Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments

Christopher J. Alberts
Audrey J. Dorofee

September 2005

Networked Systems Survivability Program

Technical Note
CMU/SEI-2005-TN-032

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.

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).

Contents

List of Figures

Acknowledgements

We would like to acknowledge the following individuals for reviewing this report and providing comments:

- Julia Allen
- Jeff Collmann
- Johnathan Coleman
- Eileen Forrester
- Bill Wilson
- Carol Woody

We would also like to acknowledge Suzanne Couturiaux for editing the document.

Abstract

The global business environment continues to grow in complexity. The typical business process is no longer under a single point of management control. Instead, it has become common for management of a work process to be shared among multiple groups. The permanent enterprise, defined by an organizational chart, has been replaced by the virtual enterprise, defined by the mission being pursued. Activities today are rarely supported by dedicated, stand-alone technologies. Rather, interoperable, networked technologies form the backbone of our information infrastructures. Today, managers must deal with interrelationships and dependencies among technologies, data, tasks, activities, processes, and people that were unimaginable just a few short years ago. Unfortunately, conventional risk analysis techniques have proven inadequate for characterizing risk in today's complex operational environments, so it was necessary to develop new and innovative approaches. The Mission Assurance Analysis Protocol (MAAP) defines an advanced, systematic approach for analyzing operational risk and gauging mission assurance in complex work processes. This report presents the concepts and underlying theories behind the MAAP, highlights results from early piloting of the technique, and outlines future research directions.

1 Introduction

Historically, responsibility for completing a mission and the resources needed to pursue it were 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. Supply chains, where business processes cross organizational boundaries, are commonplace today. In the modern business environment, workflow is no longer neatly contained within organizational boundaries. In fact, management control of work processes is often distributed among multiple organizations or groups. As a result, managers are increasingly finding themselves in the unenviable position of having responsibility for ensuring the completion of a mission while not directly controlling all of the resources needed to accomplish it. They cannot simply worry about managing risks arising in the activities they oversee. They must now be prepared to identify and address risks inherited from upstream activities and attempt to minimize the risks they impose on downstream activities. Success in the modern business environment requires a collaborative management approach that includes the ability to coordinate the risk management activities of multiple organizations.

1.1 The Need for an Enhanced Risk Management Approach

A crucial step when managing risk in any operational setting is determining the extent to which risk can affect operational performance. Risk assessments are useful when evaluating performance because they identify potential operational failures. We have spent the past decade researching better ways of identifying, analyzing, and managing risk in an attempt to help managers avoid such failures. Our early research focused on managing risk in software development programs. Here we worked with numerous programs and helped them implement cutting-edge methods for reducing their risks and developing better software and systems [Dorofee 96]. Later, we turned our attention to a different type of risk, information security risk, where we examined how security risks could affect an organization's ability to achieve its mission [Alberts 02].

Initially, we assumed that software development and security risk management were fundamentally different in nature, with each requiring a custom suite of tools and techniques. However, after developing distinct risk management approaches for both domains, we decided to revisit that assumption. As we sorted through endless volumes of assessment data, we began to notice similarities and patterns among them, which indicated that risk management in the two areas might share a mutual foundation. We then began to think about developing a common risk management solution, one that could be used in many diverse operational environments.

At about the same time, outsourcing and collaboration were becoming increasingly popular, fueled by the flexibility and portability provided by distributed computing. We began to see significant changes in the business landscape. The permanent enterprise, defined by an organizational chart, was fast becoming obsolete. It was being replaced by the virtual enterprise, defined by the mission being pursued. Work-process activities were no longer supported by dedicated, stand-alone technologies. Rather, interoperable, networked technologies formed the backbone of the information infrastructures supporting work processes. Management and staff had to deal with interrelationships and dependencies among technologies, data, tasks, activities, processes, and people that were unimaginable just a few years before. Not surprisingly, the complexity inherent in these collaborative environments beckoned for new and innovative approaches for managing risk.

Finally, we also noticed subtle, yet profound, changes in how managers were beginning to view risk management. Traditionally, their views were divided into two schools of thought. The first associated negative connotations with the word *risk*. Managers from this school often forbade staff members from openly discussing the possibility that risk could occur, which eliminated any possibility of mitigating its effects. By contrast, people adhering to the second school of thought viewed risk management as a means of avoiding failure. They would not hesitate to invest resources to manage specific sources of risk (e.g., security risk) in an attempt to evade particular hazards that could lead to disaster. Over the past few years, as we met with managers from a variety of government and business organizations, we began to see a third point of view emerge.

Rather than ignoring risk altogether or viewing risk management as a means of avoiding failure, some managers have begun to see risk management as a way to position themselves for success. They possess a holistic view of risk and are looking for ways to integrate information about different types of risk, such as process, security, and interoperability risks. They are seeking a single risk profile that provides insight into a mission’s potential for success. These managers are asking for a comprehensive risk assessment technique capable of consolidating information about a broad range of risk factors, rather than the piecemeal solutions so prevalent today.

Based on this anecdotal evidence, we decided to pursue the development of enhanced risk management tools and techniques that are designed to address the needs of today’s managers. We performed initial research to better understand the problem space, and, before long, a new body of research emerged.

1.2 Establishing a New Research Direction

Our initial goal for this new area of research was to develop tools and techniques to assess the potential for mission success in complex operational environments. This particular goal required us to extend our research in two directions. First, we needed to find a means of determining the degree to which a given mission is likely to succeed, thus establishing a measure of mission assurance. The ability to characterize the degree of risk in an operational environment enables management to gauge its potential for success, which is the central goal of mission assurance. Unfortunately, our initial research indicated that conventional risk assessment and management techniques were inadequate for establishing mission assurance.

Second, we needed to ensure that the tools and techniques for risk assessment and management were sufficiently robust to handle the degree of complexity prevalent in today's operational environments. We were particularly interested in exploring the potential for using risk management as a basis for process improvement and focused our research accordingly. As a result, we began to look at the types of risk affecting the performance characteristics of work processes, and this particular focus put work processes at the center of our research.

A work process is a collection of interrelated work tasks that achieves a specific result [Sharp 01]. It includes all tasks, procedures, organizations, people, technologies, tools, data, inputs, and outputs required to achieve desired objectives. The literature uses several terms synonymously with work process, including business process, workflow, and process. In this document, we use all four terms interchangeably.

Advances in technology, such as distributed computing and the Internet, have enabled people to link work processes together. The end result of connecting several small processes is a larger, more complex process, which includes numerous activities as well as intricate interrelationships and dependencies among those activities. Our initial survey of conventional risk assessment techniques indicated that they are inadequate for establishing comprehensive risk profiles[1] of complex work processes. In most cases, the risk analysis approaches underlying these conventional techniques are too simplistic to handle the inherent complexity of modern business processes.

A distributed work process is a type of complex workflow that is especially intriguing to us. In these processes, the flow of work products crosses organizational boundaries, which, in turn, requires management control of the process to be shared by multiple organizations. Typically, no one has end-to-end management authority in a distributed work process, which makes risk assessment and management extremely difficult propositions in these environments. We view distributed processes as an extreme example of process complexity and as a definitive test case for any techniques that we develop.

1.3 Hierarchy of Missions

After developing our research strategy, we began to execute it. We quickly learned that terminology was going to cause problems. Many common terms—such as *risk*, *process*, and *procedure*—do not have universally accepted definitions. Their meanings differ based on the circumstances in which they are used. This terminology problem has proved to be especially troublesome because our research is applicable to many diverse environments, including

[1] A *risk profile* is a generic term used when referring to the combination of factors that lead to risk in a given situation. In Section 6, we present a specific way of representing a mission's operational risk profile using a risk causal chain.

military, federal civilian, and industry settings. The word that seems to cause the most confusion is *mission*.

In its broadest sense, a mission describes 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. The term *mission* can also refer to the specific result being pursued by executing a work process. The mission of a work process must support appropriate department and organizational missions, while also outlining the tangible objectives of the process. In addition, each activity in a work process has a distinct mission.

For example, the organizational mission of the National Aeronautics and Space Administration (NASA) is to explore space. Each of NASA's programs, such as the shuttle program, has a unique mission that supports the overarching organizational mission. In addition, each space shuttle launch also has a distinct mission, where astronauts are required to perform specific experiments. And each of those experiments also has its own unique mission, or purpose. In essence, NASA has a hierarchy of missions, where each lower level mission aligns with and supports those above it.

A hierarchy of missions exists within all organizations. Ensuring that all missions in the hierarchy are aligned is an essential component of operational effectiveness. In fact, with outsourcing and collaboration becoming so widespread, the hierarchy often extends beyond a single organization to include multiple organizations, which can make aligning the mission hierarchy considerably more difficult to achieve.

As used in this document, the term *mission* refers to the set of objectives, or the goal state, being pursued when executing a work process. Put another way, the mission defines what success looks like for a process. In this context, a mission defines the tangible, and in many cases, measurable, objectives of a process. This concept is critical to our work, which examines how risk can affect the operational performance of work processes and cast doubt on the potential for mission success.

1.4 Scope of This Report

This technical note documents our work to date with respect to analyzing the mission assurance of work processes. It presents the concepts and underlying theories behind the Mission Assurance Analysis Protocol (MAAP), which is an approach for gauging the potential for mission success in work processes. The main focus of MAAP is developing advanced risk analysis techniques for highly complex and distributed work processes. However, we believe that MAAP can also be used to analyze risk in virtually all work processes, from very simple workflows to those that are distributed among multiple organizations.

This body of research is a work in progress, and this report provides a snapshot of our current thinking. To date, we have completed one pilot of MAAP and are currently looking for additional pilot opportunities. Additional reports will be published as appropriate, based on future research findings.

1.5 Structure of the Report

This technical note is divided into seven sections. This introduction serves as the first section; it provides background about the need for advanced risk management tools and techniques and introduces MAAP. Section 2, “Defining Risk,” provides the foundational concepts of risk management. It introduces the notion of operational risk, which is a specific type of risk featured throughout the remainder of the document. The guiding principles behind mission assurance are provided in Section 3, “Mission Assurance.” This section also establishes the link between mission assurance and operational risk.

We shift gears with Section 4, “Sources of Operational Risk.” Here, we propose the five categories of operational risk sources that are common to work processes. Next, in Section 5, “Operational Risk in Distributed Processes,” we look at the characteristics of operational risk in processes where management control is shared by multiple organizations. In this section, we establish the need for a new risk analysis approach that can handle the complexity inherent in distributed environments. The fundamental concepts of MAAP are presented in Section 6, “Mission Assurance Analysis Protocol (MAAP).” Finally, Section 7, “Applications and Future Directions,” completes the report by providing an overview of pilot activities for MAAP and outlining our future research directions.

1.6 Target Audience

As a whole, this report is written for people who have experience assessing and managing risk in operational settings. It presents a conceptual argument outlining the need for advanced risk management approaches, and it uses strategies, tools, and techniques commonly employed in today’s business environment as a basis of comparison. It also provides a general overview of the research we conducted when developing MAAP. People with the following types of expertise will likely derive the most benefit from reading this report: experienced operational managers, specialists in risk management, practitioners in business process design, organizational development experts, and Six Sigma black belts.

At the same time, casual readers might find that Sections 1-3 and 7 contain useful introductory material regarding operational risk management and mission assurance. However, Sections 4-6 delve into the details of advanced risk analysis, making these sections more suitable for readers with sufficient experience and expertise.

1.7 Focus on Risk

MAAP defines an approach for gauging the potential for mission success in work processes. It helps managers understand how various issues can influence process performance, and it incorporates advanced risk analysis techniques to effectively characterize the potential of experiencing operational failures. As a result, any presentation of MAAP must begin with a discussion of risk, which is the topic of the next section.

2 Defining Risk

The term *risk management* is used in a number of diverse disciplines and implies different meanings to different audiences [Kloman 90]. For example, the insurance industry relies on risk management techniques when setting insurance rates. To a hospital administrator, risk management is related to quality assurance concerns. Safety professionals view risk management in terms of reducing the number of accidents and injuries. Thus, the details about risk and how it supports decision making depend upon the context in which it is applied [Charette 89].

Because the term *risk* is used in diverse environments, there are many subtle variations in how it is defined in each. As a result, there is no universally accepted definition of risk. At the same time, some characteristics of risk are consistent across its many applications. In fact, for risk to exist in any circumstance, the following three conditions must be satisfied:

1. There must be loss associated with a situation.
2. There must be some uncertainty with respect to the eventual outcome.
3. Some choice or decision is required.

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 measurable aspects of risk. Keeping this in mind, the essence of risk, no matter what the domain, is succinctly captured by the following definition: *Risk is the possibility of suffering harm or loss*.

While it is one thing to be aware of the impending danger, harm, or loss associated with risk, it is entirely another matter to do something about it, or to manage it. Risk management defines a discipline for balancing the opportunities you seek against the losses you wish to avoid. It also provides the means for anticipating and addressing the numerous obstacles that can get in your way. When you follow a risk management approach, you put yourself in position to achieve your objectives through informed and proactive decision making.

2.1 Speculative and Hazard Risks

To address the rather complicated nature of risk, some people further subdivide it into two types: speculative and hazard risks [Young 01]. Figure 1 illustrates the differences between these two categories. With speculative risk you can realize a profit, improving your current situation relative to the status quo. At the same time, you have the potential to experience a loss, making you worse off than you are at present. Gambling is an example of speculative risk. When you place a bet, you must weigh the possibility of gaining additional money against the prospect of losing what you wagered.

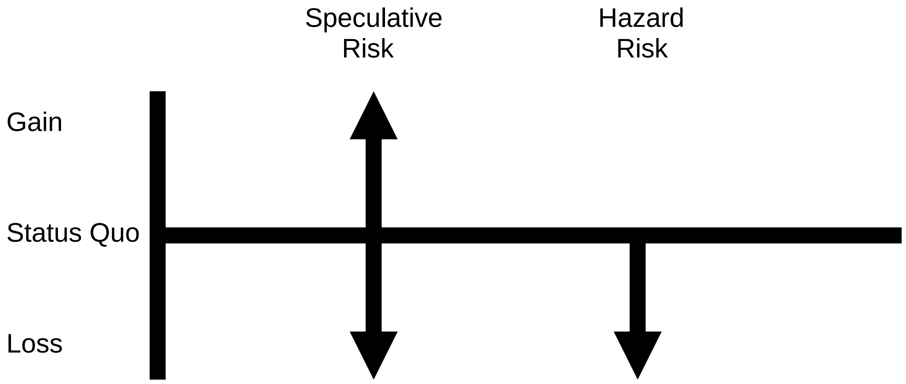

Figure 1: Speculative and Hazard Risks

By contrast, hazard risk only has potential losses associated with it, providing no opportunity to improve upon your current situation. Security risk provides an excellent example of hazard risk. When you install a security system in your residence, you are attempting to make it more difficult for a thief to break into the house and steal your valuables. In this case, you are using the system as a deterrent. However, in the best-case scenario, no one breaks into your house, and your money and valuables remain safely stored inside. Your wealth remains unchanged. Even in the most favorable of circumstances, you cannot improve upon the status quo by becoming more prosperous. You only keep what you already possess.

2.2 Business Risk

To this point in the document, we have focused on general concepts associated with risk, not on any particular context. We now narrow our focus as we set our sights on business risk, which encompasses all risks affecting a company’s business strategy. When viewed as a whole, business risk is speculative in nature; it requires managers to balance the risk of investing organizational capital against the potential return on that investment. This balance of risk and profit drives all business decisions. However, achieving equilibrium is never easy because of the complex nature of organizations and their business environments. Business risk tends to be multifaceted in nature and encompasses a wide variety of sources, including

- the organization’s financial situation
- the forecast for the organization’s market sector
- the strategies and practices of competitors
- potential changes in the domestic and international economies
- the potential impact of new technologies
- the potential impact of changing laws and regulations

- the organization’s operational work processes

Not surprisingly, businesses exhibiting long-term profitability often excel in many areas, including business risk management. However, our experience indicates that even companies with best-in-class risk management practices are finding it difficult to deal with certain aspects of business risk, such as the degree of *operational risk* now threatening them.

2.3 Operational Risk

Operational risk is a form of hazard risk affecting day-to-day businesses operations and, as such, is one of the many facets of business risk. As management executes its work processes, operational risks begin to emerge. Deficiencies inherent in processes can lead to inefficiencies and problems during operations, adversely affecting the chances for success.

Our current research focuses on operational risk because our experience indicates that its impact on organizations is growing. Managers are waging an ever-increasing battle with it and often find themselves on the losing end of that fight. New tools and techniques are needed to neutralize the growing danger posed by this particular form of risk. However, before we can even begin to propose an approach for managing it, we must first examine what makes it so hard to control.

The best place to start when exploring the intricate nature of operational risk is establishing its relationship to the mission underlying a work process. Recall that the term *mission,* when used in the context of a work process, refers to the set of objectives, or the goal state, being pursued when executing the process. It essentially defines what success looks like for a process. Operational risk affects that picture of success by casting doubt on the possibility the mission will be achieved.

Unfortunately, just as there is no single definition of the word *risk*, there is no universal definition for the term *operational risk*. In the absence of a standard, we opted to use the following definition: *Operational risk is the potential failure to achieve mission objectives.*[2] Notice that the definition includes both uncertainty (the potential failure of an operational process) as well as loss (the inability to achieve mission objectives), thus making it consistent with all definitions of risk presented earlier.

[2] The Basel Committee on Banking Supervision has published a capital adequacy framework commonly known as Basel II [BIS 04]. It defines *operational risk* as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. We considered using the Basel II definition of operational risk. However, we found it to be too limiting for our purposes because sources of risk are embedded in the definition. The categories of threat (i.e., sources of risk) we propose in Section 4 of this document include categories that go beyond the scope of the Basel II definition. As a result, we opted to use a broader definition that does not include sources of operational risk.

2.3.1 Operational Risks Versus Problems

Some people are prone to confusing operational risks with problems and often view them as interchangeable. However, in reality, the two concepts are quite different from each other. Recall that operational risk is a form of hazard risk, focusing on the *possibility* of mission failure. Uncertainty is a central tenet of operational risk and indicates doubt about whether or not a failure will occur. By contrast, when you are facing a problem, you are experiencing some form of distress or loss. There is absolutely no uncertainty about its occurrence.

The best way to differentiate between an operational risk and a problem is to focus on the time frame associated with each. Operational risk looks into the future, focusing on problems and failures that have not yet occurred, while a problem describes a situation that is presently taking place. Put another way, you can think of an operational risk as a potential future problem.

2.3.2 Operational Risk Tolerance

Mitigating operational risk requires an investment of resources; therefore, it is important to understand exactly how much you should spend. Real-world constraints, such as limited funds and resources, restrict the extent of mitigation efforts and require managers to make difficult choices about which risks to address actively. When allocating mitigation resources, management must weigh the potential for risk reduction against the associated costs, with the overarching goal of keeping risk at an acceptable level. *Operational risk tolerance is the maximum overall exposure to operational risk that will be accepted, given the costs and benefits involved*. The concept of operational risk tolerance is illustrated in Figure 2.

The vertical axis of the graph in Figure 2 indicates the amount of operational risk affecting a given mission, while the horizontal axis indicates the passage of time. Before any mitigation action is taken, the operational risk in the figure must exceed management's tolerance. Management must be willing to invest resources to reduce it. Once mitigation actions are implemented, some amount of risk, called *residual risk*, remains. Management generally continues applying mitigation resources until the residual risk falls within tolerance, as illustrated in Figure 2.[3] At that point, management takes no further mitigation action unless changing conditions warrant it (e.g., if a risk becomes a problem or if the risk profile changes).

The concept of operational risk tolerance is important because it influences the nature and extent of problems that are likely to occur during business operations. More operational risk generally equates to a greater occurrence of problems. And if management assumes too much

[3] In Figure 2, operational risk tolerance is represented by a line on the graph, which implies that it is a discrete value. However, in some instances, it might be more appropriate to define operational risk tolerance as a range with upper and lower limits rather than as a distinct value. The decision of how to represent operational risk tolerance will be influenced by a variety of factors, including the granularity of the analysis technique used (e.g., qualitative versus quantitative) and the amount of data available.

risk, it will likely end up in crisis mode, which will inevitably force management to assign valuable resources to activities that do not directly support its objectives.

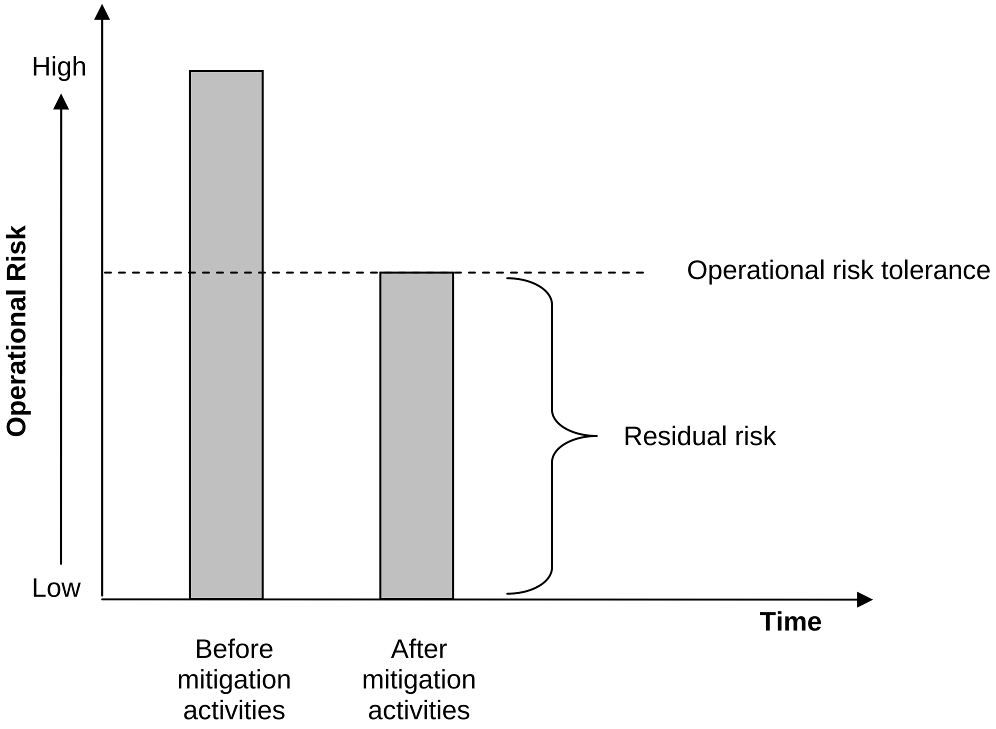

Figure 2: Operational Risk Tolerance

Maintaining operational risk at an acceptable level over time is thus a worthwhile management activity. Although the notion of keeping operational risk within tolerance is relatively straightforward from a conceptual point of view, achieving it in practice is not a simple endeavor. Our experience indicates that using operational risk tolerance to guide risk management activities can require considerable effort on the part of management and staff.

2.3.3 Challenges in Managing Operational Risk

Finally, today’s managers are finding it extraordinarily difficult to deal with the degree of operational risk confronting them on a daily basis. Although many factors contribute to this problem, two are especially influential.

First, some risks are not communicated effectively to people who are in the best position to manage them. Personnel who work most closely with a work process normally have an optimal vantage point for observing its nuances, and they understand its shortcomings and flaws. They develop unique insights into how operational risks can adversely affect their abilities to do their jobs. However, they are often unable to manage those risks because they do not usually have sufficient authority to allocate mitigation resources. At the same time, they may not bring sensitive issues to the attention of their managers because they fear reprisals or other repercussions. In other instances, people might not even know with whom they should discuss their concerns. If these risks are not communicated to management, they cannot be adequately addressed.

The second reason why operational risk is so difficult to control is the inability to effectively manage process and technological complexity, making it difficult to establish accurate risk profiles. People normally understand the fundamental performance characteristics of the processes and technologies they use, and they learn enough about them to complete their assigned work tasks. This basic knowledge of the operational environment is also sufficient for identifying many risks related to those tasks. However, people generally do not understand all of the subtleties and nuances inherent in complex environments. For example, they might not realize how their tasks and activities relate to those of other staff members, groups, and enterprises. They also might not recognize how their part of the work process connects with and supports related processes. In addition, management is often unable to see the benefit of investing the time and resources required to characterize subtle and complex operational risks. As a result, risk arising from operational complexity often goes unmanaged. Instead, it acts like a ticking time bomb within processes and technologies that goes unnoticed until it produces catastrophic failure.

Operational risk affects work processes by laying a foundation for future problems. Managers must carefully evaluate their options and make thoughtful decisions when attempting to keep operational risk under control. The ability to manage operational risk effectively is one factor that separates successful managers from the rest of the pack. Their proactive ability to avoid obstacles provides them confidence in their potential for success, which is a hallmark of mission assurance.

3 Mission Assurance

We have all heard about or participated on projects that have battled one crisis after another. Too often resources that are allocated to these projects are wasted fighting fires instead of being optimized in pursuit of the mission. Crises divert people's attention from the tasks at hand, ultimately leading to cost, schedule, and quality problems. In addition, problems may build upon each other, until at some point, mission failure is assured. Fortunately, most disasters can be prevented because there are usually indications of failure long before the resulting catastrophe occurs. It is essential to seek out indications of failure and take timely action to avoid it, so that management can have confidence in the project's chances for success.

3.1 Defining Mission Assurance

Based on our research, there is no universal definition for mission assurance. However, most of its definitions include one common theme: the belief, or conviction, that mission objectives will be satisfactorily achieved. Using published information about mission assurance in combination with our risk management experience, we have derived the following definition: *Mission assurance is establishing a reasonable degree of confidence in mission success*.

Mission assurance is not a binary attribute that is either present in or absent from a given situation. On the contrary, it falls along a continuum, with guaranteed success at one end of the scale and guaranteed failure at the other. The degree of mission assurance inherent in a work process is inversely related to the amount of operational risk affecting that process. As a result, when operational risk is reduced, mission assurance increases in kind. And the desired level of mission assurance is achieved when operational risk to the mission is kept within tolerance.

3.2 Mission Assurance Strategy

Figure 3 depicts the basic strategy supporting mission assurance and illustrates the importance of striking a balance between operational risk management and problem resolution activities. Unfortunately, operational risk management is often overlooked or performed poorly, causing many managers to accept more risk than they should. Greater risk is an indicator of a greater number and severity of problems during operations. As a result, management redirects too many resources to handle an ever-increasing series of crises, leaving fewer people available to work toward mission objectives. By contrast, keeping operational risk within tolerance minimizes problems during operations and enables management to more easily handle any problems that occur, while directing most of its effort toward achieving the mission at hand.

Three fundamental tactics for achieving mission assurance are also illustrated in Figure 3. The first tactic is addressing operational risk when processes are being designed and developed. Too often, developers lack a sufficient appreciation of the operational environment in which processes will ultimately be used. They tend to overlook the importance of dealing with risk prior to operations, preferring instead to let others deal with it during process execution. This inaction translates to a lost opportunity, because certain risks can be mitigated and, in some cases, avoided altogether when a process is still in the planning stages. There are also economic considerations for reducing operational risk as early as possible. It is generally more cost effective to mitigate risks during design and development than waiting until operations.

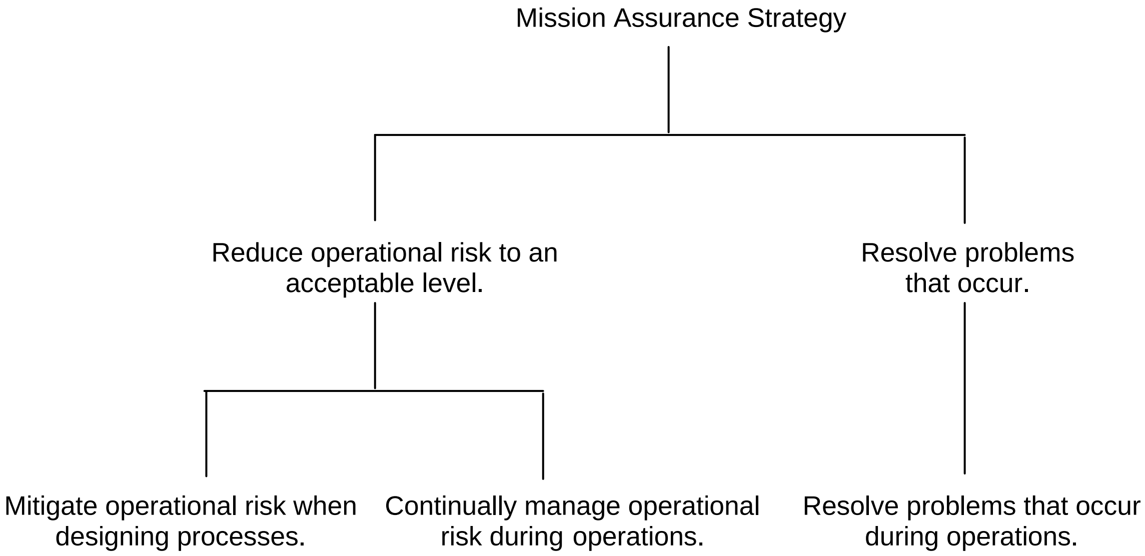
Mission Assurance Strategy
Reduce operational risk to an acceptable level.
Resolve problems that occur.
Mitigate operational risk when designing processes.
Continually manage operational risk during operations.
Resolve problems that occur during operations.

Figure 3: Mission Assurance Strategy

Although it is a good idea to mitigate as much risk as possible during design and development, your options are somewhat limited. Many sources of risk first become apparent during operations, making it impossible to tackle the resulting risks before processes are in use. Thus, you must also manage risk during process execution, which is to the second tactic of the mission assurance strategy. Continual attention to risk management during operations reinforces mitigation actions already taken and helps ensure that risk is maintained at an acceptable level over time.

The third and final tactic—resolving problems that occur during operations—complements the first two. Even the most aggressive risk management programs do not *eliminate* risk; they merely reduce it. Thus, you will always have some amount of uncertainty regarding your chances of success. The goal is to tilt the odds in your favor by minimizing the amount of uncertainty you ultimately accept. Being able to effectively manage operational risk enables you to apply resources to the few problems that will inevitably occur when work processes are conducted.

The fundamental concept of mission assurance is straightforward: a reasonable degree of confidence in mission success is established when operational risk is kept within tolerance. In many cases, keeping operational risk within tolerance is easier said than done. Effective operational risk management requires an attention to detail as well as an ability to abstract. It forces you to look at both the global and local properties of a process in an effort to gauge performance. It requires understanding what success looks like in order to predict the potential for failure. And recognizing what can cause those failures is an essential part of controlling risk. The next section describes the details of operational risk by examining its causes.

4 Sources of Operational Risk

In our past research, we studied different facets of operational risk. We first looked at how poor risk management led to failure in many software development projects. We also studied organizational security and examined how security risks can adversely affect an organization's mission. Upon reviewing our research in both areas, we saw many similarities and patterns. We began to notice how our previous work focused on pieces of a larger puzzle. We decided it was time to pursue the broader themes by looking at operational risk and the sources responsible for producing it.

4.1 Threat and Risk

People in position to allocate mitigation resources must first become aware of a risk before they can address it. In fact, our experience indicates that the ability to communicate risks in a clear and consistent manner is a common characteristic of most effective risk management programs. Establishing a common structure for communicating risks is one practice that enables people to articulate their concerns more effectively. The basic format for expressing risk information is called a *risk statement*, which is framed around the concepts of threat and risk. Figure 4 illustrates the relationship between threat and risk that provides the foundation for a risk statement.

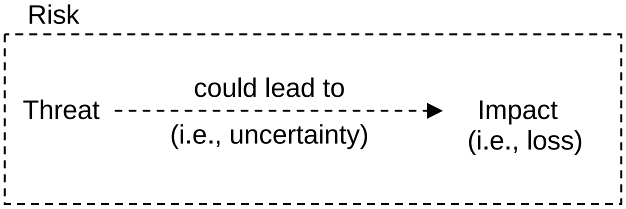

Figure 4: Threat and Risk

A threat is a circumstance or event with the potential to cause harm or loss; threats capture the source of concern, doubt, anxiety, or uncertainty at the heart of risk. However, threat, by itself, illustrates only *what* is causing your concern, not *why* you are concerned. To understand the reason behind your anxiety, you must also understand the impacts, or consequences, that are potentially triggered by the threat. When you describe one or more potential impacts, you have effectively described a risk. A risk statement is thus a cause-and-effect pairing of a threat with the impacts it can produce.

4.2 Painting a Picture of Risk

A succinct risk statement provides a means for communicating your concerns to others. It also helps when you are deciding how to address a risk because it provides the following key pieces of information:

- The threat component focuses on what is currently causing concern and provides useful information for determining specific steps required to mitigate a risk.
- The impact component focuses on potential immediate and long-term consequences triggered by a threat, and it describes the possible losses you might sustain. Understanding the depth and breadth of potential consequences is useful information when determining the amount of time, resources, and effort that should be allocated to mitigating a risk.

The risk statement is a practical technique for capturing and recording risks, and it provides a consistent means for conveying these risks to others. However, the structure alone does not guarantee success. The content must also be clear and concise, and it must enable risks to be easily understood by all. Developing a risk statement requires people to succinctly articulate the sources of their concerns (i.e., threats) as well as the potential consequences (i.e., impacts), which our experience shows is not as easy as it might appear.

When identifying risks, people often rely upon tools that document common sources of risk, such as surveys, questionnaires, or checklists. These instruments help to focus attention on a wide range of threats and prompts people to consider as many sources of risk as possible. Unfortunately, based on our field experience, many surveys, questionnaires, and checklists are not as exhaustive as they need to be, and they often omit important sources of risk.

4.3 Categories of Operational Threat

Over the years, we have performed risk assessments in a variety of operational settings. Over time, we began to notice an interesting trend: Similar threats seemed to trigger risk in very different domains. At first, this trend seemed counterintuitive to us. Why would threats to software development projects be so similar to those affecting organizational security processes? To answer this question, we began to dig a littler deeper. We reviewed a vast array of materials when looking into this phenomenon (including numerous publications and the results of many risk assessments[4]). As a result of this work, we identified the five categories of threat depicted in Figure 5. To our surprise, all threats documented in the reference materials and assessment results neatly mapped into the five categories.

[4] We performed an extensive survey of the risk management publications as part of this work, including published works by Alberts, Carr, Charette, and Haimes [Alberts 02, Carr 93, Charette 89, Haimes 04]. We also examined the results of risk assessments in the following areas: software development, information security, and incident management. These assessments were conducted with a variety of organizations, including groups from the government, financial, manufacturing, health care, and technology sectors.

By the same token, there were significant gaps regarding the range of threats included in all assessment techniques surveyed. Most focused on two or three of the categories, while either ignoring or giving cursory attention to the others. For example, risk assessments for software development projects typically had reasonable coverage in the design and activity categories, but paid little attention to mission, environment, and event threats. As a result, threats from those three categories would likely be overlooked during risk identification and analysis activities, which could lead to incomplete assessment results. We believe that the five categories provide a benchmark of operational risk sources and could be used to identify gaps in surveys, questionnaires, and checklists employed in many assessments.

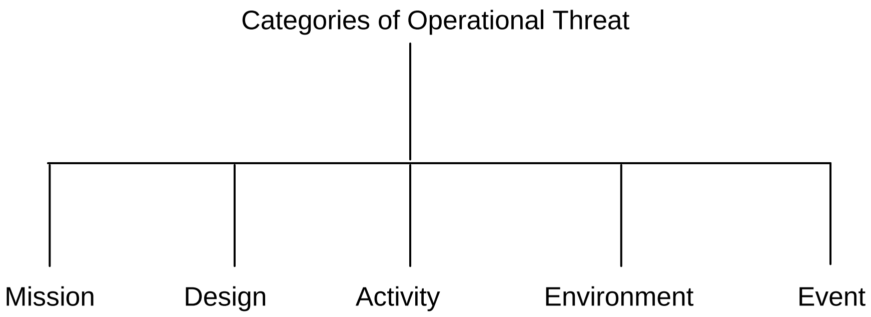

Figure 5: Categories of Operational Threat

The research regarding the categories of threat is a work in progress. We cannot rule out the possibility that additional data will lead us to add a category. Likewise, while these categories seem to cover threats to work processes, we have not looked extensively at how well they address threats in other problem spaces, such as in technological systems. We intend to look at broader applications for these categories at some point in the future. At the present time, we are focusing on operational risk as it relates to work processes. In the remainder of this section, we take a closer look at each category, beginning with mission threat.

4.3.1 Mission Threat

The mission is the cornerstone of a work process and defines what success looks like. If that picture is skewed or flawed, the entire system could be out of balance and produce unexpected, or unwanted, results. For example, if the technical objectives of a software development project are overly ambitious in relation to its budget, you will have to make difficult choices when beginning the project. Lacking the requisite funds, you might be forced to cut back on staff allocated to certain tasks, or you might decide to eliminate certain equipment expenditures. Something, somewhere, has to give.

The consequences of your choices will not be felt immediately, but somewhere during the course of the project you will almost certainly encounter a crisis. When that crisis occurs, you will have to make some difficult decisions. You might be forced to adjust the technical objectives by aligning them more closely with the remaining budget. Or you might have to consider assuming a cost overrun for the project. If the former is chosen, you will have the unpleasant task of informing your customer that the software lacks some of its promised features. If the latter is selected, your management will undoubtedly be eager to hear your explanation for the budget overrun. The imbalance that existed from day one will have come full circle and will require a change to the mission objectives.

A mission threat is a fundamental flaw, or weaknesses, in the purpose and scope of a work process. It injects considerable vulnerability into the very foundation of a work process and exposes it to a substantial amount of operational risk. The vulnerability can manifest itself in a number of tangible ways and can affect all aspects of the process, from the layout and arrangement of activities to the resources assigned to those activities.

4.3.2 Design Threat

While the mission describes the goal, or objectives being pursued, the design of a process delineates the roadmap for achieving the mission. It outlines the resources needed to complete the job as well as all steps, decisions, and handoffs required to execute the process successfully. A design threat is an inherent weakness in the layout of a work process. It can have far-reaching consequences because it embeds risk within the structure of a process.

A bottleneck is an excellent example of a design threat, illustrating how inefficiencies can be designed into a process. The presence of a bottleneck means that the flow of work products exceeds the capacity designed into the process, which limits the flow at a particular point in the process. Such restrictions cause the process to function at a lower level of efficiency than required to meet mission objectives and casts doubt on the potential for success.

4.3.3 Activity Threat

Whereas the mission and process design provide the blueprint for operations, activity management is focused on assembling, organizing, and overseeing the resources needed to execute that plan. An activity threat is a flaw, or weaknesses, arising from the manner in which activities are managed and performed. This type of threat can result from a variety of sources, ranging from people’s actions to unreliable performance of support technologies. In essence, activity threats occur when actual performance deviates from what was planned or anticipated.

For example, think about what happens when inexperienced people, who also have not received adequate training and education for their positions, staff a process. Do you expect novices to perform their assigned tasks seamlessly? In all likelihood, they will be prone to making mistakes and poor decisions, at least initially, which puts the mission at risk.

4.3.4 Environment Threat

In an ideal world, managers would be able to ignore the outside world, focusing solely on the tasks at hand. However, processes are not executed in vacuums. Managers need to be keenly aware of their surroundings and understand how environmental conditions can affect their work. An environment threat is an inherent constraint, weakness, or flaw in the overarching operational environment in which a process is conducted. It represents an inherited source of threat, making it especially difficult to manage in many instances.

Think about an organization plagued by low morale among its staff. People who work in such environments tend to have higher rates of absenteeism, often leaving key activities short staffed. They may also take less pride in their work, choosing to go through the motions each day. The end result of such apathy is poor performance, which, of course, places mission objectives at risk. Although the manager of a given work process might not be responsible for the root causes of low staff morale, he or she must deal with its effects on process performance, which will likely not be an easy task.

4.3.5 Event Threat

Because our world is constantly changing, we must be on guard for sudden events that can immediately derail progress. An event threat is a set of circumstances triggered by an unpredictable occurrence that introduces unexpected change into a process. A computer virus is a good example of an event threat. Many vulnerabilities are embedded in the computer systems that we use every day. Some can affect a computer’s performance during routine use by causing it to crash periodically. By contrast, others lie dormant within the computer’s operating system and applications and do not produce any visible effect on the computer’s performance during day-to-day operations.

A computer virus is a program that is designed to exploit these dormant, apparently benign, vulnerabilities and that causes infected computers to act erratically. People with malicious intent design these programs with the ultimate goal of wreaking havoc throughout the business community. Viruses can be sent as email attachments, becoming active when unsuspecting users open those attachments. Although there are different types of viruses, which affect computers and their supporting networks in different ways, they typically produce similar results, 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 puts the work-process mission at risk. Notice that the vulnerability in this example posed no threat to production during typical operating conditions. It took an unpredictable event, in this case the proliferation of a computer virus, for damage to occur.

4.4 Extrinsic and Intrinsic Risk

Of the five categories of threat, event threats stand out as being fundamentally different from the others. With event threats, vulnerabilities do not directly place a mission at risk; they are merely a conduit for risk and lie dormant during normal business operations. An event must combine with one or more of these vulnerabilities to actually produce risk. If there is no possibility of the event occurring, there is, by definition, no risk. In this document, the risk produced by an event threat is called *extrinsic risk* because its underlying trigger (i.e., the occurrence of an event) occurs outside of expected or predictable operational conditions. The mechanism responsible for generating extrinsic risk (i.e., an event in conjunction with one or more vulnerabilities) also influences its basic properties, which are measured using probability and impact. In general, the probability associated with extrinsic risk is heavily influenced by the likelihood that its triggering event will occur. As a general rule, events with the potential for producing very high, often catastrophic, consequences have very low probabilities associated with them.

By contrast, threats from the other four categories (mission, design, activity, and environment) do not require an external trigger to produce operational risk. In this case, the mere act of conducting a work process in combination with certain vulnerabilities is sufficient. The risk generated by these four categories is called *intrinsic risk* because it is an inherent part of process execution. The characteristics of intrinsic risk are quite different from those of extrinsic risk. For example, intrinsic risks are often more likely to occur than extrinsic risks because the stimulus needed to produce intrinsic risks (i.e., process execution) is always present. In addition, while extrinsic risk often produces catastrophic consequences, experience shows that intrinsic risks can cause a variety of impacts, ranging from negligible to very high. Catastrophic impacts triggered by a specific source of intrinsic risk, although possible, are rare.

The five categories of threat thus define a broad range of operational risk sources. As noted earlier, few risk assessments consider threats from all five categories. Instead, they focus on a subset of threats, which makes it impossible to reach any conclusions regarding mission assurance. You cannot establish a reasonable degree of confidence in mission success without considering a broad spectrum of threats during an analysis. At the same time, there are additional factors that complicate risk analysis in distributed processes. In the next section, we describe the unique issues that make characterizing operational risk in distributed processes so problematic.

5 Operational Risk in Distributed Processes

The business landscape has changed dramatically in the past decade, much of it fueled by a rapidly changing technological infrastructure. Networked technologies have enabled partnerships and collaborations that were unimaginable just a few years ago. As a result, work processes are no longer constrained by geographical and organizational boundaries. Today it is common for multiple organizations to pool appropriate resources in pursuit of a single mission and bring together a diverse set of skills without regard to physical location or organizational allegiance. These *virtual organizations* are bound by common missions rather than organizational charts. It is no longer valid to assume that a single manager controls end-to-end process execution. In fact, management control is often distributed among several organizations, creating a complex operational environment that can be difficult to manage.

5.1 Distributed Processes

Recall that a process is a collection of interrelated work tasks intended to achieve a specific result by taking inputs and transforming them into desired outputs. This is the fundamental philosophy underlying all work processes. For example, think about the basic operations of a system development process. A development team collects the technology requirements of a customer and creates a technology uniquely designed to meet that customer’s needs. To accomplish its mission, the development team must follow a prescribed path, or process, that defines the proper sequence and timing of all necessary activities. And if everything proceeds according to plan, the technology produced will meet the needs originally described by the customer.

Work processes can be visually represented using workflow diagrams such as the one shown in Figure 6. Notice that the process depicted in the figure comprises four distinct activities, which must be executed in the order shown (from left to right) to achieve the mission. Process execution kicks off with Activity A1. Once it is complete, its output feeds Activities A2 and A3, which are performed in parallel. When both of these activities are complete, their outputs are forwarded to Activity A4, the last in the sequence. Upon completion of Activity A4, the process is finished. If all activities are performed correctly, the mission is successfully achieved.

A process, when viewed as a whole, exhibits unique performance characteristics that arise from the manner in which the process is structured and managed. For example, certain conditions, such as an experienced and well-trained staff, enable good performance and propel a process toward its mission. On the other hand, others, like lack of teamwork, threaten mission success. The performance characteristics of a process are influenced by many different factors, including

- its structure
- how its tasks are executed
- the operational environment in which it is executed
- how it is managed

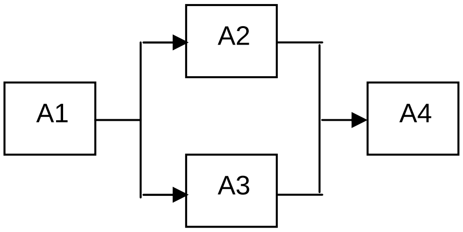

Figure 6: Work Process with Four Activities

When a single manager oversees an end-to-end process, he or she has considerable control over most aspects of its operation. If problems develop in one activity, the manager can react by reallocating people or funds from other activities to help resolve the underlying issues. However, now think about what happens when a process is linked to several others, as illustrated in Figure 7.

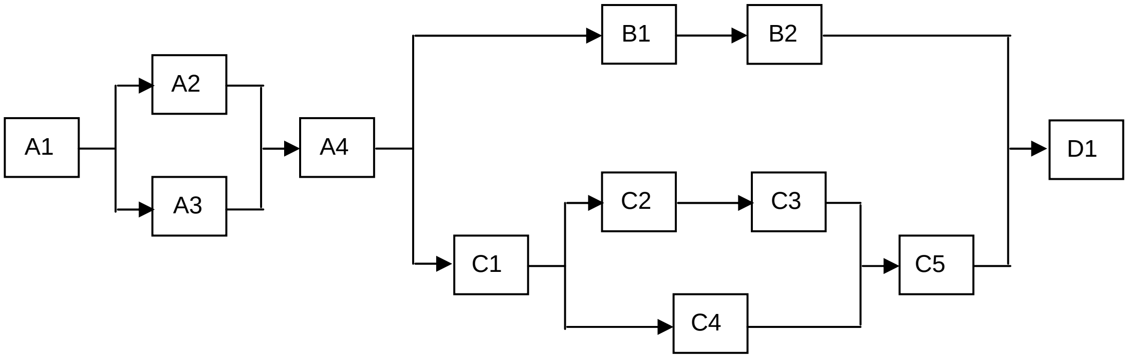

Figure 7: Distributed Work Process

Notice that the rather simple process from Figure 6 is now part of a larger process that links four distinct sub-processes. Each sub-process has its own unique set of objectives (i.e., a local mission) to achieve; however, the overall work-process mission is not achieved until the final activity is complete. As illustrated in Figure 8, four organizations have pooled their resources to complete a single mission, thus creating a distributed business process.

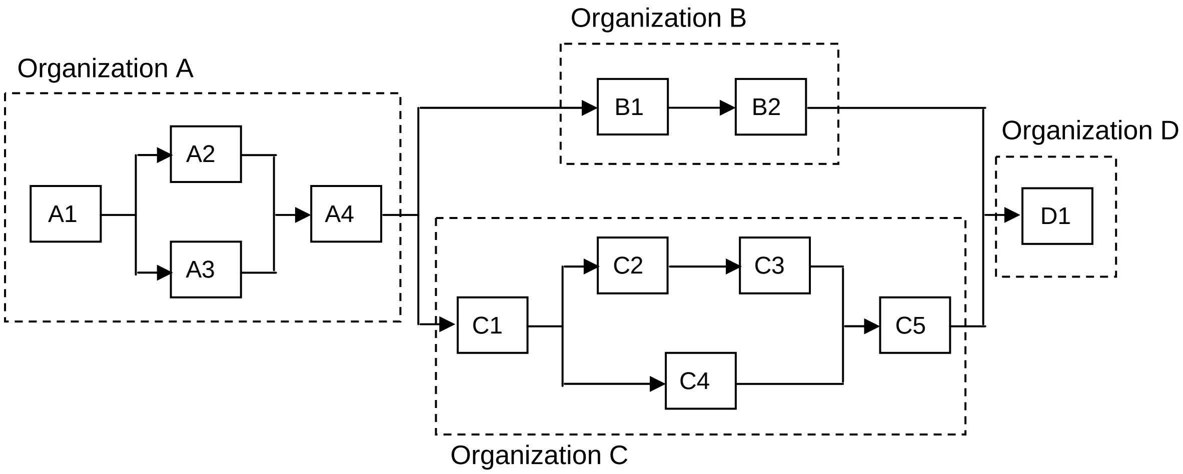

Figure 8: Four Organizations; One Mission

5.2 Lack of Uniform Operational Risk Tolerance

In distributed processes, management from each organization controls its piece of the overall process, and, in most cases, no one has management authority over the end-to-end workflow. Instead, management control is exerted locally, with contractual relationships defining the relationships among all participating organizations. Mission success is contingent upon each group fulfilling its contractual obligations. However, most contracts specify only deliverables and milestones; they leave the specifics of how to achieve them to the discretion of each organization's management. And most contracts do not mandate a common approach for managing risk; instead they give each manager considerable autonomy in this regard. As a result, there tends to be a lack of uniform operational risk tolerance in most distributed processes, as illustrated in Figure 9.

A manager's tolerance for operational risk influences the nature and extent of the problems likely to occur during operations. When managers are generally risk averse, their decisions reflect their desire to avoid risk. Likewise, managers who accept more risk are willing to endure a greater number and severity of problems during operations. Because a uniform risk tolerance is usually not imposed on a distributed process, management's tolerance for risk tends to vary throughout the process either by choice (e.g., personal preference of the manager) or circumstance (e.g., internal politics force a manager to accept more risk than he or she would like). Notice that the tolerances in Figure 9 range from low to high, creating a mismatch in how risk is managed throughout the process.

Most often, managers in a distributed process act unilaterally and assume that their actions have no effect on their partners. However, because of the inherent interrelationships and dependencies among activities in a workflow, that assumption is incorrect. In fact, the operational risk affecting a given activity in a distributed process influences the risk affecting all subsequent activities. As a result, all managers need to be aware of the risk they inherit from upstream activities and, in turn, impose on downstream activities.

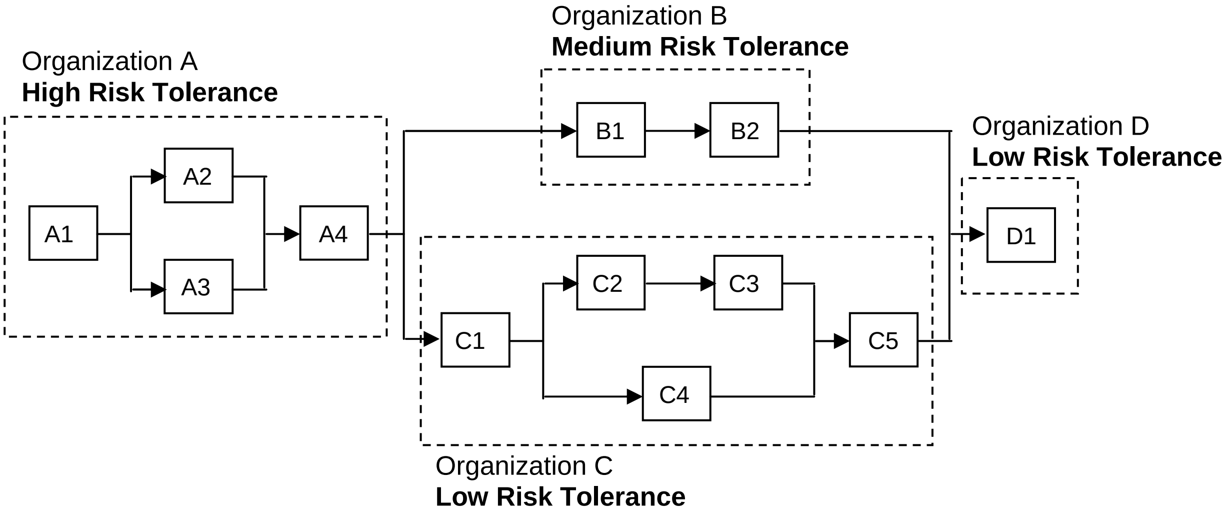

Figure 9: Lack of Uniform Operational Risk Tolerance

5.3 Inherited and Imposed Risk

Consider the distributed work process in Figure 9. Now focus on just one part of the end-to-end process: the activities performed by Organization C. You will notice that Organization C receives work products from Organization A and subsequently forwards its work products to Organization D. If you assume the perspective of Organizations C's management, your view of the distributed process becomes quite limited. As shown in Figure 10, Organizations C's management has a narrow view of the process, with little insight into what occurs before it receives work products from Organization A and after it delivers its products to Organization D.

Organization C's management likely does not have detailed knowledge of the inner workings of the processes and practices of its partners. As a result, it would be extremely unusual for Organization C's management to have much insight into how operational risk is managed by its partners. This can be problematic because Organization C's biggest risk might be the amount of operational risk it inherits from Organization A. For example, the work products it receives from Organization A *could* be riddled with defects, or they *could* arrive much later than anticipated. Managers in Organization C cannot establish an accurate risk profile without knowing the extent of the risk they are inheriting.

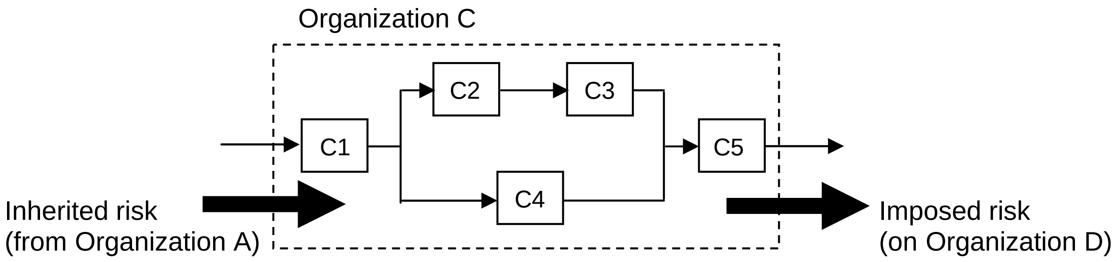

Figure 10: Inherited and Imposed Risk

Likewise, Organization C imposes some degree of operational risk on all downstream activities (in this case, the activity performed by Organization D). The amount of risk imposed on downstream activities generally depends on two factors: (1) how much risk is inherited from upstream activities and (2) the amount of risk generated locally. In this way, operational risk flows in unison with work products as they move throughout a process; it is amplified or dampened at any particular point in the workflow based on conditions at that location. Put another way, operational risk can be viewed as a dynamic property of any work process because it changes as it flows from one activity to the next.

5.4 The Dynamic Nature of Operational Risk

Consider the simple process depicted in Figure 11. Two activities are performed in sequence, with Activity Y beginning after the completion of Activity X. When both activities are performed satisfactorily, the mission for this simple process is successfully achieved.

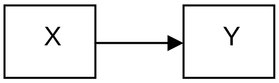

Figure 11: Basic Work Process

Now consider how a specific threat to Activity X might affect the work-process mission. A threat is a circumstance or event that can adversely affect execution of any work-process activity. Because, by definition, a work process comprises a collection of interrelated activities, a threat affecting the completion of any particular activity casts doubt on the potential for overall mission success. Put another way, a threat to any given activity triggers risk to the work-process mission. Figure 12 illustrates how a threat to Activity X puts the overall work-process mission at risk.

Notice that Figure 12 shows a direct link between a threat, T_{X1}, and the risk to the mission, R_{X1}, depicting the risk produced by a single threat. This linear approach to risk analysis is useful when interrelationships and dependencies among activities are relatively straightforward because it provides a way to sort through vast amounts of risk information quickly and reach meaningful conclusions. However, linear risk analyses do not explicitly provide a means for tracking inherited and imposed risk, which makes them less useful when analyzing complex work processes. As a result, advanced risk analysis techniques must be employed when examining how operational risk actually propagates throughout complex processes. We can no longer view operational risk as a series of independent linear occurrences. Rather, we must begin to see it as an interrelated set of circumstances, as illustrated in Figure 13.

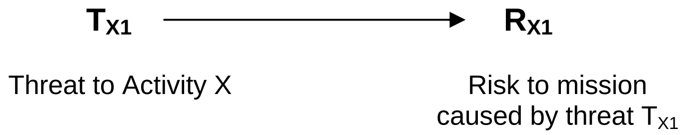

Figure 12: Simple View of Risk

Notice from Figure 13 that three threats (T_{X1}, T_{X2}, and T_{X3}) affect Activity X. In addition, the figure also introduces the concept of a control, which is important when examining how operational risk flows throughout a process. Controls include the policies, procedures, practices, conditions, and organizational structures designed to provide reasonable assurance that a mission will be achieved and undesired events will be prevented, detected, and corrected.[5] In other words, they are the circumstances that propel a process toward its mission. In Figure 13, two controls (C_{X1} and C_{X2}) affect Activity X.

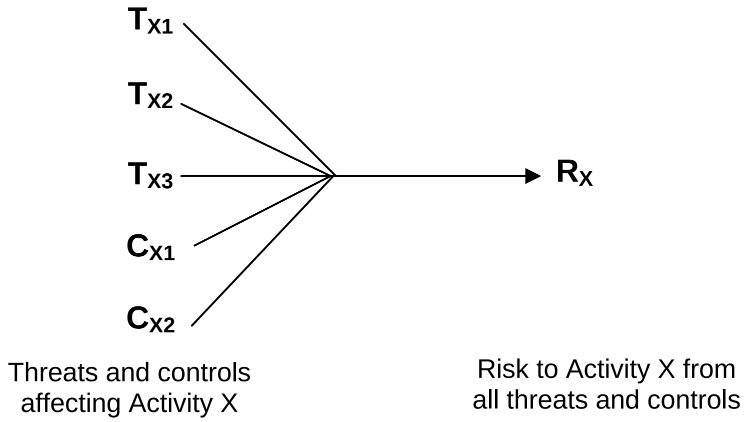
T_{X1}
T_{X2}
T_{X3}
C_{X1}
C_{X2}
R_X
Threats and controls affecting Activity X
Risk to Activity X from all threats and controls

Figure 13: Interrelated View of Risk

Numerous controls influence the execution of each activity. Some controls must be explicitly considered during risk analysis because they directly mitigate the risk at a given point in the process. In some instances, they decrease the likelihood of a risk’s occurrence, while in others, they might reduce potential losses. Thus, a true measure of the operational risk affecting any given activity must include all relevant interactions among threats and controls.

[5] The definition for *control* is derived from *COBIT*® [ISACA 00].

To illustrate the relative effects of threats and controls, consider the following example. Assume that you are performing an operational risk assessment and have noticed that the procedures for completing a key activity are not documented. As a result, people must rely on their tacit knowledge of how to perform that activity correctly. Normally, you might be concerned about the effects of insufficient documentation on process performance and identify it as a design threat. However, if the process is relatively stable over time and the staff has considerable experience and expertise performing the activity correctly, the effects produced by a lack of procedures might be lessened. In this instance, the staff's experience and expertise is considered to be a control because it is an organizational condition that counteracts the design threat. The true measure of operational risk thus requires balancing the relative effects of the threat and the control.

By looking at Figure 13, you will notice that to this point we have established the degree of operational risk affecting only Activity X. We have not begun to consider how conditions affecting Activity Y influence operational risk in the work process. Thus, the next step in the analysis is to examine the effects of operational risk on Activity Y. And since Activity Y is the final activity in the workflow, the risk analysis of the end-to-end process is considered to be complete when the analysis of Activity Y has concluded. The threats and controls affecting Activity Y are shown in Figure 14.

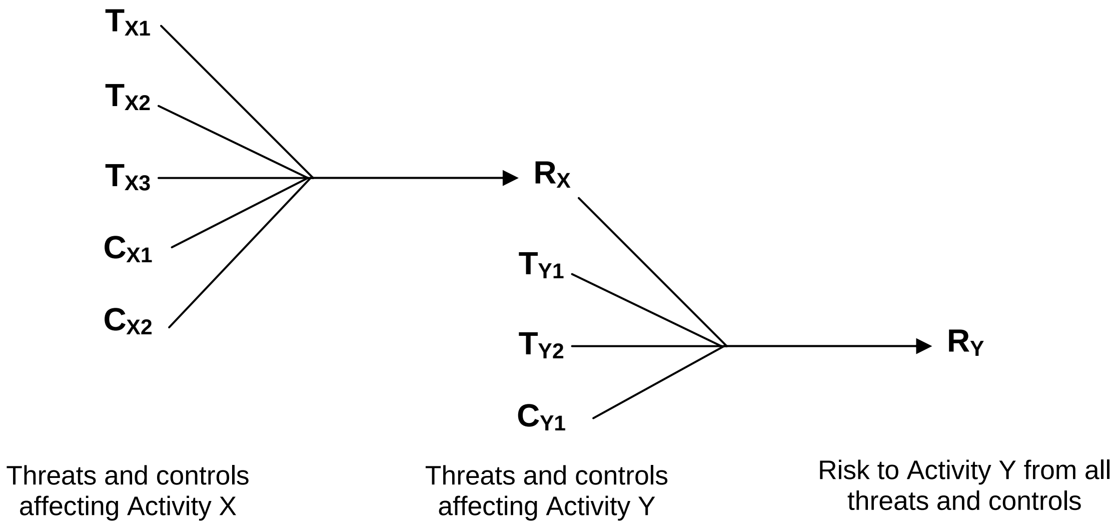
T_{X1}
T_{X2}
T_{X3}
C_{X1}
C_{X2}
R_X
T_{Y1}
T_{Y2}
C_{Y1}
R_Y
Threats and controls affecting Activity X
Threats and controls affecting Activity Y
Risk to Activity Y from all threats and controls

Figure 14: Risk to the Mission

You will notice from Figure 14 that two threats (T_{Y1} and T_{Y2}), one control (C_{Y1}), and the risk inherited from Activity X all contribute to the operational risk affecting the execution of Activity Y. Operational risk actually propagates throughout a work process by moving from one activity to the next in unison with the flow of work products. As a result, the operational risk affecting any given activity cannot be determined precisely without knowing the amount of risk it inherits from previously completed activities. In this way, operational risk can be viewed as a dynamic property of a process. It moves from point to point in a workflow and is amplified or dampened based on the relative conditions at each point.

For example, assume that Activity X has a high risk to its schedule, meaning that there is a reasonable likelihood that Activity Y will receive its inputs much later than planned. For the purposes of this example, assume that a two-week delay is likely. Activity Y thus inherits a schedule risk, a potential two-week delay, from Activity X. However, the effect of this inherited risk cannot be fully determined until all threats and controls affecting Activity Y are also considered.

What if Activity Y has a buffer in place that enables it to absorb up to a three-week delay (e.g., adequate inventory, arrangements with an alternate supplier, slack in the schedule)? This particular control, by itself, has dampened the inherited risk. Other controls might further negate the risk, while the threats affecting Activity Y might reinforce it. As a result, Activity Y's schedule risk is the product of all threats and controls affecting Activity Y in combination with the schedule risk it inherits from Activity X.

To this point in the document, we have discussed the importance of the following issues in establishing an accurate operational risk profile:

- considering threats from the five categories presented in the previous section during risk identification and analysis, which ensures that a broad range of risk sources is factored into the analysis
- viewing operational risk as a dynamic entity, which examines how risk changes as it propagates throughout a work process

To establish accurate operational risk profiles in distributed work processes, there is one final issue to consider. A risk analysis must also account for the operational risk caused by the emergent properties of distributed processes.

5.5 Operational Risk and Emergent Properties

An emergent property is a characteristic of a system that is derived from the interaction of its parts and that is not observable or inherent in the parts when considered separately. Some threats arise from the emergent properties of a distributed process. These particular threats, called emergent threats, are particularly problematic because they are not easily observed from the vantage points of participating organizations. As a result, the risk triggered by emergent threats typically is neither identified nor effectively managed.

For example, assume that you are asked to perform a risk assessment on a distributed process. As part of the assessment, suppose you want to determine if the local mission of each sub-process (i.e., the part of the work process managed by a particular organization) supports the overall work-process mission. Having proper alignment among all missions (i.e., all local missions and the overall mission) is important because it means that objectives throughout the work process are synchronized. Otherwise, execution of activities in different parts of the process will not be adequately coordinated, which can affect process performance and the prospect for successfully completing the overall mission.

As you conduct the assessment, you talk to representatives from each organization about a variety of topics, including how they view their particular missions. Suppose you find remarkable consistency in how people within each organization view their mission, which indicates that each organization’s management chain has done an exceptional job of communicating its view of local goals and objectives. You have identified a control for the process because establishing a common view of local goals and objectives among staff members is a circumstance that facilitates correct and complete execution of related tasks and activities.

However, you might also notice that while people *within* each organization have a common understanding of their local goals and objectives, there are problems in how local missions align with one another as well as how they align with the overall work-process mission. As a result, people throughout the process may actually be working at cross-purposes, which casts doubt on the prospects for successful completion of the overall mission. This is an example of a threat arising from an emergent property of a work process. Notice that this particular threat was not observable from the vantage point of any single organization. It became apparent only after looking at data from all organizations.

The emergent threat featured in the above example is a mission threat because it points to a serious flaw in the structure and alignment of the mission hierarchy for the work process. In fact, threats from all five threat categories can arise from the emergent properties of a work process. The characteristics of emergent threats are consistent with those from the five categories of threat; however, they are triggered by emergent, rather than local, conditions.

Because emergent threats arise from interactions among various parts of a process, managing the risk produced by them is difficult. In a distributed process, there is usually no centralized management authority. As a result, no one is in position to notice emergent threats, making it likely that the emergent threats will go unnoticed and that the resulting risk will go unmanaged. Even if people are aware of an emergent threat, they usually lack the management authority to do anything about it. In fact, since these threats cross organizational boundaries, no individual likely has sufficient authority to manage the resulting risks. A collaborative management effort is required in most cases, which is often difficult to achieve in practice.

5.6 A New Analysis Approach

Characterizing the operational risk in a distributed process is not a simple endeavor. The overwhelming majority of risk analysis techniques lack the sophistication necessary to gauge mission assurance in distributed processes. In particular, these techniques do not

- track inherited and imposed risk

- effectively characterize risk arising from the interrelationships and dependencies among threats and controls
- account for the operational risk arising from the emergent properties of distributed processes
- estimate the mission's operational risk exposure

With the amount of collaboration and outsourcing in today's business environment, distributed processes are commonplace. Managers are not armed with sufficient tools for characterizing operational risk in these complex environments, which puts them at a distinct disadvantage when doing battle with operational risk. To level the playing field, new approaches for analyzing operational risk are needed. In the next section, we present an advanced approach for analyzing operational risk that is capable of handling the complexity inherent in distributed processes.

6 Mission Assurance Analysis Protocol (MAAP)

Because conventional techniques proved to be inadequate for analyzing operational risk in complex processes, we were forced to create a new approach. Our development effort produced MAAP, which is specifically designed to analyze operational risk in distributed work processes. Although MAAP was specifically designed with distributed processes in mind, it can also be used to analyze the effects of operational risk on simpler workflows. This section captures the preliminary results of our work and presents the fundamental concepts behind MAAP.

6.1 Setting the Scope of a Risk Analysis

The first step in any risk analysis is explicitly defining what is considered to be within the scope of the analysis as well as what is beyond its scope. This step is crucial because it defines the breadth and depth of the analysis. The scopes of most conventional risk analysis techniques are framed around logical or physical entities, such as projects, groups, organizations, enterprises, technologies, assets, or sites. The corresponding analysis examines ways in which a particular entity might fail to achieve its mission. Implicit in this approach is the assumption that a one-to-one mapping between an entity and its mission exists. However, this assumption does not hold in distributed processes, where, by definition, multiple entities must work together to achieve a single mission. Focusing the analysis on a single entity in a distributed process can lead to local optimization of risk mitigation activities in lieu of global risk reduction. It also makes it difficult to account for emergent threats and to track inherited and imposed risk.

There is a second drawback to defining the scope of an analysis using a logical or physical entity. In today's business environment, any given entity is likely to be part of multiple missions. For example, many project teams support multiple missions at any given time, each with different objectives and deliverables. The assumption of a one-to-one mapping between an entity and its mission is a simplification that has considerable ramifications on the results of a risk analysis.

Assuming such a linear point of view makes it difficult, if not impossible, to examine the effects of competing and conflicting missions because each mission and its relationship to the entity has not been explicitly established. The resulting threat is not factored into the analysis, leading to an incomplete operational risk profile. In addition, the baseline for measuring risk is ambiguous because multiple missions are in play and none has been established as a benchmark for measuring risk. Lacking a definitive yardstick against which operational risk can be measured, conventional risk analysis techniques will likely produce unclear, ambiguous, or inconsistent results.

An alternative means of setting the scope of a risk analysis is required when examining operational risk in distributed environments. You can no longer assume that a unique relationship exists between an entity and its mission. Rather, you must accept the following realities of modern business environments:

- Many entities can work together to achieve a single mission. (This is a many-to-one mapping between entity and mission.)
- Any given entity can support multiple missions at any given time. (This is a one-to-many mapping between entity and mission.)
- Many entities can work together to achieve a given mission *and* each of those entities can also support multiple missions at any given time. (This is a many-to-many mapping between entity and mission.)

Recall that operational risk is the potential failure to achieve mission objectives. Notice that mission is featured prominently in this definition, highlighting its importance as the focal point of operational risk. Following this line of reasoning, it makes sense to frame the risk analysis around the mission, providing an unambiguous anchor for the subsequent analysis. By using the mission to set the scope for analysis, you are defining the explicit benchmark against which operational risk will be measured. Ideally, all entities instrumental in achieving the mission should be included in the risk analysis, thus enabling you to establish the role of each entity in relation to the mission. If a given entity cannot be included in the analysis, you must view it as a source of inherited risk to those parts of the work process that are being analyzed.

Using the mission to drive risk analysis is effective in distributed environments because it

- prevents local optimization of risk mitigation activities by including multiple entities in the analysis
- accounts for emergent threats and tracks inherited and imposed risk
- enables analysis of the risk produced by competing and conflicting missions
- leads to clear, unambiguous, and consistent results by anchoring all findings to the specified mission

MAAP uses the mission to frame a risk analysis, which is a key differentiator between it and conventional techniques. In this way, MAAP is designed to sort through the complexity inherent in distributed environments and ultimately produce a more accurate operational risk profile.

6.2 What Is MAAP?

MAAP is a protocol, or heuristic, for determining the degree of mission assurance in complex processes, and it provides a structured approach for analyzing operational risk. Notice that we classify MAAP as a protocol, not as a methodology. A protocol, as used in this context, is a set of conventions that guide how an activity should be performed, but it allows great flexibility regarding how to actually conduct the activity. By contrast, a methodology is a structured organization of tasks and procedures that define specific steps for completing an activity. MAAP defines an approach for analyzing operational risk in complex environments but does not prescribe specific steps for conducting the analysis. We have intentionally made MAAP implementation independent to encourage the application of known and proven techniques (e.g., failure modes and effects analysis) within MAAP's comprehensive framework.

6.3 Operational Risk Profile

One of the key products generated when following MAAP is an operational risk profile of the mission, which essentially provides a snapshot of how operational risk can affect a given mission. It is developed by analyzing process performance in a variety of operational situations, including

- normal, or expected, operational conditions
- unpredictable circumstances, or occurrences, triggered by events

Figure 15 illustrates the notion of examining performance over a range of different circumstances, or operational states. State 1 represents process performance during normal, or expected, operational conditions, while States 2 and 3 depict performance characteristics in the presence of unpredictable events.

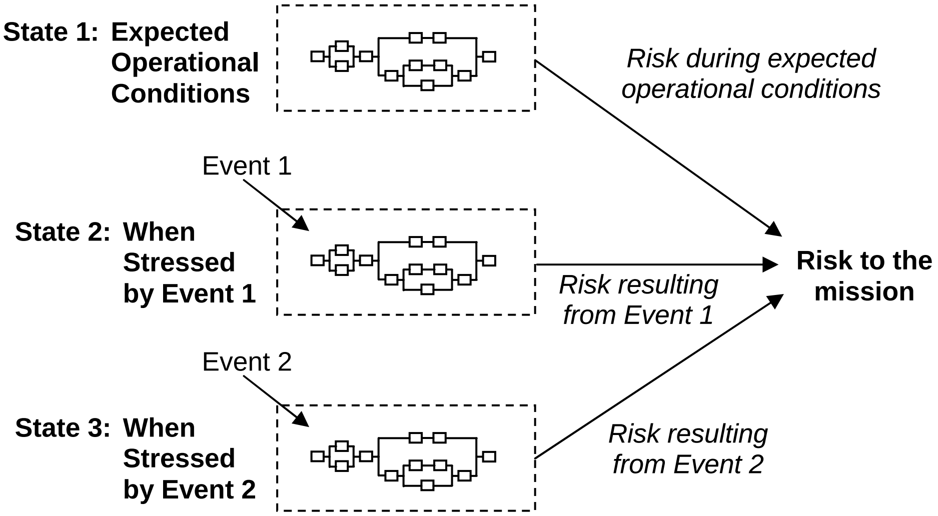
State 1: Expected Operational Conditions
Risk during expected operational conditions
Event 1
State 2: When Stressed by Event 1
Risk to the mission
Risk resulting from Event 1
Event 2
State 3: When Stressed by Event 2
Risk resulting from Event 2

Figure 15: Analyzing Risk in a Variety of Operational States

Notice that all three states contribute to the amount of operational risk affecting the mission, but each state produces its effects under a different set of circumstances. Operational risks arising during normal, or expected, operational conditions are triggered by threats inherent to work processes, and, as such, they are classified as intrinsic risks. By contrast, the risks triggered by unpredictable events are examples of extrinsic risks, which provide insight into a process's adaptive, or resilient, properties.

An operational risk profile must depict the effects of both intrinsic and extrinsic risks to fully characterize the extent to which a mission is at risk. A complete profile must include the following three key components: (1) a risk causal chain, (2) a measure of the mission's operational risk exposure, and (3) the key risk drivers. We briefly examine each component, beginning with the risk causal chain.

6.3.1 Risk Causal Chain

Figure 16 shows a risk causal chain for the work process depicted in Figure 15. A risk causal chain can be created using a cause-and-effect analysis, which is a technique commonly used in risk management and process improvement activities [Scholtes 94]. The chain provides a graphical view of operational risk by showing how threats, vulnerabilities, and controls combine to produce risk in each set of operational circumstances featured in Figure 15. Risk causal chains are important because they provide an interrelated view of operational risk and illustrate how a complex sequence of causes can place a mission at risk.

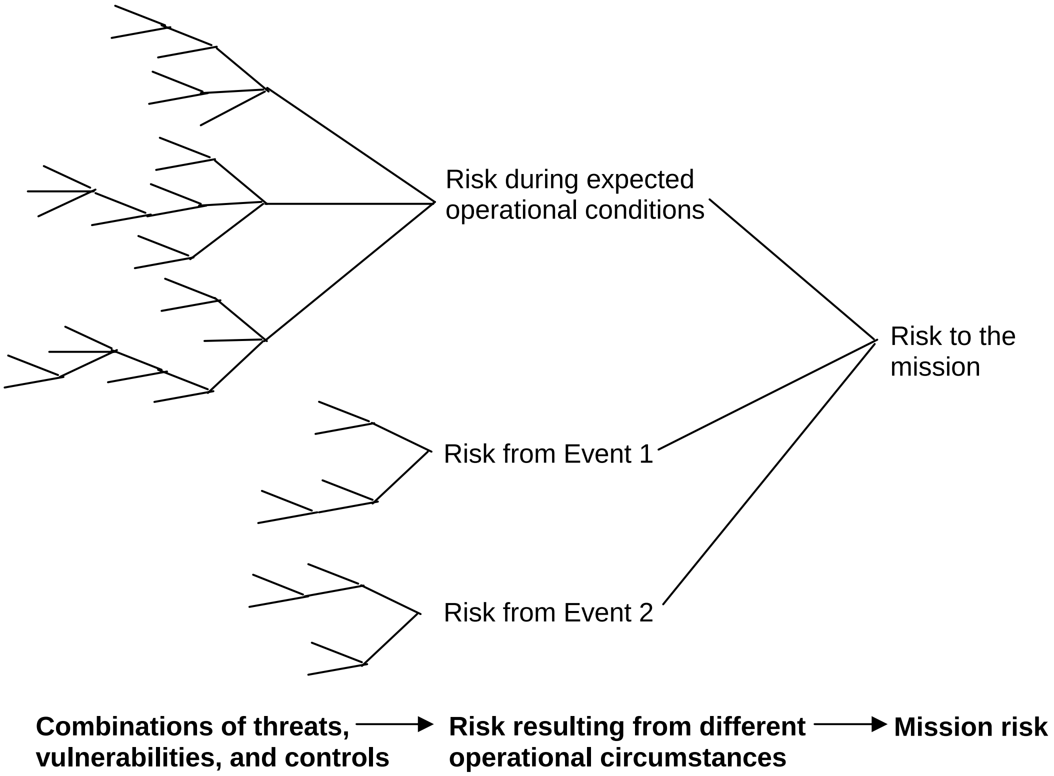
Risk during expected operational conditions
Risk to the mission
Risk from Event 1
Risk from Event 2
Combinations of threats, vulnerabilities, and controls
Risk resulting from different operational circumstances
Mission risk

Figure 16: Risk Causal Chain

6.3.2 Operational Risk Exposure

The second component of the operational risk profile is the value of the mission's operational risk exposure. This value provides a measure of the total, or aggregate, operational risk to which a mission is exposed, and it is a key indicator of mission success. Conventional risk analysis techniques do not provide a means of aggregating operational risk to the mission. In fact, our experience indicates that the data provided by most of these techniques are insufficient for estimating a mission's total operational risk exposure. As a result, managers lack the overall view of how much operational risk is actually affecting process performance, which makes it difficult, if not impossible, for them to optimize their investment in risk mitigation activities and to develop the degree of mission assurance they seek. By contrast, methodologies adhering to MAAP determine a mission's operational risk exposure, thus providing a means of gauging mission assurance.

Figure 17 illustrates the importance of establishing a mission's exposure to operational risk. By looking at the example illustrated in the figure, you will notice that the current value of risk exposure is rated as "very high," which management deems to be unacceptable. Based on the relative costs and benefits of various mitigation options, management then selects a mitigation strategy to lower its exposure. In this particular example, management's goal is to reduce its operational risk exposure to "low," which is the amount of operational risk it is willing to accept (i.e., its operational risk tolerance).

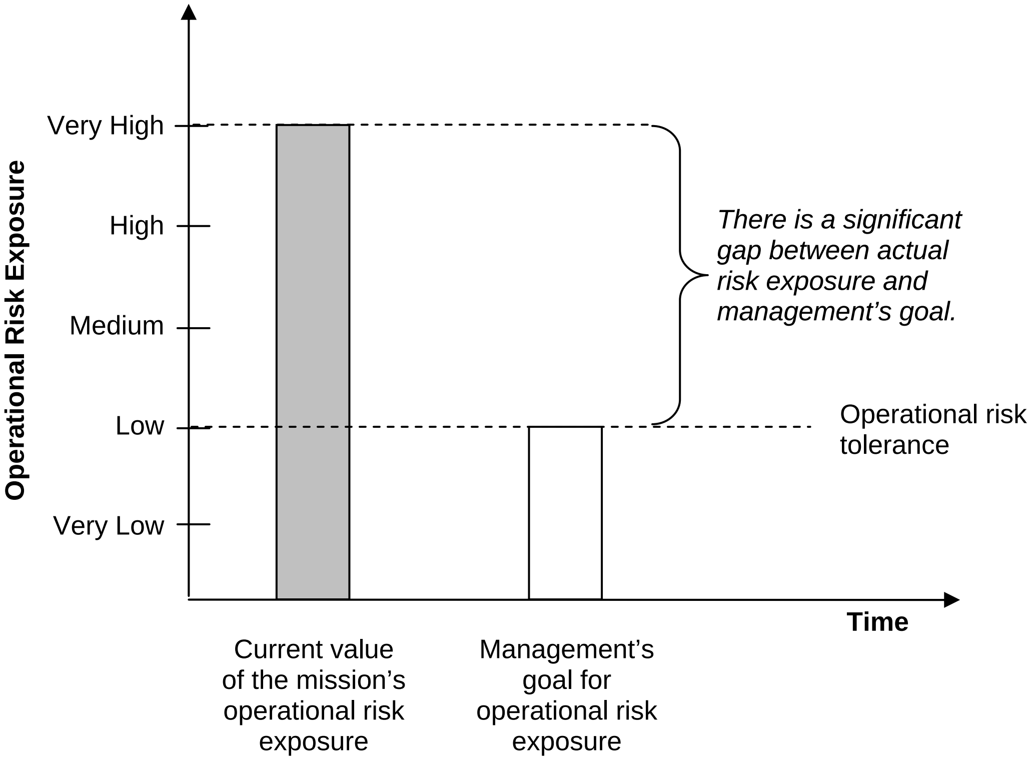

Figure 17: Bringing Operational Risk Within Tolerance

6.3.3 Risk Drivers

The final data needed to complete an operational risk profile are the key drivers of operational risk, which are identified using a critical path analysis. Risk drivers are the sources of risk having the strongest influence on the overall risk to the mission. Figure 18 illustrates drivers for the causal chain depicted in Figure 16. The bold lines in the figure highlight the main drivers of operational risk for this particular chain. Notice that the drivers form multiple critical paths throughout the causal chain and provide a natural starting point when developing risk mitigation strategies.

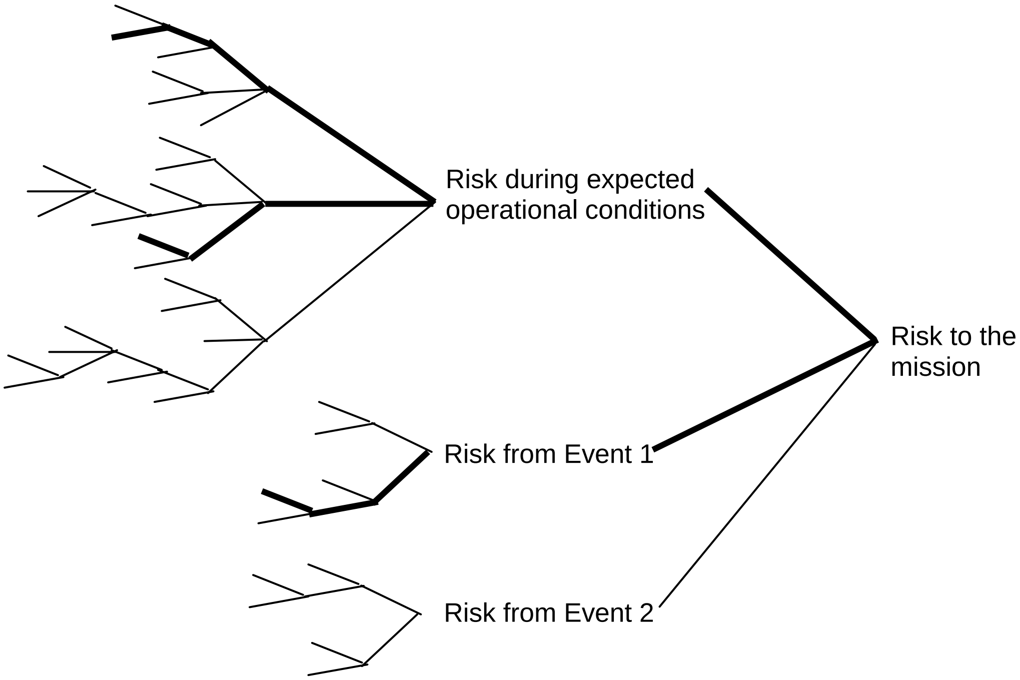

Figure 18: Key Risk Drivers

The operational risk profile is designed to provide information on a number of levels. Managers are presented with a measure of their mission's operational risk exposure, which provides insight into the effectiveness of the underlying work process. At the same time, staff members are provided with a detailed risk causal chain, including which causes are driving the overall risk to the mission. This detailed information is useful when forming mitigation strategies to reduce operational risk and improve mission assurance.

6.4 Protocol Fundamentals

MAAP thus defines a protocol for analyzing operational risk in work processes. Here, we provide our current thinking about MAAP and summarize the basic, fundamental principles underlying the protocol. The following seven guidelines collectively form the foundation of MAAP:

1. Determine mission objectives.
2. Characterize all operations conducted in pursuit of the mission.
3. Define risk evaluation criteria in relation to the mission objectives.
4. Identify potential failure modes.

5. Perform a root cause analysis for each failure mode.
6. Develop an operational risk profile of the mission.
7. Ensure that operational risk is within tolerance.

The remainder of this section describes each guideline in detail, beginning with determining mission objectives.

1. Determine mission objectives.

Goal To set the scope of the risk analysis

Description In MAAP, the mission of a work process is used to define the boundaries of the risk analysis. All activities performed in pursuit of the mission are included in the analysis, no matter where they are performed. In this way, identifying and documenting the mission sets the boundaries, or limits, of the resulting analysis.

Rationale Determining the mission objectives is important for setting the scope of the analysis (i.e., defining what will be included in the analysis as well as what will be excluded from consideration). In addition to setting the scope of the analysis, the mission also establishes the basis for measuring risk. All potential losses are examined in relation to the mission objectives during the risk analysis.

Outcome A set of documented mission objectives that set the scope of the risk analysis

2. Characterize all operations conducted in pursuit of the mission.

Goal To characterize the operational performance characteristics of a process

Description Once mission objectives are identified, all operations performed in pursuit of those objectives must be characterized to provide a benchmark of operational performance. At a minimum, you must define the following performance parameters for the process being analyzed:

- the sequence and timing of all activities needed to achieve the mission objectives, including all relevant interrelationships and dependencies among the activities
- roles and responsibilities for completing each activity
- the key objectives of each activity (i.e., the local mission of each activity)
- the relative strengths and weaknesses of each activity
- the acceptable range of normal, or expected, operating conditions for the process, including expected workflow capacity and parameters of technological performance
- known history of operational problems

The above parameters in combination with the mission objectives define an operational model for a process.

Rationale An accurate model of operational performance characteristics is essential when characterizing operational risk. It is used to illustrate where actual performance deviates from the desired or expected performance, thus providing the basis for risk identification.

Outcome An operational model of the work process being analyzed

3. Define risk evaluation criteria in relation to the mission objectives.

Goal To define one explicit standard against which operational risk can be uniformly measured

Description All potential losses in a risk analysis are measured in relation to mission objectives. Risk evaluation criteria define the parameters for estimating the values of impact and probability. However, the individual values of impact and probability do not directly provide a measure of operational risk. A separate measure, called risk exposure, is needed to reflect the amount of operational risk affecting each mission objective. Risk exposure combines the values of impact and probability to produce a single measure of risk. To determine risk exposure, you must establish specific criteria for combining individual measures of probability and impact. The same set of risk evaluation criteria must be uniformly applied to all operations related to the process.

Rationale Risk evaluation criteria are important because they provide a common benchmark against which operational risk is measured. Having a single set of criteria for all operations is an essential part of establishing a uniform operational risk tolerance in a distributed process.

Outcome A documented set of criteria used to measure impact, probability, and risk exposure

4. Identify potential failure modes.

Goal To identify the ways in which a process can fail to meet its specified performance characteristics

Description All relevant failure modes for a process are identified by analyzing performance as defined by its operational model. As used in this context, a failure mode is any situation where the process does not meet its specified performance parameters. It typically occurs when actual performance deviates from the desired or expected performance, which, in turn, can affect the ability to achieve either a local objective or one of the mission objectives. During the analysis, failure modes are identified for

- normal, or expected, operational conditions
- unpredictable circumstances, or occurrences, triggered by events

This two-pronged approach examines process performance for various operational situations, which is essential when establishing mission assurance.

Rationale Identifying potential failure modes establishes the types of impacts that can be expected during operations and provides critical information needed when identifying operational risks.

Outcome A documented list of all failure modes for a work process

5. Perform a root cause analysis of each failure mode.

Goal To identify specific risks that can result in process failures

Description A root cause analysis of each failure mode must be performed to determine the specific circumstances that trigger it. A broad range of factors must be considered in the root cause analysis, including applicable threats from the five categories, emergent threats, and inherited risks. A root cause analysis is a common technique for identifying the conditions that lead to an undesired state, such as a failure mode. This type of analysis is especially useful when identifying complex risks because it illustrates how vulnerabilities, threats, and controls combine to produce a single failure mode. It essentially produces a causal chain of risk factors that can produce a given failure mode and adversely affect process performance. When viewed together, a failure mode and the conditions that trigger it define a specific instance of operational risk.

Rationale Performing a root cause analysis is important for establishing the *combination* of vulnerabilities, threats, and controls that can produce a specific failure mode. This analysis is essential for capturing complex interrelationships and dependencies among the conditions that lead to each specific occurrence of operational risk.

Outcome A set of operational risks

6. Develop an operational risk profile of the mission.

Goal To develop a comprehensive view that accurately reflects how operational risk can affect the mission

Description Developing an operational risk profile for the mission requires three additional analysis activities. First, risks are linked in a prescribed manner, producing an aggregate view of the operational risk to the mission. In essence, a single causal chain of risk factors affecting the mission is developed. Second, the value of operational risk exposure for the mission is determined using the defined risk evaluation criteria and all relevant data collected throughout the analysis. Finally, a critical path analysis of the risk causal chain is performed to identify which factors are driving the operational risk exposure to the mission. Overall, an operational risk profile must

- track inherited and imposed risk
- effectively characterize risk arising from the interrelationships and dependencies among threats and controls
- account for the operational risk arising from the emergent properties of distributed processes
- estimate the mission’s operational risk exposure

Rationale Before substantial mitigation activities can be initiated to improve the mission assurance of a process, it is essential to develop an operational risk profile of the mission. The profile forms the basis for all operational risk management activities that follow.

Outcome An operational risk profile of the mission

7. Ensure that operational risk is within tolerance.

Goal To develop a mitigation plan for ensuring that operational risk is within tolerance

Description The value of operational risk exposure for the mission has been established. Now, management must decide whether that value is acceptable. A tradeoff analysis is performed to weigh the relative costs associated with various mitigation options against the potential for reducing the aggregate operational risk. The operational risk profile provides a basis for the tradeoff analysis, where residual risk is examined under several mitigation scenarios. The best available option is selected based on the relative costs and benefits of each scenario. The value of residual risk projected for the chosen option defines management's tolerance for operational risk.

Rationale Organizational constraints always limit the amount of mitigation resources that can be applied in any given situation. Weighing the relative costs and benefits associated with mitigation options is essential for ensuring that risk is brought within acceptable limits and maintained at that level over time, giving management reasonable confidence in mission success.

Outcome A documented mitigation plan

In limited testing, MAAP has proven useful for assessing mission assurance in distributed work processes. It provides a comprehensive view of a mission's operational risk profile and effectively conveys the underlying work process's current performance characteristics and forms a basis for improvement. We plan to continue to develop and refine the heuristic and hope to eventually use it in a wide variety of operational environments.

7 Applications and Future Directions

Rather than designing MAAP to analyze risk in a specific type of work process, such as a software development process or an operational security process, we chose to develop a general risk analysis approach that is applicable across a wide variety of processes. In this way, one risk analysis technique could be applied in numerous operational settings, obviating the need for multiple specialized assessment techniques. Figure 19 illustrates the notion that MAAP provides a foundation for analyzing risk in a variety of domains.

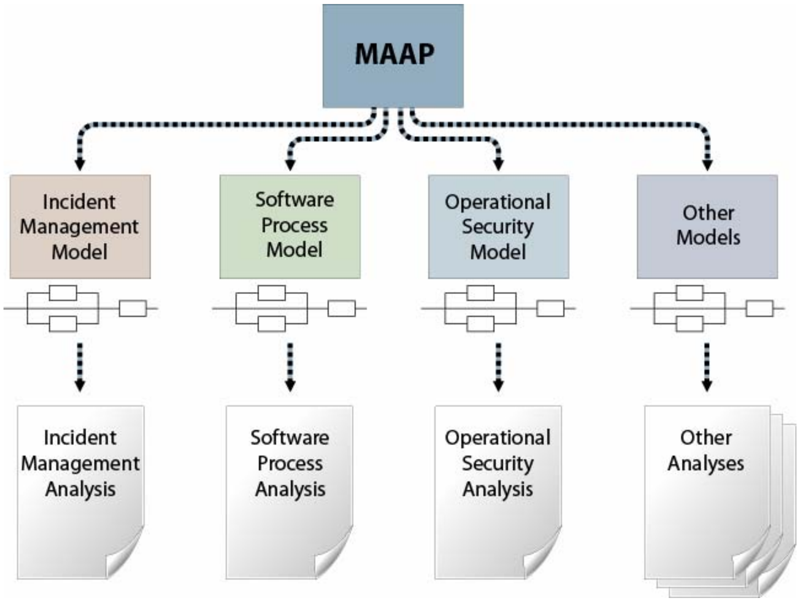
MAAP
Incident Management Model
Software Process Model
Operational Security Model
Other Models
Incident Management Analysis
Software Process Analysis
Operational Security Analysis
Other Analyses

Figure 19: General Risk Analysis Approach

We have endeavored to stay true to our goal of designing a general approach for analyzing operational risk in complex work processes. This goal forced us to rethink many of our assumptions regarding risk management as we developed MAAP and the tools required to implement it. The end result is a flexible technique with potential applicability in many disciplines.

When developing tools and techniques to implement MAAP, we decided to build upon the existing state of the practice. We used common techniques (e.g., root cause analysis) when possible and developed custom techniques (e.g., approach for evaluating mission assurance) only when needed. To determine the extent to which we have achieved our original goal, we intend to test MAAP in as many diverse environments as possible. To date, we have just started testing MAAP and have just completed our first pilot.

7.1 Analyzing Operational Risk in a Distributed Incident-Management Process

After identifying several candidate work processes, we selected a security process, incident management, to provide the first test of MAAP. Incident management is a process for preventing, detecting, and responding to cyber-security events and incidents [Alberts 04]. We selected it 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 operational risk in a distributed process.

We used the MAAP tool suite to assess operational 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. The MAAP results provided the managers with a clear indication of their incident-management mission's exposure to operational risk, which provided a snapshot of the effectiveness of the underlying work process. We were able to provide the managers with useful information without providing unnecessary details. In addition, staff members were appreciative of the details, which were quite useful in forming mitigation strategies to reduce operational risk and improve mission assurance.

By following MAAP, we were able to illustrate how inherited and imposed risk affected process performance. We also identified several emergent threats and characterized their contributions to the mission's operational risk exposure. In fact, emergent threats were the biggest drivers of operational risk in this particular assessment. Overall, we were able to provide government managers with a roadmap for improvement using the comprehensive operational risk profile produced by MAAP.

7.2 Applying MAAP to Software Development Processes

We are currently using the MAAP tool suite to help assess a distributed software development program's potential for mission success. This pilot is important because it will provide insight into how well MAAP works in a very different domain. However, because of the limited nature of this work, additional pilots must be conducted before we can fully establish MAAP's applicability to the software development domain.

7.3 Analyzing Distributed Technologies Using MAAP

We are also interested in exploring how MAAP can be used to analyze distributed technologies. Because management control of networked technologies is shared among many organizations, many issues inherent in these technologies mirror those in distributed work processes. For example, they are vulnerable to the effects of inherited and imposed risk and emergent threats, which are situations that conventional risk analysis techniques are not designed to handle.

In addition, most conventional techniques for analyzing technological risk are designed to assess a single piece of technology at any given time. This approach is problematic when applied to a distributed environment, where, by definition, multiple technologies must work together to achieve a single mission. Focusing the analysis on a specific technology could easily lead to local optimization of risk mitigation activities in lieu of global risk reduction. Likewise, any given technology is likely to support multiple missions, which makes it difficult to understand the effects of competing and conflicting missions and creates ambiguity about which mission defines the benchmark for measuring risk. As a result, focusing a risk analysis on one technology at a time could produce unclear, ambiguous, inconsistent, or incomplete results. The parallels with distributed work processes are noteworthy.

The commonalities between analyzing operational risk in distributed work processes and distributed technologies suggest that they might actually be part of a larger problem space: analyzing operational risk in distributed *systems*. As used in this context, the word *system* refers to a group of interacting, interrelated, or interdependent elements that function together as a whole to accomplish a goal. As such, both work processes and technologies are examples of specific types of systems. In our future work, we intend to explore the potential for extending MAAP to cover a wider range of distributed systems.

7.4 MAAP and Risk Management

Our work with MAAP also provides insight into the topic of *managing* operational risk in distributed environments. Organizations working collaboratively toward a single mission are normally bound by contracts, not organizational lines of authority. Managers with ultimate responsibility for overseeing mission completion typically oversee the contractual obligations of each participating organization and ensure that all commitments are met as specified in applicable legal agreements. However, those managers normally do not have end-to-end *management authority* over the underlying work process, restricting their options for managing operational risk. For example, resources cannot easily be reallocated across organizational boundaries because such actions likely violate the contracts that are in place. In this environment, traditional risk management practices may be ineffective and impractical. New practices are needed to manage risk in distributed operational environments, highlighting an obvious extension to our current research.

7.5 Future Research Directions

This technical note describes our initial work in the area of mission assurance. While this research has provided many tangible results, we also believe there are many additional research avenues to explore as we move forward. First and foremost, we intend to continue to refine MAAP and pilot it in different venues. Candidate areas for future applications include

- software assurance
- operational security
- supply chain management
- any complex mission requiring a comprehensive risk analysis

In support of our present scope of work, we anticipate refining and documenting the current suite of tools used to implement the protocol. In addition, we intend to explore the possibility of applying MAAP to assess risk in distributed technologies, thus extending the scope of our current research efforts. Finally, we would like to move beyond focusing exclusively on analyzing operational risk in distributed environments by defining a practice for managing operational risk in these settings. In essence, we view the work documented in this report as a starting point for extending the discipline of risk management rather than as a completed body of research.

References

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

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

[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). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu/publications/documents /04.reports/04tr015.html.

[BIS 04] Bank for International Settlements (BIS). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. BIS, 2004. http://www.bis.org/publ/bcbs107.pdf.

[Carr 93] Carr, M., Konda, S., Monarch. I., & Ulrich, C. *Taxonomy-Based Risk Identification* (CMU/SEI-93-TR-006, ADA266992). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1993. http://www.sei.cmu.edu/publications/documents/93.reports /93tr006.html.

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

[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.

[Haimes 04] Haimes, Yacov Y. *Risk Modeling, Assessment, and Management*. New York, NY: John Wiley & Sons, Inc., 2004.

[ISACA 00] Information Systems Audit and Control Association (ISACA). *COBIT® 3rd Edition: Executive Summary*. ISACA, 2000. http://www.isaca.org/cobit.

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

[Scholtes 94] Scholtes, Peter R. *The Team Handbook: How to Use Teams to Improve Quality*. Madison, WI: Joiner Associates, Inc., 1994.

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

[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
(Leave Blank)

2. REPORT DATE
September 2005

3. REPORT TYPE AND DATES COVERED
Final

4. TITLE AND SUBTITLE
Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments

5. FUNDING NUMBERS
FA8721-05-C-0003

6. AUTHOR(S)
Christopher J. Alberts, Audrey J. Dorofee

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2005-TN-032

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

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

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

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

The global business environment continues to grow in complexity. The typical business process is no longer under a single point of management control. Instead, it has become common for management of a work process to be shared among multiple groups. The permanent enterprise, defined by an organizational chart, has been replaced by the virtual enterprise, defined by the mission being pursued. Activities today are rarely supported by dedicated, stand-alone technologies. Rather, interoperable, networked technologies form the backbone of our information infrastructures. Today, managers must deal with interrelationships and dependencies among technologies, data, tasks, activities, processes, and people that were unimaginable just a few short years ago. Unfortunately, conventional risk analysis techniques have proven inadequate for characterizing risk in today's complex operational environments, so it was necessary to develop new and innovative approaches. The Mission Assurance Analysis Protocol (MAAP) defines an advanced, systematic approach for analyzing operational risk and gauging mission assurance in complex work processes. This report presents the concepts and underlying theories behind the MAAP, highlights results from early piloting of the technique, and outlines future research directions.

14. SUBJECT TERMS
distributed work processes, operational risk, Mission Assurance Analysis Protocol, MAAP, risk analysis

15. NUMBER OF PAGES
59

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UL