Software Engineering Institute

Executive Overview of SEI MOSAIC: Managing for Success Using a Risk-Based Approach

Christopher Alberts
Audrey Dorofee
Lisa Marino

March 2007

TECHNICAL NOTE
CMU/SEI-2007-TN-008

Mission Success in Complex Environments

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 purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Figures

Acknowledgements

The authors would like to acknowledge the contributions of the following people: Nicole Malec for the development of the requirements and pilot version of the SEI MOSIAC Toolkit; Georgia Killcrece, Robin Ruefle, and Mark Zajicek for their collaboration in piloting SEI MOSAIC methods in the incident response domain; and Julia Allen, Bill Anderson, Eileen Forrester, and Tricia Oberndorf for their review of this technical note.

Abstract

In today's business environment, multiple organizations routinely work collaboratively in pursuit of a single mission. These separate efforts result in process and programmatic complexity that is difficult to manage effectively. Mission success in these complex settings demands a collaborative management approach that effectively coordinates task execution and decision-making activities among all participating groups. Managing for mission success requires establishing and maintaining a reasonable degree of confidence that a mission's objectives will be successfully achieved. Confidence at the mission level requires establishing and maintaining a corresponding level of confidence in the people, processes, and technologies used to achieve a mission. The Software Engineering Institute (SEI) is currently developing the Mission-Oriented Success Analysis and Improvement Criteria (MOSAIC)—a suite of advanced, risk-based analysis methods for assessing complex, distributed programs, processes, and information-technology systems. With SEI MOSAIC methods, management can establish and maintain confidence in success throughout the life cycle and help provide assurance at the mission, system, and program levels. This technical note provides an executive overview of the concepts and foundations of SEI MOSAIC.

1 Introduction

The responsibility for managing a work process and the resources needed to carry out process activities have traditionally aligned along organizational boundaries. However, drivers in the business environment, such as the globalization of business and the fast pace of change, have led to an increase in outsourcing and partnering among organizations. It is now common for multiple organizations to work collaboratively in pursuit of a single mission, creating a degree of process and programmatic complexity that has proven to be difficult to manage effectively. Mission success in these complex settings demands a collaborative management approach that effectively coordinates task execution and decision-making activities among all participating groups.

Managing for mission success requires establishing and maintaining a reasonable degree of confidence that a mission's objectives will be successfully achieved. Confidence at the mission level requires establishing and maintaining a corresponding level of confidence in the

- operational processes[1] used to achieve a mission
- software-intensive systems[2] and infrastructures used to support the operational process
- projects and programs used to acquire and develop the software-intensive systems

As such, managing for mission success spans all lifecycle activities and transcends organizational boundaries, creating a multi-dimensional problem space. Unfortunately, most traditional management approaches are unable to handle the degree of complexity inherent in this problem space.

1.1 MISSION SUCCESS RESEARCH

In 2006, the Carnegie Mellon® Software Engineering Institute (SEI) chartered the Mission Success in Complex Environments (MSCE) project to develop new and innovative management approaches applicable to a variety of settings, including (but not limited to)

- large, distributed software development programs
- Department of Defense supply chains
- organizations in dynamic, rapidly changing business environments
- distributed information-technology (IT) processes
- organizations with strict reliability, security, and safety requirements
- distributed business processes
- processes supporting critical infrastructures
- software-intensive systems and systems of systems

[1] Operational processes include all tasks, policies, procedures, organizations, people, technologies, tools, data, inputs, and outputs needed to achieve the specified mission.

[2] Software-intensive systems are referred to separately because they are of special interest to our research.

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

While each of these examples has unique characteristics, all share a common aspect—complex environments that are inherently risky.

We are currently developing the SEI Mission-Oriented Success Analysis and Improvement Criteria (SEI MOSAIC)—a suite of advanced analysis methods for assessing complex, distributed programs, processes, and IT systems. With SEI MOSAIC methods, management can establish and maintain a reasonable degree of confidence in success throughout the lifecycle and help provide assurance at the mission, system, and program levels. SEI MOSAIC is *initially* focused on managing success in projects, programs, and operational processes. In the future, we intend to expand our research to software-intensive systems as well as systems of systems.

1.2 OBJECTIVES, AUDIENCE, AND STRUCTURE

This technical note provides an executive overview of SEI MOSAIC. It establishes the baseline for our research into mission success by describing fundamental concepts, definitions, and philosophy underlying SEI MOSAIC. This report also outlines our long-term research directions for this work. Future documents will provide greater detail about specific SEI MOSAIC methods and techniques.

Our primary audience for this technical note is managers of complex projects and programs who have experience assessing and managing risk in operational and development settings. People who have experience with or are interested in the following topics might find this report useful:

- systems assurance
- supply chain management
- managing processes with strict reliability, security, and safety requirements
- managing risk in critical infrastructures

We have divided this technical note into six sections. This introduction serves as the first section; it provides background about the research contained in this document. Section 2, “Achieving Objectives,” presents the basic structure of a work process and illustrates how the objectives of a work process define its picture of success. The link between risk and managing for mission success is established in Section 3, “Risk Management.” This section also introduces the concepts of outcome-based risk management and mission risk. Section 4, “Managing Mission Risk,” illustrates the basic elements of mission risk and their relationships to outcome-based risk management. The unique attributes of SEI MOSAIC are presented in Section 5, “SEI MOSAIC.” Finally, Section 6, “Applications and Future Research Directions,” provides an overview of pilot activities for SEI MOSAIC and outlines our future research directions.

2 Achieving Objectives

In its broadest sense, the term *mission* is used to describe the purpose of an organization. At the same time, it can also be used to define the goals of a specific department or group within a larger organization. A department's mission must support the broad organizational mission while also reflecting the unique objectives of that specific department. Mission can also refer to the specific result being pursued when performing a work process. The mission of a work process outlines the tangible objectives of that process, which also must support related department and organizational missions. In addition, each activity in a work process has a distinct mission, and each technology that supports an activity also has a mission. A network of missions thus exists within all organizations.[3] Success at the organizational level requires ensuring that all missions in the network are in alignment and that all mission objectives are satisfactorily achieved.

With outsourcing and collaboration becoming so widespread, the mission network often extends beyond a single organization to include multiple organizations that are often geographically distributed and culturally diverse. A multi-organizational mission network complicates efforts to align the missions within the network. In this document, we focus on a portion of this broad, multi-organizational mission network by examining work processes and their associated missions.

2.1 WORK PROCESSES

A work process is a collection of interrelated work tasks that achieves a specific result [Sharp 01].[4] It includes all tasks, policies, procedures, organizations, people, technologies, tools, data, inputs, and outputs required to achieve desired objectives. The ultimate purpose of a work process is to achieve a specific, well-defined set of objectives, or mission. Figure 1 depicts a generic work process and highlights the activities required to achieve its associated objectives.

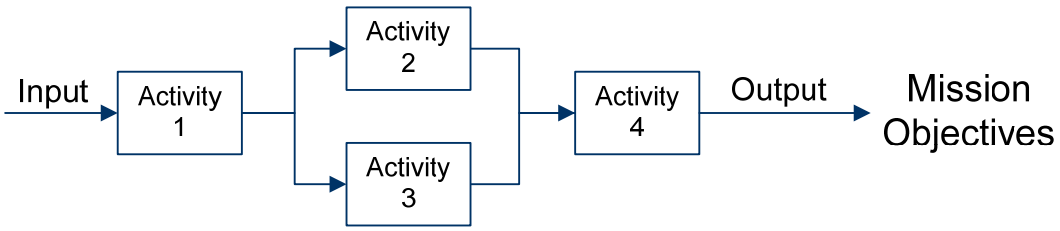

Figure 1: Work Process with Four Activities

The basic function of the process depicted in Figure 1 is to transform the input into the desired output, forming the basis of the work-process mission. To achieve that set of objectives, four activities must be executed in the order shown, while also adhering to any cost and schedule constraints. Process execution begins when Activity 1 receives its input. Upon completion of Activity

[3] We assert that mission is a recursive concept.

[4] The literature uses several terms synonymously with work process, including business process, workflow, and process. All four terms are used interchangeably throughout this report. However, as explained later in this section, the term *operational process*, as used in this report, has a different meaning attached to it.

1, its output triggers Activities 2 and 3, which are then performed in parallel. When Activities 2 and 3 are complete, their outputs are forwarded to Activity 4, the last in the sequence. Upon completion of Activity 4, the work process is finished. If all of the activities have been performed correctly, the overall set of objectives for the process will have been successfully achieved.

A work process is more than a collection of activities, however. It is a complex *organizational system* that brings together a variety of diverse components, or assets. These assets (people, technologies, equipment, facilities, information, procedures, and inputs) are organized in a specific way to achieve a particular set of objectives. Process assets are not brought together in a random manner when pursuing a mission. On the contrary, they are organized into a set of interacting, interrelated, and interdependent parts that must function as a whole to accomplish given objectives.

The specific nature of any process is strongly influenced by its unique set of objectives, or mission. Process assets must be selected, organized, and managed in a way that supports the set of objectives being pursued. As such, different types of processes exist. For example, some processes are designed to be performed repeatedly while others are intended to be performed only once. We explore this concept in the next section.

2.2 PROJECTS, PROGRAMS, AND OPERATIONAL PROCESSES[5]

Projects and programs rely on work processes that are executed once. They produce a unique product for a customer or deliver a service that is tailored for a customer's needs. For example when an organization develops a software-intensive system for a specific customer, its management charters a *project* or *program* to develop that system. The underlying work process for the project or program begins with the initial concept for the system and ends when the system is satisfactorily delivered to the customer.

In contrast to processes that support projects and programs, an operational process is typically executed more than once. For example, think about how an IT department's help desk works. Whenever the help-desk staff receives a phone call or email from a customer, a response process is triggered. Since the typical help desk receives numerous phone calls and emails each day, its response process is executed many times during business hours. In addition, help-desk personnel normally attend to multiple issues simultaneously. As such, a help-desk is designed to allow for multiple instances of its underlying processes to be performed in parallel.

The repetitious and parallel characteristics of operational processes differentiate them from the types of processes underlying projects and programs. However, all of these processes are classified as work processes and thus share many common characteristics. As a result, a common philosophy can be followed when managing projects, programs, and operational processes for success. Conducting a work process requires managing the complexity resulting from a set of interacting, interrelated, and interdependent parts that are designed to achieve a single mission. However, projects, programs, and operational processes can also be distributed among several organizations, which then adds yet another layer of complexity.

[5] In this document, when we refer to projects and programs, we are referring to the work processes associated with projects and programs.

2.3 DISTRIBUTED WORK PROCESSES

In a *distributed work process*, management control is shared by multiple managers who are often from different organizations. Over the past several years, outsourcing, collaboration, and globalization have become increasingly commonplace and necessary, which has made distributed work processes commonplace and necessary as well. The paradigm of having a single manager with absolute responsibility for an entire work process is becoming obsolete. It is being replaced by a collaborative model where management responsibility for a process is shared by several managers, each overseeing a part of the overall process.

Figure 2 depicts a simplified example of a distributed process. Notice that the rather simple process from Figure 1 is now part of a larger process that links four distinct subprocesses. Each subprocess has its own unique set of objectives that define its local mission. Each local mission is supported by local activities and they, in turn, have their own local objectives. Successful completion of local activities is required for the local mission to be declared a success. However, the overall work-process objectives are not achieved until all activities in all sub-processes have been successfully completed. As illustrated in Figure 2, four organizations have pooled their resources to complete a single set of objectives, thus creating a distributed work process. Each group in Figure 2 must adhere to the mission of its parent organization. However, the four organizations also must work together toward a common set of objectives, which creates a virtual enterprise with it own unique mission. This virtual enterprise could exist for a limited amount of time (e.g., a work process that is executed once), or it could continue for an extended period of time (e.g., an operational process, perhaps with some partners being replaced over time).

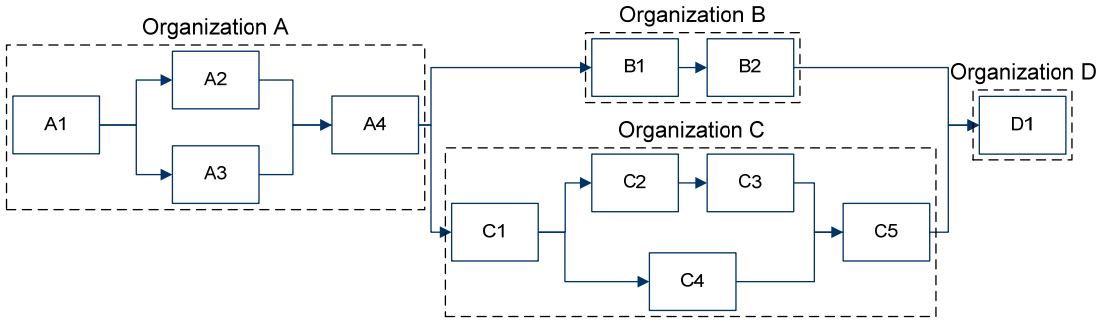

Figure 2: Work Process Spanning Four Organizations

2.4 A SET OF OBJECTIVES

The mission of a work process typically comprises three distinct types of objectives: (1) product or service, (2) cost, and (3) schedule. Product objectives define the nature of the items produced. Product objectives are often referred to as technical objectives in the software development domain. For example, if you are developing a software-intensive system, the product (i.e., technical) objectives define the functional and performance characteristics of the system as well as other desired attributes, like safety or security. If the work process provides a service, it will have service objectives instead of product objectives. Service objectives define the nature of the services provided to the recipients of those services (i.e., customers). If the service you are providing is help desk support, the service objectives will define the quality of help desk support provided to constituents (such as the required response time based on the priority of the request). Thus, prod-

uct or service objectives define the parameters of success for the products you build or the services you provide.

In some instances, a mission is defined solely by its product or service objectives. However, in most cases, constraints are also considered in relation to product or service objectives. Managers generally do not have infinite funds at their disposal, nor do they have an infinite amount of time in which to complete work tasks. As a result, cost and schedule objectives must be considered alongside the product or service objectives (and in many cases are the key drivers of management's decision, especially as time goes by and costs accrue).

These three types of objectives, when viewed together, typically define a basic mission. They specify what will be accomplished, the anticipated costs to complete all activities, and the time frame in which work will be completed. When appropriate, these objectives can be supplemented with other objectives (such as business or financial objectives) to ensure a complete picture of success. Once that picture is established, management activities must be geared toward ensuring that results satisfy those objectives. Risk management is an activity that plays a vital role in achieving a mission's picture of success, and it is the focus of the remainder of this technical note.

3 Risk Management

The term *risk* is used universally, but different audiences often attach different meanings to it [Kloman 90]. In fact, the details about risk and how it supports decision making depend upon the context in which it is applied [Charette 90]. 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. As such, no universally accepted definition of risk exists.

However, whereas specific definitions of risk might vary, a few characteristics are common to all definitions. In fact, for risk to exist in any circumstance, the following three conditions must be satisfied [Charette 90]:

1. The potential for loss must exist.
2. Uncertainty with respect to the eventual outcome must be present.[6]
3. Some choice or decision is required to deal with the uncertainty and potential for loss.

These 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 quantifiable aspects of risk. Bearing this in mind, 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 96].

3.1 SPECULATIVE AND HAZARD RISK

Sometimes a situation presents an opportunity for gain as well as the potential for loss. In other instances, only the potential for loss exists. Because of this difference, risk can thus be further subdivided into two types: speculative risk and hazard risk [Young 01]. Figure 3 illustrates the differences between these two categories.

With speculative risk you might realize a gain, which can improve your current situation relative to the status quo. At the same time, you might experience a loss, which can make your situation worse than it is at present. Gambling is an example of taking a speculative risk. When you place a bet, you must balance the potential for gain against the potential for loss. You weigh the possibility of gaining additional money against the prospect of losing the funds you wagered. When you gamble, your objective is to increase your wealth in relation to the status quo, and you are willing to put your finances at risk for the opportunity to make money

In contrast, hazard risk provides you no opportunity to improve upon your current situation; it only brings the potential for loss. For example, consider how security can be viewed as a hazard

[6] 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 note.

risk. Imagine that you are concerned about protecting valuables that are stored in your home. Your main objective in this example is to ensure that none of the valuables in your residence is removed without your knowledge and permission. After evaluating how well your valuables are protected, you might decide to install a security system in your residence to make it more difficult for a thief to break in and steal your valuables. Notice that the objective in this example, by definition, restricts the focus of risk on the potential for loss. In the most favorable of circumstances, you only keep what you already possess. There is no potential for gain.

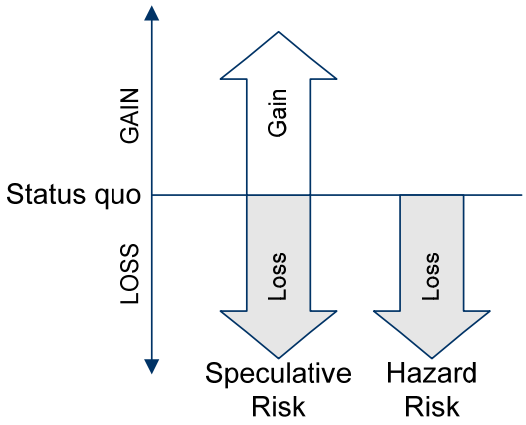

Figure 3: Speculative and Hazard Risks

Now consider the same example when viewed from another perspective. In this instance, you would like to gain peace of mind by preventing unsavory characters from gaining entrance to your house. Your objective to feel more secure defines the context in which you view risk. After analyzing the situation, you might decide to install a security system in your residence to make it more difficult for someone to break in. You might reason that the added protection will make you feel more secure and help you gain the peace of mind you seek. In this example, you are willing to invest money in a security system to provide yourself an opportunity feel more secure. The security risk in this example is speculative because it balances your tolerance for risk (i.e., the amount of money you are willing to invest in a security system) with your desire to realize an opportunity (i.e., gaining peace of mind). These two security examples illustrate how the same situation can be viewed as a hazard risk in one context and a speculative risk in another. A risk therefore is classified as speculative or hazard based on the context in which it is viewed.

> *The notion of explicitly establishing the context in which you analyze and manage risk is vitally important to ensure that you make appropriate choices about how you manage your risks.*

3.2 THREAT-BASED AND OUTCOME-BASED RISK MANAGEMENT

Hazard risk is typically viewed from a relatively narrow context, where the main focus is on how conditions and events can lead to loss. In contrast, speculative risk is normally viewed from a much broader perspective, where the main focus is on forecasting the expected outcome, or the most likely result, from a range of possibilities. Because of these fundamental differences, two distinct approaches for managing these two types of risk have traditionally been employed.

Threat-based risk management is an approach used when managing hazard risks. From the hazard perspective, a threat is a condition or event that could lead to a risk [Alberts 05]. As a result, from this point of view, a risk is viewed as a potential obstacle that can interfere with progress. A hazard risk is normally represented using a linear cause-and-effect pair that conveys two key pieces of information: (1) the threat (i.e., condition or event) that is causing concern and (2) the potential consequences of that threat [Gluch 94]. Each cause-and-effect pair, or risk statement, can be viewed as a scenario that documents the potential loss triggered by a given condition or event. Threat-based risk management generally requires people to

- identify risks that can lead to loss
- analyze the list of risk statements to determine mitigation priorities
- take action to mitigate the highest priority risks

Threat-based approaches normally focus on a particular type of risk, such as project risk, security risk, or safety risk. Focusing on a particular type of risk further restricts the context in which risk is viewed. For example, a project risk assessment [Dorofee 96 and Williams 99] will likely look at performance-related risks in great detail, but it will likely pay little or no attention to risks triggered by security issues or problems in the operational environment. Security and operational risks are considered to be beyond the scope of many project risk assessments; managers normally rely on other types of risk assessments [Alberts 02] to evaluate those risks.

In contrast, *outcome-based risk management* has traditionally been employed when managing speculative risk. Outcome-based risk management assumes an aggregate view of risk. Rather than identifying, analyzing, and managing a set of risk statements (as is done in threat-based risk management), people performing outcome-based risk management forecast the most likely outcome, or result, from a range of possibilities. The goal is to maintain the overall level of risk within an acceptable tolerance over time. Conditions and potential events must be managed effectively to ensure that risk is kept within tolerance and the most likely outcomes for a mission will be acceptable to key stakeholders. Because of their broad focus, outcome-based approaches are ideally suited for managing speculative risk in business settings.

Because it is solely focused on the potential for loss, threat-based risk management is constrained to managing hazard risk.[7] In contrast, outcome-based risk management is dependent on the context in which it is applied. It has proven to be useful throughout the years when managing speculative risk. However, it can also be employed when managing hazard risk. Our work in the area of managing for mission success is based on applying an outcome-based approach, as defined by SEI MOSAIC, in both hazard and speculative settings.

3.3 RISK AND MANAGING FOR MISSION SUCCESS

Managing for mission success requires establishing and maintaining a reasonable degree of confidence that the objectives of a project, program, or operational process will be realized. Implicit in

[7] Threat-based approaches can be used in conjunction with other techniques to assess speculative risk. A SWOT (strength, weakness, opportunity, threat) analysis is an example of using threat-based techniques as part of a broader approach that looks at speculative issues. However, when used by itself, a threat-based approach, by definition, is restricted to hazard risk.

this statement is the notion that a mission's outcome must satisfactorily achieve the objectives being pursued, which is also the key tenet of outcome-based risk management. Therefore, the basic philosophy of managing for mission success is rooted in an outcome-based approach for managing risk.

Depending upon the context, managing for mission success can focus on either hazard or speculative risk. For example, if you are developing a software-intensive system, you can define success as meeting the deliverables defined in your contract. You will be successful if you deliver a working system on time and within budget. By adopting this perspective, you have assumed a hazard view of risk. At best, you can achieve your deliverables; you have allowed no opportunity for gain.

However, you could look at the same example from a speculative point of view. Here, in addition to achieving the product, schedule, and budget objectives, you are also interested in generating profit for your organization. As such, the business objectives for the project are considered alongside the product, schedule, and budget objectives. Success is now defined as delivering a working system, on time, and within budget as well as generating profit for the organization. The financial objectives for the project provide the opportunity for loss and gain, making this situation speculative.

We have coined the term *mission risk* to describe the type of risk associated with managing for mission success. Here, mission risk is defined as the potential gains or losses represented by a mission's possible outcomes. Mission risk thus represents the variance of outcomes for a given set of objectives. This type of risk is not inherently speculative or hazard in nature. In each situation, the mission's objectives dictate whether mission risk is classified as a speculative or hazard risk. Overall, the key to managing mission risk lies with the ability to manage a mission's outcomes effectively.

4 Managing Mission Risk

A wide range of outcomes is usually possible when executing a project, program, or operational process. Some of these outcomes will be acceptable to stakeholders, while others will be deemed unacceptable. Managing a mission's potential outcomes is the main focus of mission risk management. When a work process is executed, several factors influence which outcome is most likely or expected to occur (referred to as the expected outcome). Figure 4 highlights the five basic elements integral to mission risk management:

- context
- execution
- conditions
- potential events
- range of potential outcomes

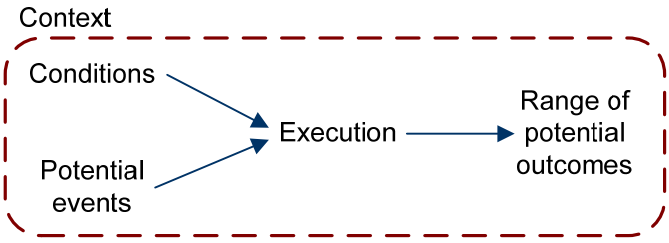

Figure 4: The Five Elements of Mission Risk

Context provides the background, situation, or environment in which a work process is executed. It generally includes the key objectives being pursued as well as stakeholders' expectations for those objectives.[8] As such, it defines the picture of success for a given set of objectives and provides the lens through which all potential outcomes are viewed and interpreted. Defining the context is thus an essential first step when determining a mission's potential for success.

For example, assume that you are a project manager who is overseeing the development of a software-intensive system. Suppose that the following objectives are most important to you: product, cost, and schedule objectives. These objectives indicate that you are focused on developing a fully functional system on time and within budget. Now, suppose that stakeholders (such as senior managers in your organization) are very concerned about cost overruns and have made it clear that the project cannot exceed its budget. As a result, the cost objective becomes your primary objective among the three, and your tolerance for cost risk is low. Your decision making will be driven by your low tolerance for cost overruns. As a result, when you are forced to make trade-offs, you will weight unacceptable outcomes related to cost greater than those related to product and schedule objectives. The context in this example has been defined by three project objectives and the expectations related to those objectives. Without setting an appropriate context, you can-

[8] Stakeholders include all interested parties, customers, and suppliers, both internal and external to an organization.

not definitively determine how to gauge success or how to assess any given outcome. Context thus forms the underlying foundation for managing mission risk.

Execution describes what is being done to achieve a set of objectives. With respect to a work process, execution refers to the activities that are performed when working toward the objectives. *Conditions* define the circumstances that directly or indirectly influence execution and drive an outcome toward success or failure. As a work process is executed, these conditions affect the eventual outcome. In some instances, conditions directly influence the outcome, while in others, they indirectly affect the outcome by creating exposure to negative or positive events. Both types of conditions are explored in greater detail below, beginning with those that directly influence a mission's outcome.

Consider an example where a team is developing a software-intensive system. Suppose that the following condition is present: team members have not previously worked with the design language being used on the project. This could cause them to make mistakes or take more time when working on tasks. As such, this condition may drive product, cost, and schedule objectives toward one or more undesired outcomes. Here, the condition has a direct influence on the eventual outcome.

Now, consider conditions that expose a mission to the effects of events that might occur. During normal day-to-day operations, these conditions lie dormant and do not produce any visible effect on results. However, certain events in combination with these dormant conditions can influence the expected outcome.[9]

A computer virus, for example, is a program that is designed to exploit certain conditions (called vulnerabilities) and infect computers causing them to act erratically. People with malicious intent design these programs with the ultimate goal of wreaking havoc throughout the business community, such as degrading the performance of computers and networks or rendering them unavailable for use. If a work process is highly dependent on the availability of infected computers and networks, production can be temporarily halted, which can lead to an undesirable outcome.[10] Notice that the condition, the system's vulnerability, poses no threat to production during normal operations. It takes an unpredictable event, the proliferation of a computer virus, for damage to occur. This particular condition only affects the process' outcome when a relevant event occurs.

A *potential event* is an unpredictable occurrence that combines with one or more exposing conditions to affect performance and thus drive the outcome toward success or failure. As such, conditions and potential events are called outcome drivers because of their effect on the eventual result.

It is important to note that you cannot focus on a single condition or event when managing mission risk. Some conditions and events tend to guide a mission toward a successful outcome, while

---

[9] Events can have a positive or negative effect on a mission's outcome depending on the specific nature of the event. For example, an increase in funding would likely be perceived as a positive event that might put a mission in better position for success. On the other hand, a decrease in funding would likely be perceived as a negative event that might adversely affect a mission's outcome.

[10] Undesirable from the business' perspective, that is. From the virus developer's perspective, this would be considered a successful outcome.

others tend to drive a mission toward an unsuccessful outcome. You need to consider the relative influence of all outcome drivers when assessing mission risk.

The *range of potential outcomes* defines the set of possible results that can be achieved when working toward a set of objectives. As illustrated in Figure 5, a range of outcomes is possible for any given process prior to and during its execution. In addition, the figure shows that

- Some outcomes will be considered to be acceptable, while others will be viewed as unacceptable.
- Multiple outcomes can be viewed as acceptable for any given mission.

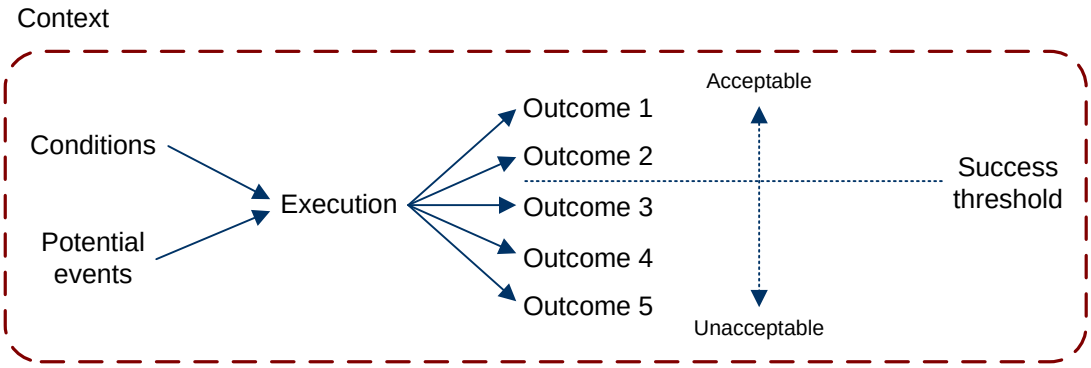

Figure 5: A Range of Potential Outcomes

The dividing line between acceptable and unacceptable outcomes is called the *success threshold*. The placement of the success threshold conveys management's overall tolerance for risk by delineating which outcomes are considered to be acceptable and unacceptable for each objective (i.e., defining the acceptable variance of outcomes for each objective). The tolerance for risk in a situation is normally influenced by choice (e.g., personal preference of the key decision maker) as well as by circumstances (e.g., stakeholder expectations force a manager to accept more risk than he or she would like).

Given a specific set of circumstances, the relative chance of each possible outcome occurring for an objective can be estimated at a given point in time. The relative probabilities of all outcomes for an objective are called the *outcome distribution* for that objective. One outcome from the distribution, called the expected outcome, will be considered to be most likely to occur.

A detailed analysis of mission risk will typically examine the outcome distribution for each objective (1) under normal circumstances (i.e., in the absence of potential events) and (2) when stressed by potential events. Ideally, the expected outcome for each objective will be within tolerance during both normal and stressed circumstances. When an expected outcome(s) is out of tolerance (i.e., below the success threshold), decision makers must perform a tradeoff analysis to determine an appropriate course of action. The underlying goal of managing mission risk is to ensure that the expected outcome is acceptable to stakeholders. Conditions and potential events (i.e., outcome drivers) must be managed appropriately to make acceptable outcomes more likely than unacceptable outcomes.

5 SEI MOSAIC

The trend toward distributed projects, programs, and operational processes has led to a high degree of organizational and technological complexity that can be difficult to manage effectively. Managers often struggle to make sense of this complexity, which places many critical missions at risk of failing. SEI MOSAIC defines an outcome-based approach for assessing and managing a mission's potential for success. It is designed to analyze organizational and technological issues that are well beyond the capabilities of most traditional risk analysis approaches. Central to this approach is the modular design, or toolkit structure, of SEI MOSAIC's analysis methods.

5.1 MODULAR DESIGN

One lesson we learned from our past research is that a one-size-fits-all method will not meet the broad needs of the community. While many organizations follow similar practices from a conceptual point of view, the ways in which those practices are implemented vary greatly. Each organization is different and has its own way of doing business. Consequently, the methods people use when managing projects, programs, and operational processes tend to reflect the unique nature of their organization and environment.

SEI MOSAIC's analysis methods are designed to be modular, which provides great flexibility when applying them. You can think of SEI MOSAIC as a toolkit, similar in concept to a carpenter's toolkit. Each of a carpenter's tools is designed for a specific task. The combination of tools used on any job is based on the specific requirements of the tasks that must be completed. In the same way, SEI MOSAIC comprises a flexible set of methods that can be used to solve a variety of analysis problems. Figure 6 shows a conceptual diagram of the SEI MOSAIC toolkit, which includes a collection of protocols (and their associated activities), techniques, and supporting artifacts.

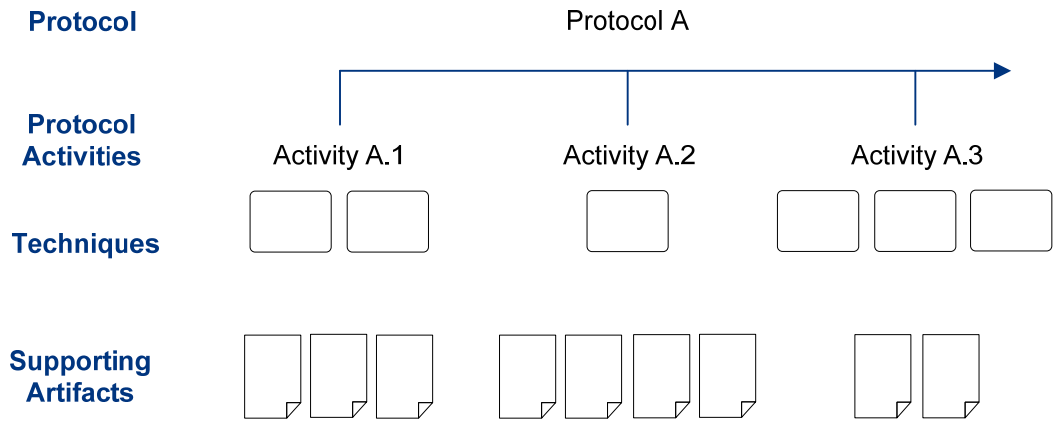

Figure 6: SEI MOSAIC Toolkit

The underlying basis for every SEI MOSAIC analysis method is a *protocol*, which defines the basic framework for conducting the analysis. A protocol defines the sequence of activities that

must be performed but does not indicate how to perform them. You can think of a protocol and its associated activities as providing the basic requirements for conducting an analysis.

Figure 6 also represents the collection of techniques and supporting artifacts that are part of the SEI MOSAIC body of knowledge. A technique defines a specific practice that can be used to perform a protocol activity. For example, think about a protocol in which the following activity is prescribed: *Gather data from people*. Many interviewing and surveying techniques can be used to gather data from people who are knowledgeable about a subject. The objective is to select the technique that is most appropriate for your given set of circumstances. In some cases, an interview might be the best choice, while other instances might call for a survey that people complete anonymously. In either case, you get the information you need; you just use different means to collect it.

Now, suppose you decide to gather the data you need by conducting an interview with a set of carefully chosen participants. During the interview session, you frame the discussion around a set of key questions. That list of questions is a tool that is an essential part of conducting an efficient and effective interview and is an example of a supporting artifact. When you conduct any technique, you will likely use one or more supporting artifacts to gather, analyze, or record data. Worksheets, templates, and tools are all examples of supporting artifacts.

Protocols (and their associated activities), techniques, and supporting artifacts form the basis for analysis methods in SEI MOSAIC. Figure 7 shows how a method is created by linking techniques and supporting artifacts with a protocol's activities. The collective set of techniques and artifacts used to conduct the protocol (represented by the shaded boxes) constitute a method for that protocol.

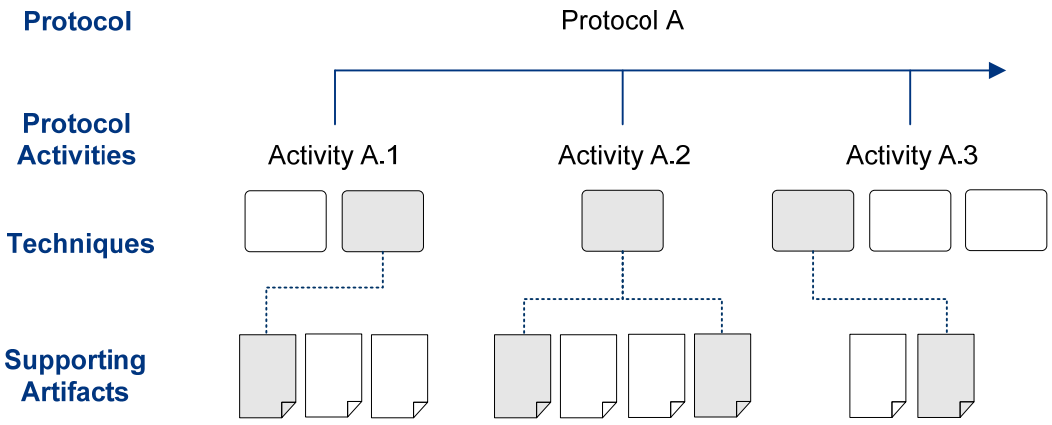

Figure 7: A Method Consistent with Protocol A

An SEI MOSIAC method defines

- which activities need to be performed during an analysis (as defined by a protocol)
- how to perform each activity (as defined by the selected techniques and artifacts)

As shown in Figure 8, multiple methods can be consistent with the same protocol. Notice that different techniques and artifacts are highlighted in Figure 7 and Figure 8. The two methods ac-

complish the same analysis goals as defined by the common protocol they follow, but each incorporates a unique set of techniques and artifacts.

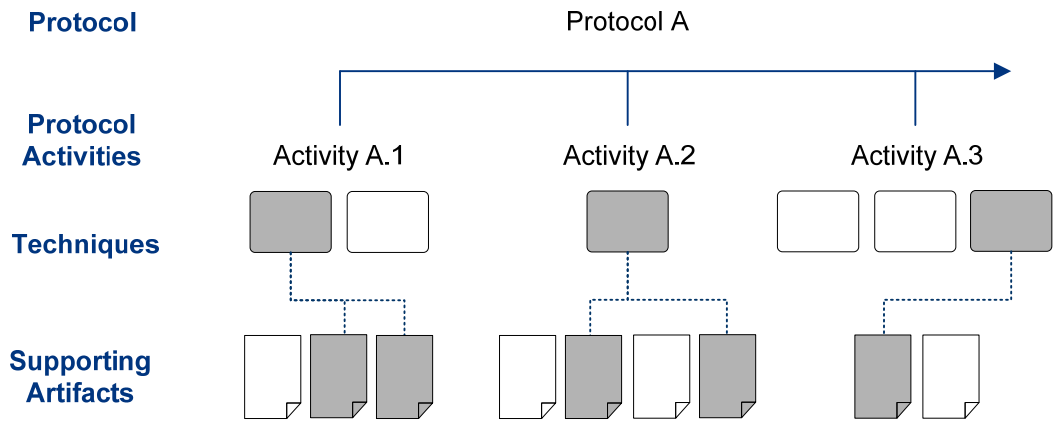

Figure 8: A Second Method Consistent with Protocol A

SEI MOSIAC allows for great flexibility when performing an analysis. Each SEI MOSAIC analysis method must be tailored to a given situation, or problem space, which optimizes that method based on the circumstances at hand.

5.2 CURRENT SEI MOSAIC PROTOCOLS

To this point in our research and development activities, we have developed the following base protocols for analyzing mission risk:

- Mission Diagnostic Protocol (MDP)
- Mission Assurance Analysis Protocol (MAAP)

MDP is a rapid analysis to assess a mission's potential for success based on current conditions. Upon completion, managers have a sense of a mission's current state of health based on an evaluation of key indicators for that mission. With results in hand, managers can decide on a course of action intended to reduce the overall risk affecting a mission and, as a result, improve the mission's chances of succeeding. This time-efficient analysis can be performed at any point in the life cycle.

In contrast, MAAP is a comprehensive analysis used to systematically examine conditions and potential events that place a mission at risk. Upon completion, managers have a detailed understanding of a mission, including an operational model of the mission, customized analysis artifacts, a measure of the mission's expected outcome, and strategies to increase the potential for success. Managers use MAAP's operational model and analysis results to bring mission risk within tolerance and chart a course for success. This in-depth analysis can be conducted at strategic points in the mission life cycle.

To date, we have piloted both protocols in the field and are in the process of refining and documenting them. In the next section, we take a closer look at our pilot activities and at a few ideas for future research related to SEI MOSAIC.

6 Applications and Future Research Directions

Rather than designing SEI MOSAIC for a specific problem space, such as large DoD programs or financial organizations, we chose to develop a general analysis approach that is applicable to many diverse environments. In this way, a single philosophy can be used in numerous settings, obviating the need for multiple specialized assessment techniques.

When developing SEI MOSIAC protocols, techniques, and supporting artifacts, we leveraged the existing state of the practice whenever possible. We used common analysis techniques when appropriate, such as root cause analysis, and developed custom techniques when needed, such as a means of forecasting a mission's expected outcome. At this point in time, we are piloting and refining MAAP and MDP.

6.1 MAAP PILOTS

A cyber-security process, incident management, was our initial pilot case for MAAP.[11] Incident management is a process for preventing, detecting, and responding to cyber-security events and incidents [Alberts 04]. We selected it as the initial domain for piloting MAAP for two main reasons. First, experience indicates that many organizations initially focus on managing events and incidents when developing a cyber-security capability. Second, responsibility for performing activities in an incident-management process is often distributed among several organizations, which provided us an opportunity to examine mission risk in a distributed process.

We used MAAP to assess mission risk in a large government organization's incident-management process, which included three distinct points of management control and three geographic locations. At the conclusion of the analysis, senior managers from the government organization understood exactly how well events and incidents were managed throughout their organization. MAAP forecasted the expected outcome for the process in a variety of operational circumstances, providing a snapshot of the process' likely performance during expected and stressed conditions. We were able to provide managers with useful information without overwhelming them with unnecessary details. At the same time, MAAP enabled us to generate very detailed information that staff members could use when developing action plans for improving performance.

By following MAAP, we were able to characterize the impact of a range of conditions and potential events on the mission's potential for success. In the end, we were able to provide government managers with a roadmap for improvement using the comprehensive risk profile produced by MAAP.

6.2 MDP PILOTS

To date, we have piloted MDP in two very different environments: (1) incident management and (2) technology development. Our piloting of MDP in the area of incident management comple-

[11] An incident management capability is also commonly referred to as a Computer Security Incident Response Team (CSIRT).

mented our development and piloting of MAAP. As described above, we employed MAAP as a stand-alone assessment of an incident-management capability. In contrast, we used MDP to supplement a function-oriented assessment[12] of an incident-management capability [Dorofee 06].

The goal of the function-oriented assessment is to determine the extent to which the building blocks of an incident-management capability (e.g., activities, procedures, tools) are in place. However, it does not provide any estimate of the capability's overall effectiveness. To address this gap, we used MDP to estimate the overall state of health of the incident-management capability by evaluating a set of key indicators. Supplementing the function-oriented assessment with MDP helped managers understand how well cyber-security incidents were being managed and enabled those managers to chart a course for improvement.

Performing MDP in conjunction with the function-oriented assessment did not significantly increase the time needed to conduct the assessment and had no effect on the resources required for the assessment. At the same time, it produced a wealth of information about the incident management capability's state of health that helped frame the results of the function-oriented assessment. As such, MDP has become a standard supplement to the function-oriented assessment that the SEI is currently using when it evaluates an organization's incident-management capability.

The second environment in which we piloted MDP was technology development. In this instance, a large, complex medical organization needed a time-efficient means of evaluating new technology projects to determine which had the greatest potential for success. Management was overseeing a large portfolio of technology investments and wanted to manage its risk appropriately. We tailored a set of indicators to the needs and requirements of the investment problem space and to the organization.

We used MDP to assess an ongoing project and highlight key risk factors that were affecting the project. Management indicated that failure was not an option for this particular project. In this pilot, MDP highlighted several issues that had been overlooked or downplayed by management and showed how those issues cast doubt on the project's potential for success. A tailored method for applying MDP was transitioned to the medical organization for its continued use.

6.3 FUTURE RESEARCH DIRECTIONS

This report describes our initial work in the area of managing for mission success. While this research has provided many tangible results, we also believe there are many additional research avenues to explore in the future. Foremost, we intend to continue to refine SEI MOSAIC and pilot its protocols in different venues. Candidate areas for future applications include

- systems assurance
- supply chain management

[12] In a function-oriented assessment, an organization is measured against a baseline set of functions, or practices, to determine if those functions are actually performed. This type of assessment only evaluates whether each individual function is performed efficiently and effectively. It does not evaluate whether the overall collection of functions leads to efficient and effective performance of an end-to-end process. Using an analogy, a function-oriented assessment tells you if you have all the pieces in a jigsaw puzzle box; however, it does not examine whether the pieces have been assembled correctly to produce the desired picture.

- processes with strict reliability, security, and safety requirements
- management of critical infrastructures

Finally, our early focus when developing SEI MOSAIC has been on analyzing mission risk in complex environments. In our future research, we intend to define approaches for managing mission risk over time. In essence, we view the work documented in this technical note as a starting point for extending the discipline of risk management rather than as a completed body of research.

References

[Alberts 05]
Alberts, Christopher & Dorofee, Audrey. *Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments* (CMU/SEI-2005-TN-032, ADA441906). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/publications/documents/05.reports/05tn032.html.

[Alberts 04]
Alberts, C.; Dorofee, A.; Killcrece, G.; Ruefle, R.; & Zajicek, M. *Defining Incident Management Processes for CSIRTs: A Work in Progress* (CMU/SEI-2004-TR-015, ADA453378). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu/publications/documents/04.reports/04tr015.html.

[Alberts 02]
Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE*^{SM} *Approach*. Boston, MA: Addison-Wesley, 2002.

[Charette 90]
Charette, Robert N. *Application Strategies for Risk Analysis*. New York, NY: McGraw-Hill Book Company, 1990.

[Dorofee 06]
Dorofee, A; Killcrece, G.; Ruefle, R.; & Zajicek, M. *Federal Computer Network Defense (CND) Metrics Evaluation Method*, Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006.[13]

[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. http://www.sei.cmu.edu/publications/books/other-books/crm.guidebk.html.

[Gluch 94]
Gluch, D. *A Construct for Describing Software Development Risks* (CMU/SEI-94-TR-014, ADA284922). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1994. http://www.sei.cmu.edu/publications/documents/94.reports/94.tr.014.html

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

[Sharp 01]
Sharp, Alec & McDermott, Patrick. *Workflow Modeling: Tools for Process Improvement and Application Development*. Boston, MA: Artech House, 2001.

[13] Anticipated publication date is April 2007.

[Williams 99]
Williams, R.; Pandelios, G.; & Behrens, S. *Software Risk Evaluation (SRE) Method Description (Version 2.0)* (CMU/SEI-99-TR-029, ADA441900). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999.
http://www.sei.cmu.edu/publications/documents/99.reports/99tr029/99tr029abstract.html

[Young 01]
Young, Peter C. & Tippins, Steven C. *Managing Business Risk*. New York, NY: American Management Association, 2001.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	March 2007	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Executive Overview of SEI MOSAIC: Managing for Success Using a Risk-Based Approach	FA8721-05-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, and Lisa Marino

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2007-TN-008

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	

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

In today's business environment, multiple organizations routinely work collaboratively in pursuit of a single mission. These separate efforts result in process and programmatic complexity that is difficult to manage effectively. Mission success in these complex settings demands a collaborative management approach that effectively coordinates task execution and decision-making activities among all participating groups. Managing for mission success requires establishing and maintaining a reasonable degree of confidence that a mission's objectives will be successfully achieved. Confidence at the mission level requires establishing and maintaining a corresponding level of confidence in the people, processes, and technologies used to achieve a mission. The Software Engineering Institute (SEI) is currently developing the Mission-Oriented Success Analysis and Improvement Criteria (MOSAIC)—a suite of advanced, risk-based analysis methods for assessing complex, distributed programs, processes, and information-technology systems. With SEI MOSAIC methods, management can establish and maintain confidence in success throughout the life cycle and help provide assurance at the mission, system, and program levels. This technical note provides an executive overview of the concepts and foundations of SEI MOSAIC.

14. SUBJECT TERMS	15. NUMBER OF PAGES
mission success, managing success, risk, risk management, complex systems, risk analysis tools, risk analysis techniques, risk management tools, risk management techniques, managing complexity, complex systems management, risk analysis	35

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