *Examples of items that influence plan execution* Resources available for plan execution; funding allocated to the plan; responsibility for implementing the plan; authority for implementing plan; verification of completion; visible support of management *Examples of data that can be used to evaluate plan implementation* Tracking measures for effectiveness and efficiency of mitigation plan execution; tracking measures for verifying plan completion; triggers for contingency or alternate plans	O9	Executed Mitigation Plan

Requirement		Related Output	
REQ 16	Data for tracking mitigation plans are collected, analyzed, documented, and reported. *Examples of items that influence collection of tracking data* Organizational guidance for selecting tracking measures; organizational guidance for communicating, documenting, and updating tracking data; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders; approach for collecting measurement data; approach for analyzing measurement data; frequency requirements for collecting tracking data *Examples of types of tracking measures* Tracking measures for effectiveness and efficiency of mitigation plan execution; tracking measures for verifying plan completion; triggers for contingency or alternate plans	O10	Tracking Data
REQ 17	Tracking decisions for mitigation plans are documented appropriately. *Examples of items that influence tracking decisions* Organizational guidance for communicating, documenting, and updating tracking decisions; requirements for approving tracking decisions; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders; decision-making criteria *Examples of common tracking decisions* Modify the mitigation approach and develop a new plan; modify an existing mitigation plan; implement a contingency plan; close a risk	O11	Tracking Decisions

Phase 3 Requirements

The following are the framework requirements for *Phase 3: Sustain and Improve Risk Management*.

Requirement		Related Output	
REQ 18	Selected risk management assets and work products are under configuration control. *Examples of assets under configuration control* Risk management plan; methods and tools; risk sources, risk criteria *Examples of work products under configuration control* Risk profile; mitigation plans; tracking decisions; status reports	SO1	Controlled Risk Management Assets and Work Products
REQ 19	Lessons learned are collected and documented for the risk management practice. *Examples of items that influence lessons learned* Requirements for developing lessons learned; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders; types of effectiveness measures collected for the risk management practice; strengths of the risk management practice; weaknesses of the risk management practice; changes in best practices; new standards or changes to existing standards or regulations; new methods and tools or changes to existing methods and tools	SO3	Lessons Learned

Requirement		Related Output	
REQ 20	The risk management practice is updated as appropriate based on lessons learned. *Examples of items that influence how lessons are incorporated* Change management process; organizational guidance for managing change; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders *Examples of items that could be updated or changed* Risk management plan; funding for risk management; methods; tools; resources; training	SO3	Updates to Risk Management Practice

Appendix: Evaluating a Risk Management Practice

This appendix provides a set of worksheets that can be used to evaluate a risk management practice and establish conformance with the Risk Management Framework. Conformance is established through satisfaction of the framework requirements. Non-conformance to any requirement generally indicates a less effective and potentially inadequate risk management practice.

Directions:

You must complete the following two steps when evaluating each requirement.

1. **Evaluate each requirement in the checklist by checking the most appropriate box. The following table defines the range of responses for each requirement.**

Response	Definition
Satisfied	The requirement is met by the risk management practice.
Partially Satisfied	The requirement is partially met by the risk management practice. Some aspects of the requirement are not met satisfactorily.
Unsatisfied	The requirement is not met by the risk management practice.
Don't Know	More information is needed to evaluate the requirement.

2. **After you evaluate each requirement, document the rationale for your response in the space provided. Note where your response is based on objective data and where it is based on more subjective data, such as opinions.**

Evaluation: Framework Requirements

Requirement	Response
Stakeholder Sponsorship	
1. Support of risk management by key stakeholders is tangible, active, and visible. *Examples of sponsorship* Organizational policies; memos from senior management; resources; funding; risks discussed at management meetings	❑ Satisfied ❑ Partially Satisfied ❑ Unsatisfied ❑ Don't Know
Risk Management Plan	
2. A risk management plan is defined, documented, and approved. *Examples of plan content* Objectives; scope; resources; descriptions of methods and tools; sources of risk; risk management criteria; communication framework; schedule and triggers for conducting evaluations; effectiveness measures	❑ Satisfied ❑ Partially Satisfied ❑ Unsatisfied ❑ Don't Know
Risk Sources	
3. Risk sources are defined, documented, and kept current. *Examples of documents containing risk sources* Publicly available lists and taxonomies; domain-specific lists and taxonomies; organizational lists and taxonomies *Examples of risk categories* Program management, technical, organizational, infrastructure, support services, and product	❑ Satisfied ❑ Unsatisfied ❑ Partially Satisfied ❑ Don't Know
Risk Management Criteria	
4. Risk management criteria are defined and documented. *Examples of risk management criteria* Probability, impact, and risk exposure criteria; decision-making criteria (e.g., for escalation or prioritization); criteria that establish risk tolerance; criteria for communicating with collaborators, partners, subcontractors, suppliers, customers, and other stakeholders	❑ Satisfied ❑ Unsatisfied ❑ Partially Satisfied ❑ Don't Know

Evaluation: Framework Requirements

Rationale
Stakeholder Sponsorship 1.
Risk Management Plan 2.
Risk Sources 3.
Risk Management Criteria 4.

Evaluation: Framework Requirements (continued)

Requirement	Response
Tailored Methods and Tools	
5. Methods and tools used to support risk management activities have been appropriately tailored for use. *Examples of methods and tools* Procedures for conducting risk management activities; risk management criteria; risk sources; worksheets; automated support tools; report generators; databases	❑ Satisfied ❑ Partially Satisfied ❑ Unsatisfied ❑ Don't Know
Trained Personnel	
6. People who perform risk management activities are prepared to conduct them. *Examples of people who need training* Managers, technical leads, and staff who participate in risk management activities; risk manager; risk database administrator *Examples of types of training* Awareness training; method training; tool training	❑ Satisfied ❑ Partially Satisfied ❑ Unsatisfied ❑ Don't Know
Risk Statement	
7. A risk statement is documented for each risk using a standard format. *Examples of items that influence the format and use of risk statements* Organizational guidance for communicating, documenting, and updating risks; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders	❑ Satisfied ❑ Unsatisfied ❑ Partially Satisfied ❑ Don't Know
Context	
8. Context is documented for each risk. *Examples of items that influence the format and use of context* Organizational guidance for communicating, documenting, and updating risks; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders *Examples of context* Root causes; aggravating conditions; mitigating conditions; relationships and dependencies with other risks	❑ Satisfied ❑ Unsatisfied ❑ Partially Satisfied ❑ Don't Know

Evaluation: Framework Requirements (continued)

Rationale
Tailored Methods and Tools 5.
Trained Personnel 6.
Risk Statement 7.
Context 8.

Evaluation: Framework Requirements (continued)

Requirement	Response
Probability	
9. Probability is evaluated and documented for each risk. *Examples of items that influence the use of probability* Probability criteria; organizational guidance for assessing probability; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders	❑ Satisfied ❑ Partially Satisfied ❑ Unsatisfied ❑ Don't Know
Impact	
10. Impact is evaluated and documented for each risk. *Examples of items that influence the use of impact* Impact criteria; organizational guidance for assessing impact; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders	❑ Satisfied ❑ Partially Satisfied ❑ Unsatisfied ❑ Don't Know
Risk Exposure	
11. Risk exposure is evaluated and documented for each risk. *Examples of items that influence the use of risk exposure* Risk exposure criteria; organizational guidance for assessing risk exposure; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders	❑ Satisfied ❑ Unsatisfied ❑ Partially Satisfied ❑ Don't Know
Risk Profile	
12. A profile of all risks is developed, documented, and kept current. *Examples of items that influence the development of a risk profile* Organizational guidance for communicating, documenting, and updating the risk profile; requirements of methods and tools; format of risk statements; risk profile format; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders	❑ Satisfied ❑ Unsatisfied ❑ Partially Satisfied ❑ Don't Know

Evaluation: Framework Requirements (continued)

Rationale
Probability 9.
Impact 10.
Risk Exposure 11.
Risk Profile 12.

Evaluation: Framework Requirements (continued)

Requirement	Response
Mitigation Approach	
13. A mitigation approach is established and documented for each risk. *Examples of items that influence selection of a mitigation approach* Organizational guidance for communicating, documenting, and updating a mitigation approach; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders; risk tolerance; decision-making criteria *Examples of common mitigation approaches* Accept a risk and take no action; transfer a risk to another party; restructure activities to avoid a risk by eliminating the possibility of it occurring; take action to reduce or contain a risk	❑ Satisfied ❑ Partially Satisfied ❑ Unsatisfied ❑ Don't Know
Mitigation Plan	
14. A mitigation plan is defined and documented for each risk that is actively being addressed. *Examples of items that influence development of a mitigation plan* Organizational guidance for communicating, documenting, and updating a mitigation plan; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders; risk tolerance *Examples of a mitigation plan's content* Objectives for the plan; resources responsible for completing each action; schedule for completing all actions; funding allocated to performing the plan's actions; measures for tracking the execution of the plan (in relation to the schedule and cost); measures for tracking the effectiveness of the plan; a contingency plan and triggers when appropriate	❑ Satisfied ❑ Partially Satisfied ❑ Unsatisfied ❑ Don't Know
Executed Mitigation Plan	
15. Mitigation plans are implemented as intended (unless circumstances force a change in direction). *Examples of items that influence plan execution* Resources available for plan execution; funding allocated to the plan; responsibility for implementing the plan; authority for implementing plan; verification of completion; visible support of management *Examples of data that can be used to evaluate plan implementation* Tracking measures for effectiveness and efficiency of mitigation plan execution; tracking measures for verifying plan completion; triggers for contingency or alternate plans	❑ Satisfied ❑ Unsatisfied ❑ Partially Satisfied ❑ Don't Know

Evaluation: Framework Requirements (continued)

Rationale
Mitigation Approach 13.
Mitigation Plan 14.
Executed Mitigation Plan 15.

Evaluation: Framework Requirements (continued)

Requirement	Response
Tracking Data	
16. Data for tracking mitigation plans are collected, analyzed, documented, and reported. *Examples of items that influence collection of tracking data* Organizational guidance for selecting tracking measures; organizational guidance for communicating, documenting, and updating tracking data; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders; approach for collecting measurement data; approach for analyzing measurement data; frequency requirements for collecting tracking data *Examples of tracking measures* Tracking measures for effectiveness and efficiency of mitigation plan execution; tracking measures for verifying plan completion; triggers for contingency or alternate plans	❑ Satisfied ❑ Partially Satisfied ❑ Unsatisfied ❑ Don't Know
Tracking Decision	
17. Tracking decisions for mitigation plans are documented appropriately. *Examples of items that influence tracking decisions* Organizational guidance for communicating, documenting, and updating tracking decisions; requirements for approving tracking decisions; requirements of methods and tools; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders; decision-making criteria *Examples of common tracking decisions* Modify the mitigation approach and develop a new plan; modify an existing mitigation plan; implement a contingency plan; close a risk	❑ Satisfied ❑ Partially Satisfied ❑ Unsatisfied ❑ Don't Know
Controlled Risk Management Assets and Work Products	
18. Selected risk management assets and work products are under configuration control. *Examples of assets under configuration control* Risk management plan; methods and tools; risk sources; risk criteria *Examples of work products under configuration control* Risk profile; mitigation plans; tracking decisions; status reports	❑ Satisfied ❑ Unsatisfied ❑ Partially Satisfied ❑ Don't Know

Evaluation: Framework Requirements (continued)

Rationale
Tracking Data 16.
Tracking Decision 17.
Controlled Risk Management Assets and Work Products 18.

Evaluation: Framework Requirements (continued)

Requirement	Response
Lessons Learned	
19. Lessons learned are collected and documented for the risk management practice. *Examples of items that influence lessons learned* Requirements for developing lessons learned; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders; types of effectiveness measures collected for the risk management practice; strengths of the risk management practice; weaknesses of the risk management practice; changes in best practices; new standards or changes to existing standards or regulations; new methods and tools or changes to existing methods and tools	❑ Satisfied ❑ Partially Satisfied ❑ Unsatisfied ❑ Don't Know
Updates to Risk Management Practice	
20. The risk management practice is updated as appropriate based on lessons learned. *Examples of items that influence how lessons are incorporated* Change management process; organizational guidance for managing change; needs of decision makers, collaborators, partners, subcontractors, suppliers, customers, and other stakeholders *Examples of items that could be updated or changed* Risk management plan; funding for risk management; methods; tools; resources; training	❑ Satisfied ❑ Unsatisfied ❑ Partially Satisfied ❑ Don't Know

Evaluation: Framework Requirements (continued)

Rationale
Lessons Learned 19.
Updates to Risk Management Practice 20.

References/Bibliography

URLs are valid as of the publication date of this document.

[Alberts 2002]
Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE[SM] Approach*. Boston, MA: Addison-Wesley, 2002 (ISBN 0-321-11886-3). www.sei.cmu.edu/library/abstracts/books/0321118863.cfm

[Alberts 2009]
Alberts, Christopher & Dorofee, Audrey. *A Framework for Categorizing Key Drivers of Risk* (CMU/SEI-2009-TR-007). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2009. www.sei.cmu.edu/library/abstracts/books/09tr007.cfmw

[Charette 1990]
Charette, Robert N. *Application Strategies for Risk Analysis*. New York, NY: McGraw-Hill Book Company, 1990.

[Dorofee 1996]
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. www.sei.cmu.edu/library/abstracts/books/crmguidebook.cfm

[Gallagher 1999]
Gallagher, Brian. *Software Acquisition Risk Management Key Process Area (KPA)—A Guidebook Version 1.02* (CMU/SEI-99-HB-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999. www.sei.cmu.edu/library/abstracts/reports/99hb001.cfm

[Gallagher 2005]
Gallagher, B.; Case, P; Creel, R.; Kushner, S.; & Williams, R. *A Taxonomy of Operational Risks* (CMU/SEI-2005-TN-036). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005. www.sei.cmu.edu/library/abstracts/reports/05tn036.cfm

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

[Williams 1999]
Williams, R.; Pandelios, G.; & Behrens, S. *Software Risk Evaluation (SRE) Method Description (Version 2.0)* (CMU/SEI-99-TR-029). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999. www.sei.cmu.edu/library/abstracts/reports/99tr029.cfm

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	August 2010	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Risk Management Framework	FA8721-05-C-0003

6. AUTHOR(S)

Christopher J. Alberts and Audrey J. Dorofee

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2010-TR-017

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	ESC-TR-2010-017

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Although most programs and organizations use risk management when developing and operating software-reliant systems, preventable failures continue to occur at an alarming rate. In many instances, the root causes of these preventable failures can be traced to weaknesses in the risk management practices employed by those programs and organizations. To help improve existing risk management practices, Carnegie Mellon University Software Engineering Institute (SEI) researchers undertook a project to define what constitutes best practice for risk management. The SEI has conducted research and development in the area of risk management since the early 1990s. Past SEI research has applied risk management methods, tools, and techniques across the life cycle (including acquisition, development, and operations) and has examined various types of risk, including software development risk, system acquisition risk, operational risk, mission risk, and information security risk, among others.

In this technical report, SEI researchers have codified this experience and expertise by specifying (1) a Risk Management Framework that documents accepted best practice for risk management and (2) an approach for evaluating a program's or organization's risk management practice in relation to the framework.

14. SUBJECT TERMS	15. NUMBER OF PAGES
risk, risk analysis, risk management, risk management framework	72

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL