Software Engineering Institute

Risk Management Considerations for Interoperable Acquisition

B. Craig Meyers

August 2006

TECHNICAL NOTE
CMU/SEI-2006-TN-032

Toward Interoperable Acquisition, an Independent Research and Development Project

Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

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

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

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

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

Table of Contents

List of Figures

List of Tables

Acknowledgements

This work was supported by the Independent Research and Development project called *Toward Interoperable Acquisition*. We acknowledge discussions with our colleagues Christopher Alberts, Eileen Forrester, and Carol Sledge. We also acknowledge discussions with Tricia Oberndorf.

Abstract

This report addresses interoperable risk management: the interoperability of organizations that engage in risk management in the context of a system of systems. The state of risk management practice—the specification of standards and the methodologies to implement them—is addressed and examined with respect to the needs of system-of-systems interoperability. The current practice is found to be insufficient to achieve interoperability with regard to risk management. A number of research questions are raised to associate this topic with the needs of the larger context of interoperable acquisition.

1 Introduction

There is an increased emphasis on providing system-of-systems capabilities instead of those for a particular system. When one considers the larger system-of-systems view, interoperability assumes a position of paramount importance. Traditionally, interoperability has been considered in the context of a system's operation. Recent work by the Carnegie Mellon®[1] Software Engineering Institute (SEI) has broadened the concept of interoperability to include other system aspects, notably those related to the management and construction of systems [Morris 04].

This technical note addresses the topic of interoperable acquisition for the case of risk management. We introduce the following definition:

> **interoperable acquisition:** the set of practices that enable acquisition, development, and operational organizations to collaborate more effectively to field interoperable systems. These practices are achieved through sharing relevant information and performing necessary activities that enable the collective behavior of these organizations to successfully deliver systems-of-systems capabilities.

An overview discussion of the challenges of interoperable acquisition is presented in *Interoperable Acquisition for Systems of Systems: The Challenges*. That technical note outlines the critical aspects of systems of systems and interoperability that affect the acquisition, deployment, sustainment, and operational use of systems of systems [Smith 06].[2]

One aspect of interoperability involves interoperation between entities that are responsible for program management. This particular aspect is called *programmatic interoperability*. Of special concern to this area is the concept of *interoperable risk management* where multiple organizations must interoperate with regard to risk management. The purpose of this report is to examine interoperable acquisition through the lens of risk management.

This report is organized as follows:

- Section 2 provides some background on interoperable acquisition.
- Section 3 gives a brief overview of risk management, including the rationale for its consideration in this work.
- Section 4 discusses some limitations of the current approach to risk management.
- Section 5 identifies some research topics arising from this work.
- Section 6 contains a brief summary of the report.

---

1. Carnegie Mellon is registered in the U.s. Patent and Trademark Office by Carnegie Mellon University.

2. In addition to this technical note on risk management and *Interoperable Acquisition for Systems of Systems: The Challenges* (CMU/SEI-2006-TN-034), there are two other technical notes resulting from an independent research and development (IR&D) project supported by the SEI. The other technical notes describe process (CMU-SEI-2006-TN-033) and schedule (CMU/SEI-2006-TN-035) considerations for interoperable acquisition. A fifth technical note, partially supported by the IR&D effort, will deal with programmatic interoperability issues.

2 Background

2.1 INTEROPERABLE ACQUISITION

In Section 1, we introduced the concept of interoperable acquisition. The purpose of interoperable acquisition is to more effectively allow organizations to share information and perform activities that may affect their collective behavior toward achieving interoperability. It is generally agreed that the current acquisition process is focused on a particular acquisition program, leading to the well-known stovepipe approach to acquisition. Systems of systems, with network-centric character, are dramatically different from traditional systems. Interoperable acquisition seeks to broaden the scope, role, and interaction of participants who engage in the acquisition process. Simply stated, interoperable acquisition is about achieving interoperability in the acquisition process.

In exploring interoperable acquisition, we draw a distinction between acquisition in a system-of-systems environment and acquisition of a system of systems. We use terms consistent with the meaning of acquisition in a system-of-systems environment—that some acquisition is responsible for producing a system that will form part of a system of systems. We do not use phrasing such as acquisition of a system of systems that could be construed to imply acquisition of a system of systems treated as a single unit.

The term interoperability has been used primarily with respect to operational systems. In the literature, one finds many examples where the term interoperability is used, almost entirely restricted to the operational systems domain. One theme that runs through the current definitions is *the ability of systems to work together*. This notion has led to an emphasis on a syntactic view of interoperability ("bits on a wire"), although semantic considerations are quite relevant ("what do the bits mean?").

However, we believe a more general approach to interoperability is warranted. Treating interoperability only in the context of an operational system limits its potential application and benefit. Interoperability is about the communicating entities, the information they share, and the operations that are performed based on that information. Toward this end, we offer a more general definition:

> **interoperability:** the ability of a set of communicating entities to (1) exchange specified information and (2) operate on that information according to a specified, agreed-upon, operational semantics.

Although it applies to the context of operational systems, the above definition is intended to encompass a broader scope of interoperability in systems of systems. This perspective is shown in Figure 1, a view that was developed in earlier work ([Levine 03], [Morris 04], [Meyers 05]) and leads to the consideration of **programmatic interoperability** and **constructive interoperability**, in addition to operational interoperability. We suggest that acquisition can be addressed in terms of functional domains in the management, construction, or operation of a system.

The terms programmatic interoperability, constructive interoperability, and operational interoperability represent interoperability between different domains that compose an acquisition. In particular, these domains are characterized by

- the entities (Program 1, Program 2, and so forth) that need to communicate
- the data they share
- the operations that are performed

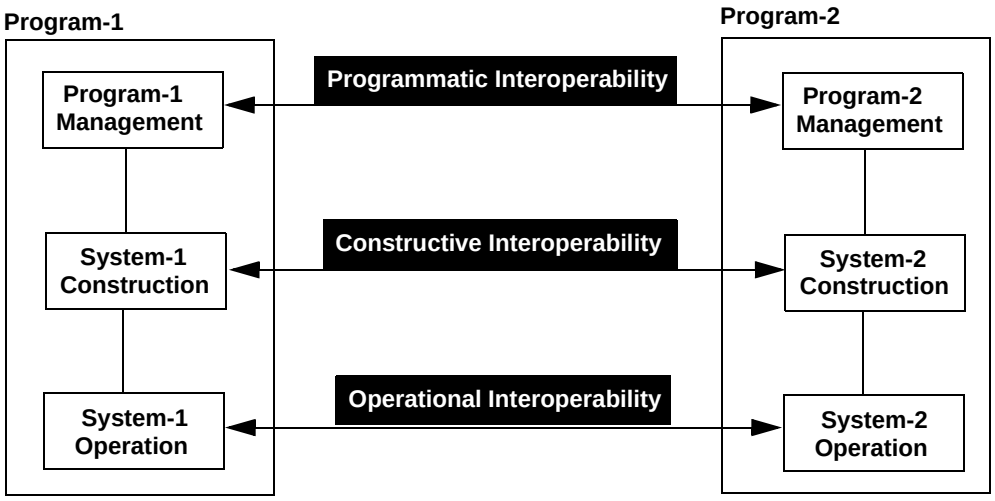

Figure 1: System-of-Systems Interoperability (SOSI) Model

There can also be interactions among the various domains as well. An example of this would be interaction between functions related to program management and system construction. Such interactions are in the vertical dimension in Figure 1.

A diagram such as Figure 1 can be easily interpreted in an overly simplistic manner. We caution against such oversimplification. While it might be a shorthand to interpret programmatic interoperability as interoperability among only program management organizations, such an interpretation is overly simplistic and incorrect. In fact, we define programmatic interoperability as:

> **programmatic interoperability**: interoperability among functions appropriate to the management domain, *independent of the organization that performs those functions.*

This definition suggests that programmatic interoperability may involve the program management office as well as others engaged in the management of a component in a system-of-systems context—such as users, contractors, suppliers, and so on. Occasionally, there is a partitioning of activities among the participants in programmatic interoperability; for example, contracting decisions are made by a limited number of organizations.

Given the preceding examination, it is relevant to discuss key influences that affect the acquisition process. Although there may be many such factors, our focus here is on those factors that closely relate to considerations regarding the basic elements of interoperability—namely, communicating entities, information shared and semantics

of operations on that information. The following discussion is couched at a higher level; we will examine these issues in more detail later in this report.

2.1.1 Scope of Interaction

Interoperability in the acquisition process is influenced by the scope of interaction among organizations that participate in the process. We consider the basic models shown in Figure 2.

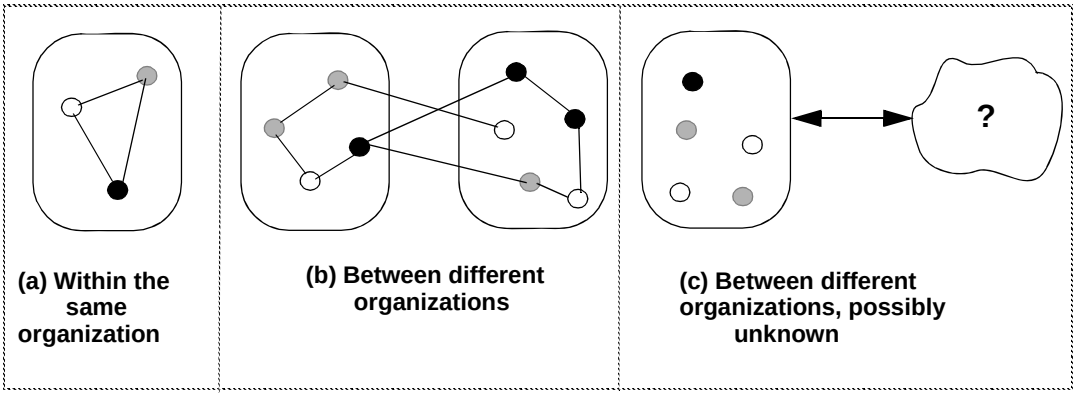

Figure 2: Models of the Scope of Interaction

The different cases are described as follows:

- Case (a) represents the interoperability that is within the context of a particular organization. In general, this is the easiest case since it is within the context of one organization.
- By contrast, in Case (b) the interoperability is between different organizations. It is assumed that the set of communicating entities is known. Dealing with different organizations brings in consideration of organizational policies and practices that might be in conflict.
- Case (c) is fundamentally different in that the identity of the other organizations may not be known. This case is analogous to an organization presenting information about risk management to others that may need such information—independently of any prior agreement about which organizations should be given that information.

The three cases can be seen as depicting two situations that are quite different. The first two cases are characteristic of a *bounded* environment, in that the communicating entities and their number are known (and assumed to be relatively stable over time). The last case is emblematic of an unbounded environment in which the identity and number of communicating entities is not known. That situation, an *unbounded* environment, is often found in network-centric operations and systems of systems.

2.1.2 Nature of Agreements

Interoperability in the acquisition process is influenced by the nature of agreements among organizations that participate in the process. Various types of agreements can be considered as part of achieving interoperability:

- contractual relationships
- memoranda of understanding
- implicit agreements (For example, if two organizations agree to conform to some standard, they have in effect entered into an agreement.)

In some sense, any type of agreement can be regarded as an influence relation. Different types of agreements are related to the character of an organization. Some aspects of the organization and its agreements are discussed in *System-of-Systems Navigator: An Approach for Managing System-of-Systems Interoperability* [Brownsword 06].

2.1.3 Shared Information

Interoperability in the acquisition process is influenced by the information that is shared. Fundamental to any discussion of interoperability is the information that is shared. Two overarching considerations are (1) what information needs to be shared and (2) who decides the information to be shared. There are interesting parallels to the factor concerned with the scope of interaction between communicating entities described in Section 2.1.1: what are the implications for the *data* that is shared in an unbounded environment, and can the determination of necessary information be made at runtime? Further, if that determination can be made at runtime, we have moved to a *dynamic* environment that is considerably more challenging—and interesting—than a static one in which the scope of information to be exchanged is bounded and known.

2.1.4 Operations

Interoperability in the acquisition process is influenced by the operations that are performed by the communicating entities. Where entities desire to interoperate, the operations performed are of ultimate concern because those operations represent the *behaviors* of the communicating entities. It is reasonable to ask:

- What behavior is expected, or required, of entities that participate in interoperable acquisition in a bounded or unbounded environment?
- Can those behaviors change over time?
- If behaviors can change, what are the implications of those changes?

2.2 INTEROPERABLE RISK MANAGEMENT

Stated simply, interoperable risk management is about interoperability with regard to the practice of risk management. Interoperable risk management is an element of interoperable acquisition, and we define it in this way:

> **interoperable risk management:** the subset of interoperable acquisition practices that enable acquisition, development, and operational organizations to identify, share, and mitigate risks that are inherent to a system of systems.

The purpose of interoperable risk management is to more effectively allow organizations to share information and perform necessary activities with regard to risk management that may affect their collective behavior. This perspective on sharing information and performing operations differs from that of a particular program. Here, the ability to share information about risk management is deemed necessary for some collection of entities to operate in a cooperative manner. The goal of interoperable risk management is to achieve a holistic perspective, encompassing the risk management practices of all entities in an interoperable acquisition rather than only those of any individual entity.

The principles introduced earlier—regarding communicating entities, information shared, and operations performed on that information—may be viewed in the context of risk management as follows:

- What are the communicating entities engaged in acquisition **with regard to risk management**? What is the nature of agreements among the entities?
- What is the **risk management information** that is needed to be shared?
- What are the operations (or behaviors) **related to risk management**?

The preceding questions focus the more general questions stated previously regarding interoperable acquisition on risk management. Before examining these and related questions, we will pause to consider some background on risk management.

3 Current Approach to Risk Management

3.1 RATIONALE

Risk management is a topic that is worthy of consideration and is used as an exemplar for this work for two reasons. First, risk management, when done well, is a powerful technique for minimizing problems and positioning a program for mission success. In today's business environment, it is common for multiple organizations to work collaboratively in pursuit of a single mission, which creates a degree of programmatic complexity that is very difficult to manage. Mission success in these complex programs requires a collaborative management approach that effectively coordinates the risk management activities of all participating groups. Interoperable risk management is thus a means of minimizing problems throughout a collaborative effort and positioning it for success.

Second, risk management is a complex organizational process where achieving interoperability can be challenging. In general, an effective risk management process must be integrated with and effectively provide support for an organization's overall business model and decision-making processes. As a result, each organization's implemented risk management process tends to be unique. Our field work has continually shown that risk management processes employed by organizations adhering to a common risk management standard are typically implemented in very different ways. In addition, many managers view their risk management processes as being proprietary and providing a competitive advantage over rival organizations. Thus, with respect to risk management, interoperability must be achieved in an environment where multiple processes are employed; in some cases, those processes are proprietary.

Together, then, the power and complexity of the risk management process make risk management a good exemplar for this study. In addition, risk management may be a means by which concerns related to interoperable acquisition are investigated because it is typical of other processes employed in acquisition. By studying risk management, we may develop insight into other processes that are also used in acquisition.

Despite the considerable amount of work on risk management, work on risk management continues to evolve—in some instances toward the aspect that interests us in this report. Some items of note include the following:

- There is ongoing work within the Institute of Electrical and Electronics Engineers (IEEE) to harmonize the standards for software (IEEE 12207) and system (IEEE 15288) life-cycle processes. A goal of this harmonization is to obtain interoperability between the two life-cycle views. One aspect common to these processes is that an existing standard for risk management (ISO/IEC 16085) is being generalized to apply to the systems level. The revised, generalized standard will add requirements and guidance for the risk management provisions of existing standards for software and system life cycles [Moore 06].

- There has been an effort underway to account for the integration of risk management across systems and enterprises and between enterprises. This work also addresses issues and opportunities in the same context as risks and the processes and tools needed to deal with risks across enterprises [Holzer 06]. In addition, there is ongoing work that considers risk management in extended enterprises and also addresses opportunities [Alberts 05].

3.2 CURRENT APPROACH

There is a large body of work related to the subject of risk management. As part of this effort we have examined a number of documents related to risk management. The documents include the following:

- *ISO/IEC Guide 73: Risk Management—Vocabulary—Guidelines for use in standards* [ISO 02]
- Australia/New Zealand *Risk Management Guidelines Handbook*[3] [ANZS 04]
- IEEE Standard 1540-2001: *IEEE Standard for Software Lifecycle Processes—Risk Management* [IEEE 01]
- *Risk Management Guide for DoD Acquisition* [DoD 00]
- *Continuous Risk Management Guidebook* [Dorofee 96]

This list represents the spectrum of international and national standards-body efforts, as well as community efforts representing accepted practices defined by the U.S. Department of Defense (DoD) and the SEI.[4] We refer to the above set of specifications as **base documents** for consideration of risk management. The amount of material in each of the documents varies, sometimes considerably. In general, the documents that also incorporate methods (such as the *Continuous Risk Management Guidebook* and the *Risk Management Guide for DoD Acquisition*) include more detailed information about the process.

There are other documents that provide guidance on process, such as *A Guide to the Project Management Body of Knowledge, Guidelines for Process Integration and Product Improvement*, and *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners* ([PMI 04], [Chrissis 03], [NASA 02]). Still other documents in the field of system engineering discuss risk management, including the *Systems Engineering Handbook* and *Systems Engineering Fundamentals* ([INCOSE 04], [DoD 01]). Incorporation of these and perhaps other documents into the set of base documents is an item of possible future work.

Risk management encompasses a number of concepts; we have examined the set of base documents to understand those concepts and summarized them in Table 1. These concepts relate to a particular risk, rather than to a process that might be used in risk management. As indicated, there is considerable similarity in terminology among the documents assessed.

---

3. This document is derived from the Australia/New Zealand National Standard 4360 (2004) that was fundamental in ISO standard [ISO 02]. Hence, treating National Standard 4360 separately would duplicate material from the ISO Standard.

4. Note that the *Risk Management Guide for DoD Acquisition* and the *Continuous Risk Management Guidebook* ([DoD 00], [Dorofee 96]) contain not only a specification of a standard but also a methodology to apply it.

Table 1: Concepts in Base Documents that are Associated with Risk Management

ISO/IEC Guide 73: Risk Management—Vocabulary—Guidelines for use in standards	Risk Management Guidelines Handbook	IEEE Standard for Software Lifecycle Processes—Risk Management	Risk Management Guide for DoD Acquisition	Continuous Risk Management Guidebook
• Consequence • Event • Probability • Risk • Risk criteria • Source	• Consequence • Event • Frequency • Hazard • Likelihood • Loss • Probability • Residual risk • Risk • Risk criteria • Stakeholders	• Acceptability • Consequence • Hazard • Likelihood • Probability • Project risk profile • Risk • Risk category • Risk exposure • Risk state • Risk threshold	• Assessment status • Category • Consequence • Date submitted • Description • Event • Identification number • Key parameters • Likelihood • Priority • Probability • Responsible individuals • Risk • Risk statement • Status • System/sub-system • Time sensitivity	• Classification • Condition • Consequence • Context • Exposure • Identifier • Impact • Measure • Priority • Probability • Risk • Risk statement • Time frame

Risk management is also described from a process perspective. The role of process in terms of acquisition is well known. We examined the set of base documents to understand the various processes that are referenced. A summary of the process terminology appears in Table 2.

The processes used in risk management are similar, as indicated in Table 2, in that they all have some form of identification, analysis, and treatment of risk. There are some differences, however. For example, one difference occurs in the way that the process itself is managed. Although a difference such as this is not specific to the subject of the risk management, it can have implications for how well the process is performed.

Table 2: Processes in the Base Documents that are Associated with Risk Management

ISO/IEC Guide 73: Risk Management—Vocabulary—Guidelines for use in standards	Risk Management Guidelines Handbook	IEEE Standard for Software Lifecycle Processes—Risk Management	Risk Management Guide for DoD Acquisition	Continuous Risk Management Guidebook
• Risk analysis • Risk evaluation • Risk treatment • Risk acceptance • Risk communication	• Communicate and consult • Establish the context • Risk identification • Risk analysis • Risk evaluation • Risk treatment • Monitoring and review • Recording the risk management process	• Plan and implement risk management • Manage the project risk profile • Perform risk analysis • Perform risk monitoring • Evaluate the risk management process	• Risk planning • Risk assessment • Risk handling • Risk monitoring	• Identify risks • Analyze risks • Plan • Track • Control • Communicate

An example of the risk management process identified by the IEEE is shown in Figure 3 [IEEE 01]. That process is developed from the perspective of risk management in the software life cycle. Another example of the risk management process is shown in Figure 4 [ANZS 04].

From our analysis of existing risk management documents, we see a high degree of similarity among the concepts and processes they specify. We believe this similarity reflects a convergence of various organizations toward adopting a standard practice of risk management. As we will see in Section 4, however, there are difficulties "beneath the surface" that limit the application of current practices to achieve interoperability in the context of risk management.

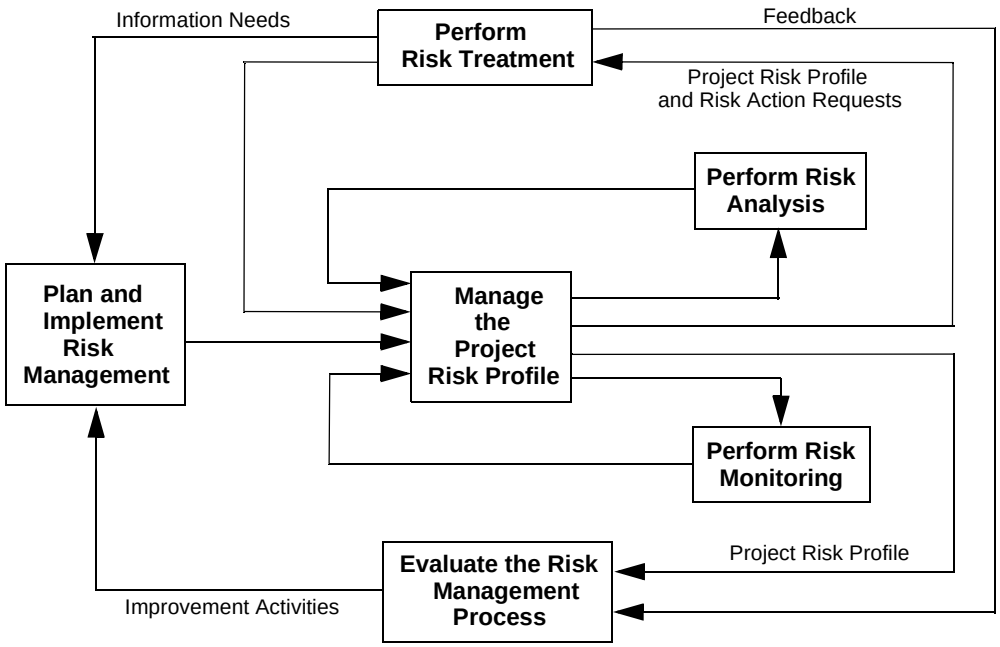

Figure 3: IEEE Risk Management Process Model

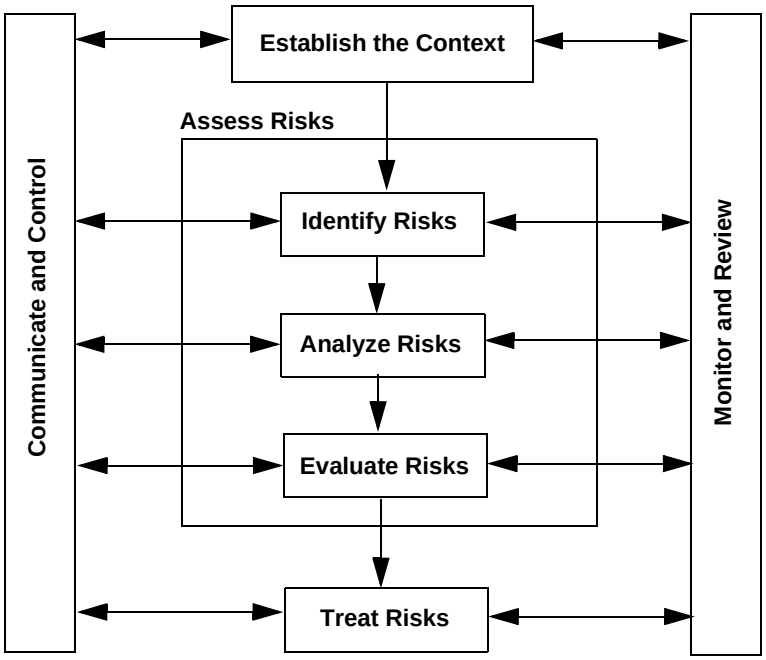

Figure 4: Risk Management Process from AN/NZS 4360

4 Limitations of Current Approaches to Risk Management

Although they do not explicitly consider interoperable risk management, the base documents we have discussed are valuable to this investigation because they form the set of practices often cited for risk management. Our analysis of those documents reveals that current specifications of risk management are insufficient to achieve interoperable risk management. We say this for two reasons:

1. Current risk management specifications do not define concepts to the degree needed to achieve interoperability.
2. Current risk management specifications do not address the operations necessary to achieve interoperable risk management.

4.1 SPECIFICATIONS OF DATA

Current risk management specifications are largely limited in their approach to the definition of concepts. Only one of the base documents examined in this work contains a specification of a risk statement, expressed in terms of a condition-consequence pair.

In general, the specification of a risk statement is lacking in certain aspects:

- Not all standards address the same topics, despite the amount of material that has been written about risk management. For example, the ISO/IEC standard does not define the concept of a risk statement, although the SEI guidebook does ([DoD 00], [Dorofee 96]).
- Different terminology is used; a noteworthy example is the use of terms *condition* and *event*. Do these terms convey the same meaning (i.e., different names for the same thing)? Or is there some nuanced difference they are meant to express? Generally, a *condition* is considered for something passive in nature (e.g., "there is water on the floor") while an *event* is active in nature (e.g., "a person may fall").
- The permitted structure (i.e., grammar) of a risk statement is often not specified.[5] Even if one accepts it as appropriate for a risk statement, the condition-consequence form is silent with respect to the structure of the condition and consequence (i.e., the clauses). What is the grammar of a risk statement? May the words *or* and *and* be used to couple the terms of a risk statement? What are the temporal considerations? Are we heading toward a formal specification of a risk statement? Do we need one?

Issues such as those identified above must be resolved to achieve interoperability with regard to risk management.

Also, current risk management specifications are insufficient for use in interoperability in an acquisition context. We will illustrate this point by the example of the term

5. In at least one case [Dorofee 96], there is some discussion about the structure of a risk statement, which is due to some earlier work [Gluch 94].

probability. The results shown in Table 1 on page 9 are illuminating but do not address the level of detail necessary for purposes of this research. A closer look at the base documents regarding probability leads to the information presented in Table 3.[6]

Table 3: Use of the Term Probability

Source	Definition
ISO/IEC Guide 73: Risk Management—Vocabulary—Guidelines for use in standards	Extent to which an *event* is likely to occur. • Note 1: ISO 3354 gives the mathematical definition of probability as "a real number in the scale 0 to 1 attached to a random event. It can be related to a long-run relative frequency of occurrence or to a degree of belief than an event will occur. For a high degree of belief, the probability is near 1." • Note 2: Frequency rather than probability may be used when describing risk. • Note 3: Degrees of belief about probability can be chosen as classes or ranks such as - rare/unlikely/moderate/almost certain, or - incredible/improbable/remote/occasional/probable/frequent
Risk Management Guidelines Handbook	A measure of the chance of occurrence expressed as a number between 0 and 1 • ISO Guide 73 defines probability as the "extent to which an event is likely to occur" • ISO 3354 gives the mathematical definition of probability as "a real number in the scale 0 to 1 attached to a random event." It goes on to note that probability "can be related to a long-run relative frequency of occurrence or to a degree of belief than an event will occur. For a high degree of belief, the probability is near 1." • 'Frequency' or 'likelihood' rather than 'probability' may be used in describing risk.
IEEE Standard for Software Life Cycle Processes—Risk Management	Not specifically discussed. Instead, they use the term *likelihood*, defined as "A quantitative or qualitative expression of the chances that an event will occur."
Risk Management Guide for DoD Acquisition	Not specifically defined. The probability of occurrence is defined as "states the likelihood of the event occurring, based on definitions in the program's Risk Management Plan."
Continuous Risk Management Guidebook	The likelihood that risk will occur.

Notice that probability may be defined in either a quantitative or qualitative manner. In the quantitative description, it is customary to define probability as a (real) number in the range of [0.0, 1.0]. In a qualitative approach, probability is often described in terms of some set of values. For example, the values of high, medium, and low are often seen, but others such as those identified in Table 3 (see Note 3 of the ISO/IEC Guide 73 standard content) are also found.

While a probability value may be expressed in either a qualitative or quantitative manner, there is no *requirement* that the relation between these two measurement

6. The material in Table 3 is taken verbatim from the indicated source.

schemes be provided. For example, does a qualitative value of *high* represent a quantitative value of 0.7 (or possibly 0.9)?

We believe there is a need for a specification of data related to risk management that is sufficiently robust to meet the needs of interoperable acquisition. Consider again the example of probability. A possible specification related to probability might contain the language illustrated in Figure 5.

3.1.4: Probability

1. Probability is the likelihood than an event will occur.
2. Probability may be expressed in either a quantitative or qualitative manner:
   a. When expressed as a quantitative measure, probability represents a real number in the range of 0.00 to 1.00.
   b. When expressed as a qualitative measure, the values *unlikely*, *low*, *medium*, *high*, and *almost certain* are accepted.
3. If both qualitative and quantitative values of probability are used, there must be a specification of how those values are related. The default profile for the relation between qualitative and quantitative measures of probability shall be defined as follows: unlikely (0.1), low (0.25), medium (0.5), high (0.75), and almost certain (0.9).

Figure 5: Example Specification of Probability

This example illustrates but one area where the development of a shared vocabulary would be of value. We believe that language such as that illustrated in Figure 5 is required to achieve interoperable risk management: There must be a way to resolve possible ambiguities in interpretation of information related to risk management.

The preceding example of probability is a concept about which agreement may be relatively easy to reach.[7] However, for other concepts, reaching agreement may be difficult. Consider the case of **impact** that reflects the nature of a possible loss. For a small organization, a loss of $100,000 may be significant. For a very large organization, that loss would be less significant. This distinction illustrates that the **context** of risk management information may be relevant.

Another concern is that the current specifications of risk management may be incomplete, lacking information that is necessary to achieve interoperability among organizations engaged in risk management.

Two examples will illustrate this concern about incomplete specifications:

- One would expect that there needs to be some **identifier** of a risk statement that is necessary to uniquely identify risk statements when they are exchanged.

7. Notice, though, that even the information in Figure 5 is open to interpretation. For example, instead of the qualitative values shown, one might desire a smaller set of values (just high, medium, and low, for example) or a larger set. This debate can be pushed back to the requirements specification. There, most people would agree that "There shall be a means to provide a qualitative measure of a probability." Issues often then arise in the refinement of such a statement. Problems such as this one are an age-old topic in the standards development community.

- One would also expect that there is some **state**, or status, of a risk that is maintained. What is the state model of a risk? Would the state model of a risk have the values *open* and *closed* or, perhaps, *valid* and *invalid*?

However, only two base documents addressed in this work listed an identifier or a risk state as one of the basic concepts (see Table 1 on page 9).

Consideration for interoperability has other implications that must also be addressed. In particular, we are thinking of the syntax (representation) and semantics of information exchanged. For example, is the risk status represented in terms of the familiar red-yellow-green values? If another project uses five values of color, how will interoperability be achieved? While syntactic issues are the easier of the two problems, the question of semantics looms large when one considers interoperability. Without a shared understanding of the semantics, problems are guaranteed to ensue.

4.2 SPECIFICATION OF BEHAVIORS

A second area of concern is that the existing specifications do not address the operations (behaviors encapsulated in processes) necessary to achieve interoperability among organizations that participate in risk management. Here, one may suggest questions such as

- If some entity identifies a new risk, should such information be made available to others, and if so, how? To whom? And when?
- How is the priority of a risk statement determined when one operates in a shared, distributed environment?
- If the state of a risk statement changes, what behaviors are expected?
- How can risk mitigation plans be developed for the case where participants are distributed in different organizations?

The question of syntactic and semantic concerns, raised earlier in regard to information, looms even larger when one considers the **shared behaviors** necessary to achieve interoperable risk management.

To illustrate this point, we show an example in Figure 6 of some possible requirements for operations related to interoperable risk management. The language has been written in terms of requirements that should be satisfied by some organization participating in interoperable risk management. This figure also contains references to the specification of a risk statement and its attributes.

We emphasize that this example is narrowly drawn. It purposefully does not address a number of factors. For example, is the distribution of information accomplished by a publish-subscribe mechanism? Or what quality of service is expected with information transfer; is reliable transfer assumed? The discussion of distribution of risk management information is a topic in its own right!

Notice in Figure 6 that we use the term *made available to others.*This phrasing is oriented toward a requirements specification. The means by which the information is

made available to others (e.g., publish-subscribe, posting on a Web page, or email) is considered a refinement question.

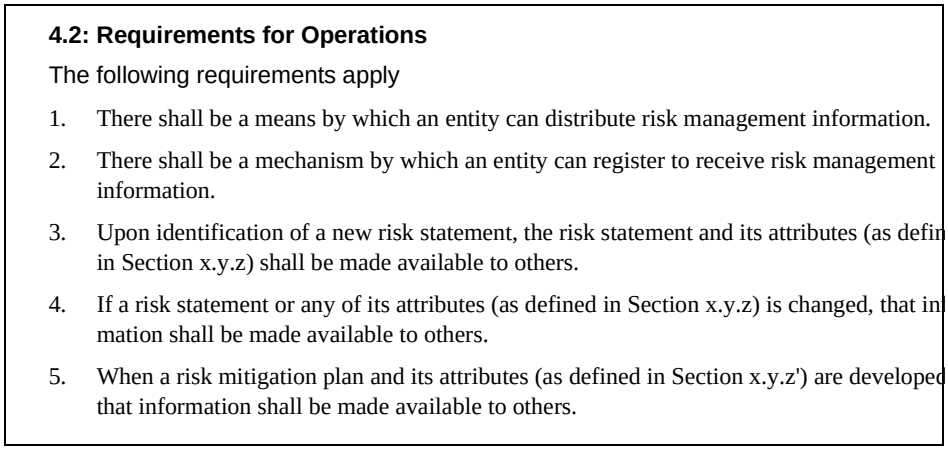

Figure 6: Sample Requirements for Operations Related to Interoperable Risk Management

4.3 SUMMARY

We recognize the need for a standard specification of concepts and operations relative to risk management. It is expected that such a specification will increase commonality of language for some domain. It is hoped, too, that such a specification will decrease the chance of incomplete or ambiguous interpretation. However, we have shown that those problems do indeed exist when viewed from an interoperable perspective. In addition, there are other considerations. For example, organization policies or politics can easily derail the most well-intentioned approach.

5 Research Questions

During the course of this work, many questions were identified that have bearing on the question of interoperable risk management. These questions are discussed in this section.

QUESTIONS REGARDING INFORMATION

Just what information related to risk management should be made available to other entities that are also engaged in interoperable risk management?

A start on the necessary information was provided in Section 3.2, in particular the concepts identified in Table 1 on page 9. While that discussion provides a starting point, more needs to be done. Recall, for example, the discussion of how one approaches the concept of probability, illustrated in Table 3 on page 13. There are companion questions to the main one cited, as well. For example, should a risk statement be provided in its entirety (i.e., as a condition-consequence pair), or is only the consequence of relevance? And what is the appropriate specification of a risk statement, including its possible temporal dependence?

Should there be a means to determine the quality of information provided, and if so, how would that means be determined?

It is natural for a receiver of information to want to know its quality. Consider the example of two programs, Program-1 and Program-2, that have a dependency of some sort, perhaps on schedule. Program-1 is interested in the risks that Program-2 has that may result in a failure to meet the schedule. Thus, it is natural for Program-1 to ask Program-2 for the risks related to some schedule item. In addition, Program-1 asks for the quality of such information. How would Program-2 respond to these questions? How would Program-1 judge the validity of statements made by Program-2?

QUESTIONS ON PRACTICES

What are the general implications for process models to achieve interoperable risk management?

Here, we are concerned with process—in particular, with process models and their interactions.[8] For example, one simple model of a process is based on ETVX.[9] Perhaps more relevant is a **defined** process that accounts for the following [Chrissis 03]:

- purpose
- inputs
- entry criteria
- activities

8. As mentioned earlier, the SEI is preparing a technical note addressing process considerations in interoperable acquisition.

9. ETVX is a concept in process modeling and stands for entrance criteria, tasks, validation, and exit criteria.

- roles
- measures
- verification
- outputs
- exit criteria

Are those process model elements sufficient to deal with the problem of interoperable acquisition? Or must something be changed in the basic approach?

What are the processes of relevance to the practice of interoperable risk management?

Examples of processes in risk management were discussed in Section 3.2; see in particular the processes listed in Table 2 on page 10. A number of processes are traditionally associated with risk management, such as risk identification and risk analysis. Do these processes need to be modified? Or should new processes be added to account for interoperable risk management? If existing processes need to be modified, what changes must be made to account for interoperability in a process context? Consider, for example, the collaboration of two organizations engaged in risk identification using **different** processes. We would argue that there are new processes needed, such as those supporting data management, distribution of information, and collaboration of activities by entities that participate in interoperable risk management.[10]

Just how important are questions about process anyway?

One can make the argument that the specification of a process is not what is important to achieve interoperability in risk management. What is important are the *outputs* from the process. For example, there is a distinction between the risks identified by some organization and the process used to identify those risks. One counter to this argument is that a successful processes using an established approach can be deemed to produce more reliable outputs.

Are there current risk management methods that adequately address the needs of interoperable risk management?

The assessment we have performed of existing risk management documents is about the data and processes specified in those documents. Certainly, it would appear that if methods (strictly) conformed to the **existing** processes, they could not provide interoperable acquisition. It is possible, however, that there are methods that have solved the problem, going beyond the existing specifications. Anecdotal evidence suggests that this is not the case, but a survey of current methods is warranted. If existing methods are not sufficient to meet the need of interoperable risk management, what changes are necessary? Furthermore, note the possible close relation between specifications of a process (the what) and methods and tools used to implement that process (the how).

---

10. A *Gedanken* (thought experiment) question we have asked ourselves several times during the course of this research is to complete the following sentence: "Two processes P and P' can interoperate if and only if _____." One approach is to complete the sentence by saying, "They are well-characterized processes that have been optimized for adaptability and flexibility and for the diverse stakeholders that will be using them." Is this response correct? What does *well-characterized* mean?

INTERACTIONS AMONG PARTICIPATING ENTITIES

What is the scope and nature of interactions between the entities that participate in interoperable risk management?

The question of scope of entities that participate in risk management was raised in Figure 2 on page 4. In particular, it is necessary to distinguish between the cases of bounded and unbounded interactions among entities (see Figure 2 on page 4). Consideration of interactions leads to discussion about the agreements between the entities. How can the agreements (and the process of managing agreements) be accounted for? Also of relevance are questions related to behaviors (and protocols) for the exchange of information.

What is the role of distributed versus centralized decision making in interoperable risk management?

It is natural that there will be decisions made concerning risk management. Some decisions may be made in the context of a particular organization or program. Yet, even here, failure to recognize dependencies among the entities engaged in interoperable risk management may result in a locally optimal solution that could have adverse implications when considered in the larger context. Further, how are risk management decisions made: Is it assumed that some central authority makes decision, or is the decision-making process distributed among the relevant constituents? Where does control and authority reside?

What are the implications of the greater expected interactions among entities for achieving interoperable risk management?

If one restricts consideration to a particular program, the primary interaction is between a program management office and an agent responsible for the construction of a system, most often a prime contractor. In such a case, the interaction is strongly influenced by a contract and adherence to the contractual process (reviews, reporting, and so on). However, when multiple programs are involved, there may be an information flow from a contractor to a program management organization to some other program management organization and then perhaps to some other contractor. The point is that the number of communicating entities will increase as the scope of desired interoperability in the acquisition process enlarges. This widening of scope has implications for the interaction among the entities, as well as assurances that such communication is effective.

How can trust be established between entities that participate in interoperable risk management?

A main characteristic of interoperable acquisition is the communication among entities that participate in the overall process. Where exchange of information is concerned, it is natural to inquire as to how trust is established among the participants. There is often a perception that one should hide risk information, because it might indicate that one is performing poorly. This view leads to the question of how one gains sufficient knowledge and experience to trust the information being provided by some other participant. Establishing trust becomes more important as the scope of

interoperable acquisition widens to the point where there may only be infrequent interaction with participants, especially in an unbounded environment.

What are the limitations to the sharing of information among entities?

As the scope of entities that participate in interoperable risk management increases, there may be limitations on exchange of information among those entities due to various considerations. For example, if there are several contractors developing systems that are expected to participate in a network-centric environment, they may not be inclined to share certain information. If a contractor uses a process considered proprietary, it may not be willing to share information about that process with other contractors due to a perceived loss of competitive advantage. This example illustrates how the question of interoperable risk management can quickly be elevated to the contracting process. That is, what contractual language must be in place to assure that sharing of relevant information is in fact achieved?

OTHER RELEVANT QUESTIONS

How does context affect interoperable risk management?

It is important to understand that risk management is performed in some context that influences the selection of specifications for risk management processes, methods, and tools. An example of this principle was provided in Section 4.1, where we indicated that the concept of **impact** could depend on the context (e.g., a dollar volume loss may be considered a high risk for a small organization, but not as high for a large organization). The context may therefore influence the semantics of interoperable risk management. There are also expected to be implications for risk mitigation as a result of contextual considerations.

How can cultural issues be addressed as one moves from a project perspective to a larger, possibly unbounded, perspective?

The practice of risk management is influenced by the cultures of those organizations that participate in the process. As the scope of risk management increases, the variations in culture will become of greater concern. Cultural concerns may become barriers to communication among organizations that seek to achieve interoperable risk management.

How can the fundamental question of semantics be addressed for this domain?

When one is concerned with questions of interoperability, the issue of semantics assumes a paramount position. One often reads about **semantic interoperability**. In this area, we ask, "What is necessary to assure that interoperating entities are able to establish and maintain interoperability with respect to the semantics of some domain?" This question applies to the concept of interoperable risk management, as well as to the larger issue of interoperable acquisition.

What are the metrics appropriate to interoperable risk management?

Most process descriptions include a discussion of metrics associated with the process. Data captured by those metrics may be presented as adherence to the process or as

trends regarding risk items and their status. (See *System Engineering Leading Indicators Guide* [Roedler 05] for some background.) However, the desire for interoperable risk management may raise new issues about metrics. To achieve interoperable risk management, it is necessary to address multiple organizations for which the items of interest might be different. For example, one organization might like to measure the amount of time to provide a risk statement to other entities. Another might be interested in measures associated with collaborative activities, such as risk mitigation when different parties are involved. The added complexity of interoperable risk management is expected to be reflected in its associated measures. The development of metrics might begin from the elements of the basic definition stated in Section 2.2: communicating entities, the data they share, and the operations performed on that data. Beyond this, there are many topics that can be elaborated.

Can automated tools provide value for interoperable risk management?

We believe they can. As an example, consider the case where several programs are developing systems that are expected to interoperate. One program is interested in risks associated with a particular milestone. It registers with a service to obtain such information, and its request is processed. Then, whenever there is a new risk or a change to an existing risk for a specified milestone, the requesting program automatically receives that information.

All exchanges of information can be initiated and performed in a fully automated manner.[11] Distributing updates in this manner is just one example of where technology can bring benefit. Certainly, one reason for automating is to deal with issues of scalability as more and more entities become involved. Can a suggested approach of "more people sitting around a bigger table" solve the problem?

What are the implications of this work for other areas of importance to interoperable acquisition, such as cost or schedule?

We have only revealed the tip of the proverbial iceberg in this work. There are many areas necessary to achieve interoperable acquisition, and risk management is but one of them. The approach taken in this work has been (1) an examination of documents representing the state of the practice, (2) assessment of those documents against the needs for interoperability, and (3) identification of outstanding research questions. Would that approach work for other areas, such as schedule management in a system-of-systems context? In addition, what about the integration of various topics, such as the relation between risk management and schedule management? This topic is currently under investigation.[12]

How can the transition to interoperable risk management be achieved?

A corollary question is this: How *should* risk management be addressed in terms of interoperable acquisition? Risk management is a complex domain, and it may be bet-

---

11. A desire for greater automation in risk management carries the concomitant requirement that information be sufficiently specified. We are calling for more rigorous specification, in part, to facilitate that desire.

12. As mentioned earlier, the SEI is preparing a technical note exploring schedule management in interoperable acquisition. It also addresses the connection between risk management and schedule management.

ter to delay its consideration pending other subjects of interest to interoperable acquisition, such as schedule or performance considerations. If one accepts the assertion that the current approach to risk management is not sufficient for interoperability in a system-of-systems context, then what should be done? There would be value in a detailed examination of the concepts related to risk management in a system-of-systems context—primarily the development of a common vocabulary that is essential to promoting shared understanding. Certainly, there is an ample supply of documents from which to begin! These are our recommendations:

- an approach to interoperable risk management be developed and piloted in a bounded, multi-organizational context
- automated tools be developed to support the chosen approach
- a broader transition approach be studied further (e.g., how can one make inroads into the process community that may prove valuable?)

How does the acquisition environment affect risk management, particularly when one is interested in interoperable risk management?

Acquisition takes place in a multifaceted environment including statutes, regulations (e.g., Federal Acquisition Regulations), and agency policies and procedures that influence the practice of risk management. Policies and procedures at the level of a program office and a program executive office, as well as those contained in the *Risk Management Guide for DoD Acquisition*, are oriented toward risk in a single-system context. The issues of current impediments or needed changes in the legal context to support interoperable risk management is worthy of study.[13]

The research questions presented in this section regarding interoperable risk management have direct relevance to the larger subject of interoperable acquisition. Interoperable risk management is one aspect of interoperable acquisition. When the broader scope of interoperable acquisition is viewed—which includes aspects of interoperability with regard to cost information, schedule, quality of products and services, and others—the issues identified in this section still apply.

13. In a forthcoming SEI report, we will address the implications of Title 10 and other statutes for acquisition in a system-of-systems environment. It is worth noting here that a quick search of Title 10 shows that the phrase "risk management" does not appear. However, Public Law 107-314, in Section 804, regarding improvement in the software acquisition process, states that such a program shall include "A documented process for software acquisition planning, requirements development and management, project management and oversight, and *risk management*" [italics added]. Public Law 107-314 also calls for development of appropriate metrics for performance measurement and continual process improvement [USC 02].

6 Summary

This report has examined the subject of interoperable risk management. Risk management has served as a worthy example for the investigation of interoperable acquisition. To the extent that risk management is an accepted practice in the acquisition of a particular system, it is only natural to expect that interoperable risk management would be of significant relevance to acquisition in a system-of-systems environment. We believe this to be the case and have outlined some aspects of this problem. Further, research questions arising from consideration of interoperable risk management have broader implication for other areas of acquisition. In this sense, interoperable risk management has served as an exemplar topic of study.

Our primary conclusion is that, despite the large amount of work that has been done on risk management, the current practice of risk management is insufficient to address the needs of **interoperable** risk management. We say this for the following reasons:

- **The current specifications related to risk management are insufficient to achieve interoperable risk management.** For example, as we have seen there are concepts that are
  - insufficiently specified (e.g., the relation between qualitative and quantitative values of probability)
  - unstated (e.g., the **identifier** of a risk or its **state**)
- **Our experience indicates current methodologies for the practice of risk management are insufficient to achieve interoperable risk management.** Existing practices encapsulate behaviors that are performed with regard to risk management. However, the specifications of such practices do not address
  - data management and sharing of risk-related data
  - behaviors performed in a collective manner, including the decision-making process

It is one thing to identify weaknesses, but it is something else to provide a way forward. Certainly, we need more complete specifications regarding information and its sharing. But we also need to address how such information will be used, with the goal of establishing collective behaviors to meet the larger goal to provide interoperable systems of systems. We believe there would be value in developing and piloting an approach that can meet those needs.

In addition, we would make some observations of a more general nature, namely:

- Risk management must be viewed in the larger context of interoperable acquisition. Some work previously reported on this topic argues for consideration of an ontological perspective, frameworks and models, libraries of standard practices, management of experiential information, and an examination of the negotiation process [Meyers 05]. In addition, each of these topics would benefit from a formal study. To some degree, the exposition of risk management, and the ability to

achieve interoperable risk management, is a thread running through interoperable acquisition.

- There would be merit in considering interoperable acquisition in accordance with the principles of network-centric operations. In commercial and government environments, there is increased emphasis in moving toward a network-centric model. Among the principles of network-centric operation are shared awareness of data through fusion of sensor information, virtual collaboration among distributed entities, and performance of activities in a collaborative manner to reach some specified goal. These concepts can easily be viewed as applying to the problem of achieving interoperable risk management among a disparate collection of entities and their collaboration. Further, the network-centric perspective places emphasis on the unbounded case, where the number of entities may not be known at any given time. (See the discussion of Case (c) on page 4.) This thought also applies to the domain of risk management. We are, in the end, heading toward an application of principles that would lead to **network-centric acquisition**.

We close on an important philosophical point. It is all too easy to say that we need another standard that meets the needs of interoperable acquisition. Perhaps one could also develop associated profiles of some standard and think that all would be fine. Such a perspective is, we believe, dangerous. While a standard may be necessary, it is not sufficient. We must not lull ourselves into believing that this problem is easy: It is not.

References

URLs are valid as of the publication date of this document

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

[ANZS 04]
Standards Australia/Standards New Zealand. *Risk Management Guidelines Companion to Australian/New Zealand Standard AN/NZS 4360: 2004 (*HB 436:2004). Syndey, Australia/Wellington, New Zealand: Standards Australia/ Standards New Zealand, 2004.

[Brownsword 06]
Brownsword, L.; Fisher, D.; Morris, E.; Smith, J.; & Kirwan, P. *System-of-Systems Navigator: An Approach for Managing System-of-Systems Interoperability,* (CMU/ SEI-2006-TN-019). Pittsburgh PA: Software Engineering Institute, Carnegie Mellon University, 2006.
http://www.sei.cmu.edu/publications/documents/06.reports/06tn019.html.

[Chrissis 03]
Chrissis, M. B.; Konrad, M.; & Shrum, S. *CMMI: Guidelines for Process Integration and Product Improvement.* Boston, MA: Addison-Wesley, 2003.

[DoD 00]
U. S. Department of Defense. *Risk Management Guide for DoD Acquisition, 3rd ed.* Ft. Belvoir, VA: Defense Systems Management College Press, 2000.

[DoD 01]
U. S. Department of Defense. *Systems Engineering Fundamentals.* Fort Belvoir, VA: Defense Acquisition University Press, 2001.

[Dorofee 96]
Dorofee, A. J.; Walker, J. A.; Alberts, C. J.; Higuera, R. P.; Murphy, R. L.; & Williams, R. C. *Continuous Risk Management Guidebook.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1996. http://www.sei.cmu.edu/ publications/books/other-books/crm.guidebk.html.

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

[Holzer 06]
Holzer, T. H. "Uniting Three Families of Risk Management," *Proceedings of the Eighteenth Annual Systems & Software Technology Conference (SSTC 2006)*. Salt Lake City, UT, May 1–4, 2006. http://www.sstc-online.org/proceedings/2006.

[IEEE 01]
Software Engineering Standards Committee of the IEEE Computer Society. *IEEE Std 1540-2001 IEEE Standard for Software Life Cycle Processes—Risk Management, March 17, 2001*. New York, NY: IEEE Standards Association, 2001.

[INCOSE 04]
International Council on Systems Engineering (INCOSE). *Systems Engineering Handbook, Version 2a*. Seattle, WA: INCOSE, June 2004.

[ISO 02]
International Standards Organization (ISO). *ISO/IEC Guide 73: Risk Management—Vocabulary—Guidelines for use in standards*. Geneva, Switzerland: ISO, 2002.

[Levine 03]
Levine, L. B.; Meyers, C.; Morris, E.; Place, P. R. H.; & Plakosh, D. *Proceedings of the System of Systems Interoperability Workshop (February 2003)* (CMU/SEI-2003-TN-016, ADA416429). Pittsburgh PA: Software Engineering Institute, Carnegie Mellon University, 2003.
http://www.sei.cmu.edu/publications/documents/03.reports/03tn016.html.

[Meyers 05]
Meyers, B. C.; Monarch, I. A.; Levine, L.; & Smith, J. D. *Including Interoperability in the Acquisition Process* (CMU/SEI-2005-TR-004, ADA441244). Pittsburgh PA: Software Engineering Institute, Carnegie Mellon University, 2005.
http://www.sei.cmu.edu/publications/documents/05.reports/06tr004.html.

[Moore 06]
Moore, J. "Harmonization of Systems and Software Engineering Processes," *Proceedings of the Eighteenth Annual Systems & Software Technology Conference (SSTC 2006)*. Salt Lake City UT, May 1–4, 2006. http://www.sstc-online.org/proceedings/2006.

[Morris 04]
Morris, E.; Levine, L.; Meyers, B. C.; Place, P. R. H.; & Plakosh, D. *System of Systems Interoperability (SOSI)*: *Final Report* (CMU/SEI-2004-TR-004). Pittsburgh PA: Software Engineering Institute, Carnegie Mellon University, 2004.
http://www.sei.cmu.edu/publications/documents/04.reports/04tr004.html.

[NASA 02]
National Aeronautics and Space Administration (NASA). *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*. Washington, DC: Office of Safety and Mission Assurance, August 2002.

[PMI 04]
Project Management Institute. *A Guide to the Project Management Body of Knowledge, 3rd ed*. Newton Square, PA: Project Management Institute, 2004.

[Roedler 05]
Roedler, G. & Rhodes, D. *System Engineering Leading Indictors Guide,* Beta Release. Seattle, WA: INCOSE, December 12, 2005.

[Smith 06]
Smith, J. D. & Phillips, M. *Interoperable Acquisition for Systems of Systems: The Challenges* (CMU/SEI-2006-TN-034). Pittsburgh PA: Software Engineering Institute, Carnegie Mellon University, 2006. http://www.sei.cmu.edu/publications/documents/06.reports/06tn034.html.

[USC 02]
United States Congress. *Bob Stump National Defense Authorization Act for Fiscal Year 2003, Public Law 107-314, 116 Stat. 2458 (December 2, 2002).* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ314.107.pdf.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. **AGENCY USE ONLY** (leave blank)	2. **REPORT DATE** August 2006	3. **REPORT TYPE AND DATES COVERED** Final
4. **TITLE AND SUBTITLE** Risk Management Considerations for Interoperable Acquisition		5. **FUNDING NUMBERS** FA8721-05-C-0003
6. **AUTHOR(S)** B. Craig Meyers		
7. **PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. **PERFORMING ORGANIZATION REPORT NUMBER** CMU/SEI-2006-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**		
12.a **DISTRIBUTION/AVAILABILITY STATEMENT** Unclassified/Unlimited, DTIC, NTIS		12.b **DISTRIBUTION CODE**

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

This report addresses interoperable risk management: the interoperability of organizations that participate in risk management in the context of a system of systems. The state of risk management practice—the specification of standards and the methodologies to implement them—is addressed and examined with respect to the needs of system-of-systems interoperability. The current practice is found to be insufficient to achieve interoperability with regard to risk management. A number of research questions are raised to associate this topic with the needs of the larger context of interoperable acquisition.

14. **SUBJECT TERMS** acquisition, interoperability, interoperable acquisition, network-centric, system of systems				15. **NUMBER OF PAGES** 28 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