Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

A Taxonomy of Operational Risks

CMU/SEI-2005-TN-036

Brian P. Gallagher
Pamela J. Case
Rita C. Creel
Susan Kushner
Ray C. Williams

September 2005

Acquisition Support Program

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 Tables

Abstract

In 1993, the Carnegie Mellon® Software Engineering Institute (SEI) developed a taxonomy-based method for facilitating the systematic and repeatable identification of risks associated with the development of a software-dependent project. Since then, this method has also been used in the Software Risk Evaluation process to identify risks associated with the development of software-intensive systems.

Recently, organizations that employ software-intensive systems have requested that the SEI help identify a baseline set of risks associated with missions performed at operational sites (e.g., satellite ground stations, military units, customer service units). While the concepts embodied in the software-based taxonomy apply in this context, the taxonomy presented in this report has been constructed to better suit an operational environment.

This report presents a taxonomy-based method for identifying and classifying risks to operational aspects of an enterprise. It defines the key sources of risk associated with the mission, work processes, and constraints of an operational organization and establishes a structure for representing operational risks by grouping them into distinct classes, elements, and attributes. In addition, the appendix of this report contains a short taxonomy-based questionnaire that can be used by personnel at operational sites to identify and categorize risks.

1 Introduction

The identification of risks is a major function of the SEI's Continuous Risk Management process, along with analysis, planning, tracking, controlling, and communicating risks. Risk identification is a crucial element of successful risk management in both developmental and operational undertakings.

As with the taxonomy-based risk identification method for software development projects published by the SEI in 1993, the perspective taken in this report is that there are risks inherent in missions performed at operational sites. Furthermore, taking risks is essential to progress and failure is often a key part of learning. Existing approaches to risk management tend to be ad hoc, undocumented, incomplete, and dependent on the experience and risk orientation of key personnel at operational sites. However, project risks are usually known by personnel (though they might not use the term risk to describe them) and as a consequence can be surfaced and managed [Carr 93].

The taxonomy of operational risks provides a structure for classifying risks to operational aspects of an enterprise. It defines the key sources of risk associated with the mission, work processes, and constraints of an operational organization and establishes a structure for representing operational risks by grouping them into distinct classes, elements, and attributes. The short taxonomy-based questionnaire included in this report can be used by personnel at operational sites to identify and categorize of risks.

1.1 Audience and Context

The taxonomy of operational risks is primarily intended for use by personnel at operational sites such as satellite ground stations, military units, and customer service units that focus on completing operational missions. An *operational mission* comprises tasks that involve the practical application of principles or processes.

1.2 Document Organization

The taxonomy of operational risks presented in this document is organized as follows

- Section 1 — Introduction
- Section 2 — Class, Element, and Attribute Definitions
- Section 3 — Conclusion
- Appendix — A Short Taxonomy-Based Questionnaire for Identifying Operational Risks

The first section provides a brief overview of the perspective taken when developing the taxonomy of operational risks and describes the audience for and organization of the report. Section 2 contains the taxonomy of operational risks grouped according to class, element, and attribute with definitions provided for each entry. The conclusion contains a summary of the report contents and directions for future work. Finally, the appendix contains a short taxonomy-based questionnaire that can be used by personnel at operational sites to facilitate the identification and categorization of risks.

2 Class, Element, and Attribute Definitions

This section describes the hierarchy of classes, elements, and attributes that comprise the taxonomy of operational risks. As shown in Table 1, the taxonomy is organized into three main *classes*:

- Mission — addresses characteristics of the operational mission itself, mechanisms to request products or services, and the outputs of the operational mission
- Work Processes — addresses aspects of the choices the operational organization makes when deciding how to execute the mission
- Constraints — identifies external influences that affect the operational mission

Each of these classes is divided into its constituent parts, called *elements*. Each element is associated with a set of *attributes*, or characteristics, traits, qualities, or properties, that are used to describe the element. Individual classes, elements, and attributes are described in detail in the remainder of this section.

Table 1: The Taxonomy of Operational Risks

A. Mission	B. Work Processes	C. Constraints
1. Tasking, Orders, and Plans a. Stability b. Completeness c. Clarity d. Validity e. Feasibility f. Precedent g. Timeliness **2. Mission Execution** a. Efficiency b. Effectiveness c. Complexity d. Timeliness e. Safety **3. Product or Service** a. Usability b. Effectiveness c. Timeliness d. Accuracy e. Correctness **4. Operational Systems** a. Throughput b. Suitability c. Usability d. Familiarity e. Reliability f. Security g. Inventory h. Installations i. System Support	**1. Operational Processes** a. Formality b. Suitability c. Process Control d. Familiarity e. Product Control **2. Maintenance Processes** a. Formality b. Suitability c. Process Control d. Familiarity e. Service Quality **3. Management Processes** a. Planning b. Organization c. Management Experience d. Program Interfaces **4. Management Methods** a. Monitoring b. Personnel Management c. Quality Assurance d. Configuration Management **5. Work Environment** a. Quality Attitude b. Cooperation c. Communication d. Morale	**1. Resources** a. Schedule b. Staff c. Budget d. Facilities e. Tools **2. Policies** a. Laws and Regulations b. Restrictions c. Contractual Constraints **3. Interfaces** a. Customer/User Community b. Associate Agencies c. Contractors d. Senior Leadership e. Vendors f. Politics

A. Mission

In an operational environment, a *mission* is considered to be the primary reason for the existence of the operational organization. The mission consists of a set of defined tasks that produce a product or service for a customer. The mission could be defense intelligence operations, banking, retail sales, manufacturing, or a variety of other missions, including those performed by civil agencies.

The elements of the Mission class of operational risks cover traditional aspects of the mission, including planning, execution, and the products and services provided. Mission elements include attributes of the operational systems and the organizations that operate those systems.

1. Tasking, Orders, and Plans

The Tasking, Orders, and Plans element contains attributes that are used to characterize aspects of the information contained in the tasks, orders, and plans of an operational organization. These attributes also describe the ability of an operational system and the organization that operates it to respond to requests. The following attributes characterize the Tasking, Orders, and Plans element.

a. Stability

The Stability attribute refers to the frequency with which tasks, orders, or plans change and the effect this has on the operational organization. It can also refer to the organizations that submit tasks or orders to an organization for execution. This attribute also addresses the flexibility of the operational entity in responding to changing tasks, orders, and plans and to handling multiple sources of tasks, orders, and plans.

b. Completeness

Complete information in tasks, orders, or plans such as time of task initiation, the period during which the task is to be performed, the end time of the task, the outputs of the task, or the recipient of the results are critical to ensuring the successful execution of the task, order, or plan.

c. Clarity

Clarity of a task, order, or plan is an attribute that enables the operational organization to clearly understand what the customer needs or wants. A clearly stated request or plan requires little or no interpretation by the operational organization; interpretation by the operational organization introduces the risk of producing an inadequate or undesired result.

d. Validity

The validity of a task, order, or plan refers to its appropriateness with respect to the purpose, goals, and capabilities of the operational organization's systems. Validity of a task, order, or plan can also refer to its internal consistency or other parameters such as requesting authority.

e. Feasibility

The Feasibility attribute refers to the operational organization's ability to meet the requests of the customer. Feasibility considers the actual capability of the organization's systems to provide the necessary product or service and also the capability to provide products or services to multiple customers. For example, system capacity can pose a risk or constraint. In addition, geographic or seasonal constraints can affect feasibility.

Also included in this attribute is the ability to identify a viable quantification method for measuring the results to determine if the system has satisfied the request for products or services.

f. Precedent

The Precedent attribute addresses the ability of an operational organization to perform tasks that it has not performed previously or may not have been designed to perform. In addition, it is possible that the organization's operational systems may not have been intended for a specific type of task and there may be political issues or risks with using a system in an unintended way.

In some cases, where precedent itself may not pose significant risk, there may be risk in reconfiguring the system to perform standard operations.

g. Timeliness

The Timeliness attribute refers to the operational organization receiving the task, orders, or requests for services to allow the scheduling and performance of the task in a time frame that meets the requestor's needs. Processes used to receive tasks, prioritize them, and prepare for execution may pose risks to timely planning and execution.

Lack of customer understanding or knowledge regarding required lead times can pose risks to customer satisfaction.

2. Mission Execution

Attributes of the Mission Execution element are used to characterize the ability of the operational organization to perform tasks in an effective and timely way. The complexity of preparing the system for customer tasks is also an attribute of the Mission Execution element.

a. Efficiency

The Efficiency attribute depends on systems and personnel being prepared to accept new or updated tasks or orders and execute them in time to meet customer needs. Execution efficiency refers to the ability to prioritize tasks and orders according to multiple parameters such as schedule, customer priority, and geographic considerations.

b. Effectiveness

The Effectiveness attribute describes the organization's ability to meet customers' needs according to their tasks and orders. Included in effectiveness is the ability to evaluate effectiveness using measures that have been defined for assessing effectiveness for each task, order, or plan.

c. Complexity

The Complexity attribute includes several aspects of mission execution. For example, a task that requires difficult or complex communication may be subject to more operator errors than one for which communication is easier and standardized. Complexity in using or configuring an operational system can require additional time, which could result in lack of timely responses to customer requests. Complex interfaces among diverse organizations, customers, or system components can also reduce timeliness and accuracy.

d. Timeliness

In the context of the Mission Execution element, the Timeliness attribute refers to the ability of operational systems and personnel to execute the requested task (or to process the order) in a time frame that meets the customer's needs. This attribute depends on the work processes of the operational organization. Work processes include understanding the request, scheduling the task, and communicating commands or instructions to the operational systems or personnel in time to perform the task to obtain the desired result. Timeliness also depends on the ability of the operational systems to be reconfigured in a timely fashion, if necessary.

e. Safety

The Safety attribute relates to potential hazards from performing the day-to-day mission and the operational organization's ability to identify and manage those hazards. Risks in the safety area may be related to performing unprecedented tasks or operating in a hostile environment. Risks can arise from the operational organization's inability to value an individual voice when raising and dealing with safety issues or concerns efficiently and effectively.

3. Product or Service

The Product or Service element of the Mission class contains attributes that are used to describe the products that the operational organization produces or the services that it performs for the customer. The following attributes characterize the Product or Service element and reflect the level of customer satisfaction attained with the product or service.

a. Usability

The Usability attribute of a product or service is used to characterize human-system interaction with regard to ease with which customers can use the delivered product or service to meet their goals. In this context, usability can depend on correct configuration for use in customer environments, system accuracy, or timely delivery. Occasionally, the product or service provided by the operational organization is what the customer requested, but the requirements that the customer submitted yielded a product or service that did not ultimately meet their needs. In this situation, usability risks can be related to the Clarity attribute of the Tasking, Orders, and Plans mission.

b. Effectiveness

The Effectiveness attribute refers to the ability of a product or service to satisfy needs of the customer. Product effectiveness parameters can include timeliness, accuracy, and correctness, for example. Service effectiveness parameters may include timeliness, completeness, ease of interaction, for example. Effectiveness is measured using criteria established, in advance, by the customer in cooperation with the operational personnel. Effectiveness may be dependent on the ability to establish and manage realistic customer expectations.

c. Timeliness

The Timeliness attribute refers to delivery of a product to the customer during the time frame requested. Timeliness depends on the operational organization's ability to prepare and deliver results to the user within the time agreed to by both parties. Product delivery can also depend on external communications or other external organizations or systems that could present a risk to timely delivery.

d. Accuracy

The Accuracy attribute refers to the degree to which the output reflects the actual conditions or real-world data. For example, the output of the Global Positioning System provides results that are not perfect, but have a high degree (within 100 meters) of accuracy.

e. Correctness

The Correctness attribute describes the degree to which the product represents the product's design. For example, when a product depends on processing algorithms, correctness refers to the degree to which the algorithm produces the expected results across the range of operational parameters.

4. Operational Systems

The Operational Systems element of the Mission class contains attributes that are used to characterize the operational systems' ability to perform satisfactorily and the features that affect an operator's ability to interact with systems to produce products or perform services for the customer. The following attributes characterize the Operations Systems element.

a. Throughput

The Throughput attribute refers to operational systems' ability to satisfy the anticipated, combined needs of its customers. Throughput risks can be related to the designed capacity of the system as determined by the expected number of customers and the output needs of each. Throughput risks can also be related to specific high-volume periods or events.

b. Suitability

The Suitability attribute describes specific features that enable operational systems to meet customer needs in conjunction with the planning and execution needs of the operational organization. Issues with suitability can include inappropriate use or modification of an existing system to meet new mission requirements or needs. Also, overdesign of a system or inappropriate use of technology (old or new) can pose risk.

c. Usability

The Usability attribute of an operational system is used to characterize human-system interaction with regard to the ease with which operators can achieve tasks in a particular environment or by using a specific product. For example, the use of standard icons or positioning of items on interfaces can make using the system more "intuitive," enhancing usability. Providing operators with direct access to the needed components of a system can also enhance usability. The Usability attribute can also be used to describe the physical location of system components accessed by system operators.

d. Familiarity

The Familiarity attribute describes personnel's knowledge of, experience in, and comfort with the operational systems used to perform the mission. Familiarity reflects a

combination of formal or on-the-job training, mentoring, and experience. Risks related to the Familiarity attribute can include low productivity and low-quality results.

e. Reliability

The reliability of operational systems includes availability to process tasks and orders in the manner described in the operational concept or in the system requirements and the ability to achieve repeatable results. Availability can be affected by hardware performance or by system complexities that affect reconfiguration (hardware and software) following a system failure. Repeatable results refers to the operational organization's ability to produce the same results for products or services when given the same tasks or orders.

f. Security

The Security attribute characterizes data, system, and inter-system security aspects that can introduce risk to the operation. Data security refers the integrity of individual data elements within the operation. System security refers to the ability to restrict access to components within the system. Inter-system security refers to the ability to ensure the integrity of external interfaces and restrict access by external systems.

g. Inventory

The Inventory attribute describes aspects of managing and using raw materials to produce products or services during mission execution. Risks in this area relate to the unavailability of resources when required or the costs of having to store large amounts of raw materials waiting to be processed.

h. Installations

The Installations attribute describes aspects of operational acceptance and the integration of new capabilities into the operational environment. Risks in this area are associated with depletion of capability or throughput, increases in operational expenditures, or less than optimal inventory levels resulting from system upgrades.

i. System Support

The System Support attribute describes the ability of facilities and other personnel to provide adequate system support to meet availability, reliability, capacity, and other operational requirements. System support can include repair/replace activities and facilities maintenance. It can also include the collection and analysis of system performance data to identify areas for improvement.

B. Work Processes

The Work Processes class contains elements and attributes that are used to describe the processes through which the operational organization fulfills its mission. The element and attributes in this class can also be used to characterize the management processes, methods, and environment in which the work takes place.

1. Operational Processes

The attributes contained in the Operational Processes element are used to describe the sequence of steps, inputs, outputs, actions, verification, and monitoring activities that the operational organization follows to provide its products or services.

Risks in this category surface as a result of operational processes that are inadequately planned, defined, and documented, those that are not suited to the activities necessary to accomplish the operational mission, those that are poorly communicated to the staff, or those that are not enforced. The following attributes characterize the Operational Processes element.

a. Formality

The Formality attribute of the operational processes element describes the degree to which operational processes are defined, documented, and communicated. Lack of sufficient formality can produce inconsistent results. A lack of sensitivity with regard to organizational culture can hamper the adoption of formal processes. For examples, military processes can have a different level of formality than warehousing operations.

b. Suitability

The Suitability attribute addresses how adequately the scope of the operation and types of activities that comprise the operation are supported. Processes that are incomplete or outdated can represent risks to completing the operational mission.

c. Process Control

The Process Control attribute not only ensures the consistent use of operational processes but also consistent measurement and improvement of processes based on observations of the quality of the results and productivity goals.

d. Familiarity

The Familiarity attribute describes how familiar personnel are with the operational processes. It covers their knowledge of, experience in, and comfort with the prescribed processes. It reflects a combination of formal or on-the-job training, mentoring, and experience. Risks in this area can include low productivity and low-quality results.

e. Product Control

Product control refers to the monitoring of the product or service quality or other aspects of the final product or service at specific points in the operational processes to ensure the integrity of the final result. Products or services that do not meet quality standards can result in customer dissatisfaction.

2. Maintenance Processes

Maintenance Processes are processes that ensure that the operational infrastructure (including equipment, software, utilities, and communications) can effectively support the operational mission. Some risks identified in this category can be associated with outsourcing some or all of the maintenance processes. The following attributes characterize the Maintenance Processes element.

a. Formality

Formality of maintenance processes addresses the degree to which maintenance processes are defined, documented, and communicated. Lack of sufficient processes and procedures to guide individuals who perform maintenance tasks can result in inadequate performance. Too little formality can put maintenance results at risk or produce inconsistent results. Too formal a process can cause some maintenance needs to be ignored.

b. Suitability

The Suitability attribute with regard to maintenance processes describes the scope of maintenance, consistency with operational infrastructure, and compatibility with routine mission needs. Suitability includes adequate maintenance plans to address the complete scope of the operational infrastructure and keeping maintenance processes current with infrastructure updates. It also includes planning maintenance activities so that the maintenance schedule is compatible with routine mission needs.

c. Process Control

The Process Control attribute refers not only to ensuring the use of the maintenance processes, but also to the measurement and improvement of processes based on the quality of the results and availability of infrastructure components. Process control includes providing mechanisms for monitoring process implementation and measuring process results for improvement purposes.

d. Familiarity

Familiarity with maintenance processes characterizes knowledge of, experience in, and comfort with the prescribed processes. It reflects a combination of formal or on-the-job

training, mentoring, and experience. It includes planning to reduce the impact of new and unfamiliar processes.

e. Service Quality

The Service Quality attribute refers to the monitoring of the maintenance service quality or other aspects of maintenance service at specific points in the maintenance processes to ensure the integrity of the final results. It includes mechanisms to measure operational system availability, time to repair or update, and other measures to control the quality of maintenance activities.

3. Management Processes

The attributes contained in the Management Processes element are used to characterize risks associated with planning, monitoring, and controlling the operational budget and schedule; with managing operational personnel; and with handling external organizations including customers, contractors, and other agencies. The following attributes characterize the Management Processes element.

a. Planning

The Planning attribute characterizes the risks associated with developing well-defined operational plans, formulated with the input and consent of those affected by the plans, that respond to contingencies and overarching goals of the mission. Also included are the tasks of managing the project according to the plans and formally modifying the plans when changes are necessary. The mismatch of plans to operational needs (for flexibility or rapid re-orientation) can be a source of risk.

b. Organization

The Organization attribute describes the effectiveness of the organizational structure of the operational organization as it relates to carrying out a specific operational mission. It includes clear definitions of roles and responsibilities and assurance that operational personnel understand these roles and the decision-making hierarchy.

c. Management Experience

The Management Experience attribute characterizes the experience of all levels of managers with respect to their management ability, domain familiarity, ability to deal with scale and complexity issues, familiarity with operational processes, and hands-on operational experience.

d. Program Interfaces

The Program Interfaces attribute describes the interactions of managers at all levels with the operational personnel at all levels and with external personnel such as peer managers, senior management, and customers.

4. Management Methods

The Management Methods element contains attributes that are used to characterize an operational organization's methods for managing the mission and operational personnel. These methods include quality assurance, configuration management, staff development with respect to operational needs, and level of communication about operational status and needs. The following attributes characterize the Management Methods element.

a. Monitoring

Monitoring includes activities for obtaining and acting upon status reports, allocating status information to the appropriate operational personnel, and maintaining and using operational metrics. Lack of monitoring can result in an uncontrolled process and inappropriate or ineffective actions of operational personnel due to lack of feedback.

b. Personnel Management

Personnel management describes how operational personnel are selected and trained. The operational organization should ensure that they take part in planning and customer interaction for their areas of responsibility, work according to plan, and receive the help they need or ask for to carry out their responsibilities. This attribute includes planning growth and development opportunities for operational personnel.

c. Quality Assurance

The Quality Assurance attribute describes the procedures instituted to ensure that both the operational processes and standards are implemented properly for all operational activities and that the quality assurance function is adequately staffed to perform its duties. It includes identifying and using mechanisms to collect process implementation data and measures and a role definition for quality assurance to include process implementation assurance.

d. Configuration Management

The Configuration Management (CM) attribute describes both staffing and tools for the operational CM function and the complexity of the required CM process with respect to factors like having multiple operational sites. It involves managing the configuration of both hardware and software systems that support the operation in a manner that pro-

vides the end user with consistent, compatible products and services. Poor communication with system development organizations can increase risk in this area.

5. Work Environment

The Work Environment element contains attributes that are used to characterize the subjective aspects of the operational environment such as the amount of care taken to ensure that people are informed of business or mission goals and status, roles and responsibilities, responsiveness to staff inputs, and the attitude and morale of operational personnel. The following attributes characterize the Work Environment element.

a. Quality Attitude

The Quality Attitude attribute describes the tendency of operational personnel to do quality work in general and to conform to specific quality standards for the mission and the resulting products or services. It involves recognition and reward of positive quality attitudes and behaviors.

b. Cooperation

The Cooperation attribute is demonstrated by the level of teamwork among the operational personnel both within and across work groups. Managers at all levels support cooperation by removing barriers, establishing a common vision, and negotiating mutually acceptable goals. Managers should encourage strong working relationships across the operational organization.

c. Communication

Good communication is essential to establishing an operational environment in which cooperation is strong, morale is good, and there is pride in the quality of the results. Communicating information about the importance of the mission, the status of the mission outputs, and feedback from consumers of the products and services affects all aspects of the work environment.

d. Morale

Risks resulting from low morale can include low enthusiasm resulting in low performance or productivity; anger that can result in intentional damage to the mission; mass exodus from the operational organization; and earning a reputation that makes it difficult to recruit personnel within the organization.

C. Constraints

The Constraints class contains elements and attributes that are used to characterize the external factors that present special challenges for operational organization. Constraints can include obtaining adequate resources, compliance with regard to legal factors, or handling conflicting political influences.

1. Resources

The Resources element contains attributes that are used to describe the resources on which the mission is dependent and factors outside the operational organization's purview that are its responsibility to obtain and maintain. The following attributes characterize the Resources element.

a. Schedule

The Schedule attribute refers to the timeline and throughput of the mission that is required for achieving its objectives. Risks can be associated with unrealistic schedule constraints or overall operational throughput. Schedules for installations or upgrades of systems in addition to external constraints and expectations can also cause risks to the mission.

b. Staff

The Staff attribute describes the stability and adequacy of the staff in terms of numbers and skill levels, their experience and skills in the required technical areas, and their availability when needed. Inadequate staffing can result in an inability to meet mission requirements, mission timeliness, quality requirements, or operational infrastructure availability.

c. Budget

The Budget attribute describes the stability of the budget with respect to internal and external events or dependencies and the viability of plans and estimates for all phases and aspects of the maintenance of operational systems.

d. Facilities

The Facilities attribute characterizes the adequacy of the operational facilities for planning and executing the operational mission and for communicating and for maintaining the infrastructure to support mission execution.

e. Tools

The Tools attribute refers to the availability of adequate tools to support the management, work, and maintenance processes of the operational systems. It includes both hardware and software tools.

2. Policies

The attributes that compose the Policy element are used to characterize risks associated with laws and regulations, restrictions, and contractual constraints that may affect the ability of the operational organization to perform its mission. The following attributes characterize the Policy element.

a. Laws and Regulations

The Laws and Regulations attribute addresses federal, state, local, or international laws and regulations that can impact the mission. Personnel with applicable expertise may not be available to identify and interpret applicable laws and regulations. Identifying these risks is particularly important because legal or regulatory issues discovered late in the planning process can require that the operational plans be substantially reworked.

b. Restrictions

The Restrictions attribute describes constraints that can contribute risk to a mission. Laws, regulations, and local customs can impose restrictions to operational personnel. Local codes can impose operational facility requirements or constraints (e.g., electrical interfaces, shock or hardness requirements for system components). Environmental constraints may apply.

c. Contractual Constraints

Contractual constraints relate to use of contracts by the operational organization. Contractual constraints or requirements can impose risk if the mission delivers products or services under contract. For example, risks can be associated with incremental funding of operational tasks.

Contractual constraints can also refer to contracts for the physical space in which the operation takes place if the space is rented or leased. In this case, contractual constraints can relate to property use or configuration.

Contractual constraints can also refer to labor contracts if the system is operated by contract labor. For example, constraints that can impact operational cost can exist for how many hours people can work, their working conditions, and their benefits.

3. Interfaces

The attributes that make up the Interfaces element are used to characterize risks associated with the customer or user community, associate agencies, contractors, senior leadership, vendors, and politics external to the operational organization, which can influence the ability of the operational organization to perform its mission. The following attributes characterize the Interfaces element.

a. Customer/User Community

The Customer/User Community attribute addresses risks as they relate to a customer's technical understanding of the mission, its products and services, and the customer's ability to communicate with the operational organization. Risks in this category can include difficult relationships or poorly conceived methods for requesting information or services. Risk can also be introduced when there are no feedback mechanisms for users or customers to tell the operational organization what improvements would benefit them.

b. Associate Agencies

The Associate Agencies attribute describes risks with working with other agencies or organizations. For example, associate agencies can have conflicting political agendas or be in competition for funding. Risks can be introduced in defining and developing interfaces with systems developed by other agencies or in coordinating schedules or configuration changes.

c. Contractors

Using contractors to perform work for an operational systems organization can introduce risk. Risks can arise from unclear or inadequate task definition, inadequate or lack of communication. If contractors are integral parts of operational teams, there can be a risk of a lack of team cohesiveness.

d. Senior Leadership

Senior leadership risks can include poor communication and direction from senior management and non-optimal levels of support. Lack of leadership can contribute to other risks identified in the Work Environment element including low morale and general lack of cooperation.

e. Vendors

Vendor risks can be present in dependencies on deliveries and support for maintaining operational capability.

f. Politics

Political risks can arise from relationships with associate agencies or other companies, customers, or contractors and can affect technical decisions or ability to operate the system. Operational organizations that perform missions in international locations may need to spend extra care addressing issues that arise from operating in foreign or remote locations.

3 Conclusion

The taxonomy for identifying and classifying risks to operational aspects of an enterprise presented in this report can help personnel identify the key sources of risk associated with the mission, work processes, and constraints of an operational organization. By grouping operational risks into distinct classes, elements, and attributes a structure for representing operational risks is established. In addition, personnel at operational sites can use the short taxonomy-based questionnaire in the appendix of this report to identify and categorize risks.

3.1 Directions for Future Work

Future directions for this work include developing methods to use this taxonomy to elicit operational requirements for new system development, identify risks associated with installing new operational capabilities, and conduct cross-organizational Team Risk Management activities between operational personnel, acquisition organizations, and system developers. In addition, the short taxonomy-based questionnaire found in the appendix could be expanded to allow for a more in-depth, structured exploration of operational risks.

Appendix A Short Taxonomy-Based Questionnaire for Identifying Operational Risks

A. Mission

Consider risks to the operation that can arise because of the nature of the mission that your organization is trying to accomplish.

1. Tasking, Orders, and Plans

Question: Are there risks that could arise from the way the mission is tasked, orders are provided, or operational plans developed? Examples:

a. Stability
b. Completeness
c. Clarity
d. Validity
e. Feasibility
f. Precedent
g. Timeliness

2. Mission Execution

Question: Are there risks that could arise from executing the mission? Examples:

a. Efficiency
b. Effectiveness
c. Complexity
d. Timeliness
e. Safety

3. Product or Service

Question: Are there risks that could arise from the end product or service this operational mission provides? Examples:

a. Usability
b. Effectiveness
c. Timeliness
d. Accuracy
e. Correctness

4. Operational Systems

Question: Are there risks that could arise from the operational systems used? Examples:

a. Throughput
b. Suitability
c. Usability
d. Familiarity
e. Reliability
f. Security
g. Inventory
h. Installations
i. System Support

Other

Question: Are there other risks that could arise from your mission but are not covered by the above categories?

B. Work Processes

Consider risks to the mission that could arise from the way your organization is executing the mission.

1. Operational Processes

Question: Are there risks that could arise from the process the operational organization has chosen to execute the mission? Examples:

a. Formality
b. Suitability
c. Process Control
d. Familiarity
e. Product Control

2. Maintenance Processes

Question: Are there risks that could arise from the process the front-line (level 1) maintenance organization uses to maintain the operational systems? Examples:

a. Formality
b. Suitability
c. Process Control
d. Familiarity
e. Service Quality

3. Management Processes

Question: Are there risks that could arise from the way operational budget or schedule is planned, monitored, or controlled; or in the operational organization's structure; or its handling of internal and external interfaces? Examples:

a. Planning
b. Organization
c. Management Experience
d. Program Interfaces

4. Management Methods

Question: Are there risks that could arise from the way operational personnel are managed? Examples:

a. Monitoring

b. Personnel Management

c. Quality Assurance

d. Configuration Management

5. Work Environment

Question: Are there risks that could arise from the general environment or the larger organization to which the operational unit belongs? Examples:

a. Quality Attitude

b. Cooperation

c. Communication

d. Morale

Other

Question: Are there other risks that could arise from the way the operational unit is going about its mission but are not covered by the above categories?

C. Constraints

Consider risks to the mission that could arise from sources outside your control.

1. Resources

Question: Are there risks that could arise from resources the operational organization needs but that are outside its control to obtain or maintain? Examples:

a. Schedule

b. Staff

c. Budget

d. Facilities

e. Tools

2. Policies

Question: Are there risks that could arise from legally binding or constraining policies? Examples:

a. Laws and Regulations

b. Restrictions

c. Contractual Constraints

3. Interfaces

Question: Are there risks that could arise from outside interfaces which the operational organization cannot reasonably expect to control? Examples:

a. Customer/User Community

b. Associate Agencies

c. Contractors

d. Senior Leadership

e. Vendors

f. Politics

Other

Question: Are there other risks that could arise from factors outside control of the operational organization but are not covered by the above categories?

Bibliography

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

[Carr 93] Carr, Marvin J.; Konda, Surish L.; Monarch, Ira; Ulrich, F. Carol; & Walker, Clay F. *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/93.tr.006.html

[Gluch 94] Gluch, David P. *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

[Murphy 96] Murphy, Richard L.; Alberts, Christopher J.; Williams, Ray C.; Higuera, Ronald P.; Dorofee, Audrey J.; Walker Julie A. *Continuous Risk Management Guidebook*. Pittsburgh, PA: Carnegie Mellon University, 1996. http://www.sei.cmu.edu/publications/books/other-books/crm.guidebk.html

[Williams 99] Williams, Ray C.; Pandelios, George J.; & Behrens, Sandra G. *Software Risk Evaluation (SRE) Method Description (Version 2.0)* (CMU/SEI-99-TR-029, ADA001008). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999. http://www.sei.cmu.edu/publications/documents/99.reports/99tr029/99tr029abstract.html

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2005	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
A Taxonomy of Operational Risks	FA8721-05-C-0003

6. AUTHOR(S)
Brian P. Gallagher, Pamela J. Case, Rita C. Creel, Susan Kushner, & Ray C. Williams

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2005-TN-036

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

11. SUPPLEMENTARY NOTES

12.a DISTRIBUTION/AVAILABILITY STATEMENT	12.b DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (maximum 200 words)

In 1993, the Carnegie Mellon® Software Engineering Institute (SEI) developed a taxonomy-based method for facilitating the systematic and repeatable identification of risks associated with the development of a software-dependent project. Since then, this method has also been used in the Software Risk Evaluation process to identify risks associated with the development of software-intensive systems.

Recently, organizations that employ software-intensive systems have requested that the SEI help identify a baseline set of risks associated with missions performed at operational sites (e.g., satellite ground stations, military units, customer service units). While the concepts embodied in the software-based taxonomy apply in this context, the taxonomy presented in this report has been constructed to better suit an operational environment.

This report presents a taxonomy-based method for identifying and classifying risks to operational aspects of an enterprise. It defines the key sources of risk associated with the mission, work processes, and constraints of an operational organization and establishes a structure for representing operational risks by grouping them into distinct classes, elements, and attributes. In addition, the appendix of this report contains a short taxonomy-based questionnaire that can be used by personnel at operational sites to identify and categorize risks.

14. SUBJECT TERMS	15. NUMBER OF PAGES
acquisition, configuration management, operation, operational organization, operational system, risk, risk identification, risk management, software-intensive systems, taxonomy, risk taxonomy, software risk evaluation	38
	16. PRICE CODE

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