DISSERTATION

USING OPERATIONAL RISK TO INCREASE SYSTEMS ENGINEERING EFFECTIVENESS

Submitted by

Brian P. Gallagher

College of Engineering

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Summer 2016

Doctoral Committee:

Advisor: Ronald M. Sega

Edwin Chong
Peter Young
Thomas Bradley

Copyright by Brian P. Gallagher 2016

All Rights Reserved

ABSTRACT

USING OPERATIONAL RISK TO INCREASE SYSTEMS ENGINEERING EFFECTIVENESS

A key activity in the systems engineering process is managing risk. Systems engineers transform end-user needs into requirements that then drive design, development, and deployment activities. Experienced systems engineers are aware of both programmatic risk and technical risk and how these risks impact program outcomes. A programmatic change to cost, schedule, process, team structure, or a wide variety of other elements may impact the engineering effort and increase the risk of failing to deliver a product or capability when needed, with all required functionality, at the promised cost.

Technical challenges may introduce risk as well. If a sub-component or element of the design is immature or doesn't perform as expected, additional effort may be required to re-design the element or may even necessitate a change in requirements or a complete system re-design.

Anticipating programmatic and technical risks and implementing plans to mitigate these risks is part of the systems engineering process. Even with a potent risk management process in place, end-users reject new capabilities when the delivered capabilities fail to perform to their expectations or fail to address the end-user’s operational need.

The time between the identification of an operational need and the delivery of the resulting capability may be months or even years. When delivered, the new capability either does not fulfil the original need or the need has evolved over time. This disconnect increases operational risk to the end-user’s mission or business objectives. When systems engineers explicitly identify and mitigate operational risk, in addition to programmatic and technical risk, program outcomes are more likely to meet the end-user’s real operational need.

The purpose of this research is first to define the activities that could be used by systems engineers to ensure that engineering activities are influenced by operational risk considerations. Secondly, to determine if a focus on operational risk during the systems engineering lifecycle has a positive impact on program outcomes.

A structured approach to addressing operational risk during the systems engineering process, Operational Risk-Driven Engineering Requirements/Engineering Development (ORDERED), is introduced. ORDERED includes an exhaustive operational risk taxonomy designed to assist systems engineers with incorporating the end-user’s evolving operational risk considerations into systems engineering activities.

To examine the relationship between operational risk considerations during the systems engineering process and program outcomes, a survey instrument was developed and administered. In addition, a system dynamics model was developed to examine the relationship between operational risk and technical debt. Finally, case studies of successful and challenged programs were evaluated against characteristics of successfully addressing operational risk during the program lifecycle. These activities lead to the conclusion that a focus on operational risk during the systems engineering lifecycle has a positive impact on program outcomes.

ACKNOWLEDGEMENTS

Many individuals have inspired and encouraged me along this journey. I would like to first thank my committee members for their patience and encouragement. In 2007, Ron Sega was the Under Secretary of the Air Force and visited Carnegie Mellon University, where I was serving as a director at the Software Engineering Institute. At the end of his visit, he presented me with a challenge coin on which was the emblem of the office he held, which I still have to this day.

When Dr. Sega agreed to be my advisor, I was absolutely honored and am grateful for the time that he spent on the telephone with me and his face-to-face visits while he traveled. His encouragement and positive attitude throughout our time together provided the motivation and direction I needed to complete this research and dissertation.

I would also like to thank Dr. Nidiffer, who was a colleague and friend before he agreed to be the outside member on my committee. The first question he asked was *why*. Ken helped me understand the motivation and the commitment needed to complete the dissertation and was always available to lend advice and helpful criticism.

My former and current colleagues in the United States Air Force and at Carnegie Mellon University, Aerospace Corporation, Northrop Grumman, and CACI all provided motivation and challenged my ideas and kept them grounded in reality.

Ray Williams taught me that the topic of risk management was not yet a dead horse, and his grasp of the subject and his passion sparked my curiosity. Ceci Albert spent many hours with a whiteboard marker convincing me that we needed to reverse our thinking about systems and software engineering. Bill Novak taught me about system dynamics and how expedient decisions and unintended consequences cause recurrent failures in acquisition and engineering.

Mike Hayner taught me about managing program risk and delivering mission-critical value. Dr. Barry Boehm taught me to perform the hardest, riskiest activities first. Dr. Jack Ferguson, Jon Gross, Dr. Steve Cross, Clyde Chittister, Dr. Paul Nielsen, Jeff Yu, Dan Allen, John Mengucci, Ken Asbury, Dr. Jack London, the late Ron Higuera, and the late Tom Brandt all took a chance and provided opportunities for me to learn and explore while keeping my family fed.

Finally, I could never have completed this work without the love and support of my family. My parents, Ed and Earlene Gallagher, and my mother-in-law, Alice Hutcherson, provided unending support, as did my father-in-law and step-father-in-law, Jasper Hutcherson and Dr. Lyn Miller, before their passing.

My children, Ashley, Caitlin, Rachel, and Gabriel give me hope for the future and the energy to continue as a life-long learner. My son Brian was intelligent and the kindest young man you could ever meet. He would give you the shirt off his back even when you didn’t realize you needed it. He left us too soon, and not a day goes by that we don’t miss having him here. He was a better man than I am, and I decided to pursue a Ph.D. because he didn’t have the chance.

DEDICATION

This work is dedicated to my wife, Valerie. I met Valerie when we were both 15, and we married at 18. Her patience, encouragement, sacrifice, and wisdom kept me moving in the right direction, kept the family safe and protected, and allowed us to learn and grow as a team. Thank you for your support and unwavering love.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Systems engineering *is an interdisciplinary approach and means to enable the realization of successful systems*[1]. The practices, approaches, methods, and tools of systems engineering have been codified over time and have evolved as technology, system, and operational complexity increases. The purpose of having a set of proven practices for engineers to follow is to reduce system development risk and to increase the probability of delivering a system that meets an operational need[2].

The tools applied to a given problem are selected based on an understanding of certain quality attributes of the product under development or the management aspects of the team producing the product within cost and schedule constraints. Therefore, a given practice is considered effective only if it reduces technical, programmatic, and/or operational risk.

Technical risk identification and mitigation is concerned with the quality attributes of the end product. For example, a product may have stringent reliability requirements. Another product may have real-time processing requirements.

The systems engineering methods and tools for mitigating reliability risks may include using design patterns such as redundant hardware and software or fault detection and remediation mechanisms. Products with real-time requirements might use design patterns with the ability to ensure schedulability, and the program team may need to use advanced models to analyze process behavior.

Programmatic risk identification and mitigation is concerned with the management aspects of the development lifecycle. If a program has multiple customers who are prone to having conflicting requirements, rapid-prototyping and user juries may be used as approaches to mitigate stakeholder involvement risks. If the product is dependent on other components or products that are developed simultaneously, the program may use cross-program tools such as employing an Interface Control Working Group to mitigate the risk of the inter-operating systems having deployment issues.

Operational risk identification and mitigation is concerned with improving business and mission effectiveness by developing and deploying capabilities that mitigate evolving operational risk. If a military unit is no longer able to detect a new weapon system developed by an adversary, operational risk increases, and operational needs are identified, highlighting the requirement for new capabilities to defeat the mission threat.

If the cost of operating multiple systems decreases the effectiveness or long-term viability of the operational organization, business needs are identified that require decreasing cost and operational complexity by integrating disparate systems into fewer systems.

The measure of effectiveness of any given systems engineering practice is the ability of that practice to mitigate technical, programmatic, and/or operational risk. Technical and programmatic risk identification and mitigation are the focus of most program and systems engineering risk management processes. When a program team has a mature risk management process, it continually identifies risks that may impact its ability to produce a product that meets customer requirements within cost and schedule constraints.

One missing aspect of most systems engineering risk management processes such as those described in the Guide to the Systems Engineering Body of Knowledge[3] or the INCOSE Systems Engineering Handbook[1] is a focus on operational risk. That is, the evolving risk to the business or mission needs of the end-user. This lack of focus on operational risk during the engineering process encourages the creation of a chasm between evolving need and delivered product capabilities. The longer the development process, the wider that gap, and the end-user may be less receptive to deeming the capability operationally effective.

Wrubel and Gross describe this disconnect, stating, *...requirements for any given system are highly likely to evolve* *between the development of a system concept and the time at which the system is operationally deployed as new threats, vulnerabilities, technologies, and conditions emerge, and users adapt their understanding of their needs as system development progresses*[4].

In his 2015 report to Congress about the state of Defense acquisition, the Honorable Frank Kendall, Under Secretary of Defense for Acquisition, Technology and Logistics, observed that the Department of Defense was optimizing cost and schedule performance over technical advancement. He stated ...*there is evidence that we have been pursuing less complex systems with about the same or less risk since 2009. This aligns with my concern that in some areas we may not be pushing the state-of-the-art enough in terms of technical performance. This endangers our military technical superiority. In my view, our new product pipeline is not as robust as it should be at a time when our technological superiority is being seriously challenged by potential adversaries. Not all cost growth is bad. We need to respond to changing and emerging threats*[5]*.*

These emerging threats, vulnerabilities, and technology changes increase operational risk. When the operational risk is great, end-users bypass the traditional engineering process and create more streamlined avenues to acquire capability.

During Operation Iraqi Freedom, the United States Army faced a new and evolving threat. Enemy forces were no match for a traditional military, so they relied on asymmetric tactics. Improvised Explosive Devices became the weapon of choice because they were easy to build and deploy and were highly effective. The Army wasn't prepared in terms of either detection and defeat systems or from a psychological perspective.

Coupled with an acquisition process that was too slow to react to the evolving operational threat and outcry from both service members and the general population, the Army created the Joint Improvised Explosive Device Defeat Organization (JIEDDO) with the sole purpose of defeating this new operational risk. JIEDDO was able to bypass the Army's acquisition process and get equipment and capabilities to the field quickly.

From a tactical perspective, the focus on defeating a specific operational risk was successful. Capabilities were fielded, and lives were saved. From a strategic perspective, these quickly-fielded systems lack certain longer-term quality attributes such as robustness, evolvability, and maintainability that would have been considered in a traditional systems engineering approach. The resulting capabilities increased total cost of ownership and logistical complexity[6].

When system requirements are created to reduce strategic risk such as affordability or other long-term efficiencies, the resulting systems could be viewed as less relevant from a tactical or operational perspective. The driving strategic requirements are associated with lifecycle cost reduction, reducing redundant systems, or integrating capabilities rather than mitigating near-term operational risk.

The Air Force’s Expeditionary Combat Support System had only a vague set of objectives when it began development in 2004[7]. According to a report by the United States Senate Permanent Subcommittee on Investigations, these objectives resulted in *...a new, fully-integrated logistics system that would replace an unspecified number of older, unconnected logistics systems*. This lack of clarity and disconnect between solving critical operational threats and risks resulted in $1.1 billion in wasted funding and a system that was not deployable.

According to Senator John McCain (R-Arizona), *The Air Force’s Expeditionary Combat Support System, or E.C.S.S., is a prime example of how a system designed to save money can actually waste billions of taxpayer dollars without producing any usable capability*[8].

To increase the effectiveness of systems engineering, its practices, methods, and tools, must have a greater emphasis on eliciting and understanding operational risk and the development of enhanced methods to continually track and react to evolving operational threat and risk during the development, deployment, and sustainment phases of the system lifecycle. To that end, this dissertation introduces an approach to influence systems engineering activities with the objective of improving the operability and acceptance of engineered solutions through the use of operational risk considerations.

It also explores the relationship between a focus on operational risk and program outcomes. This approach is referred to here as Operational Risk-Driven Engineering Requirements/Engineering Development (ORDERED) and is graphically shown in **Figure 1.**

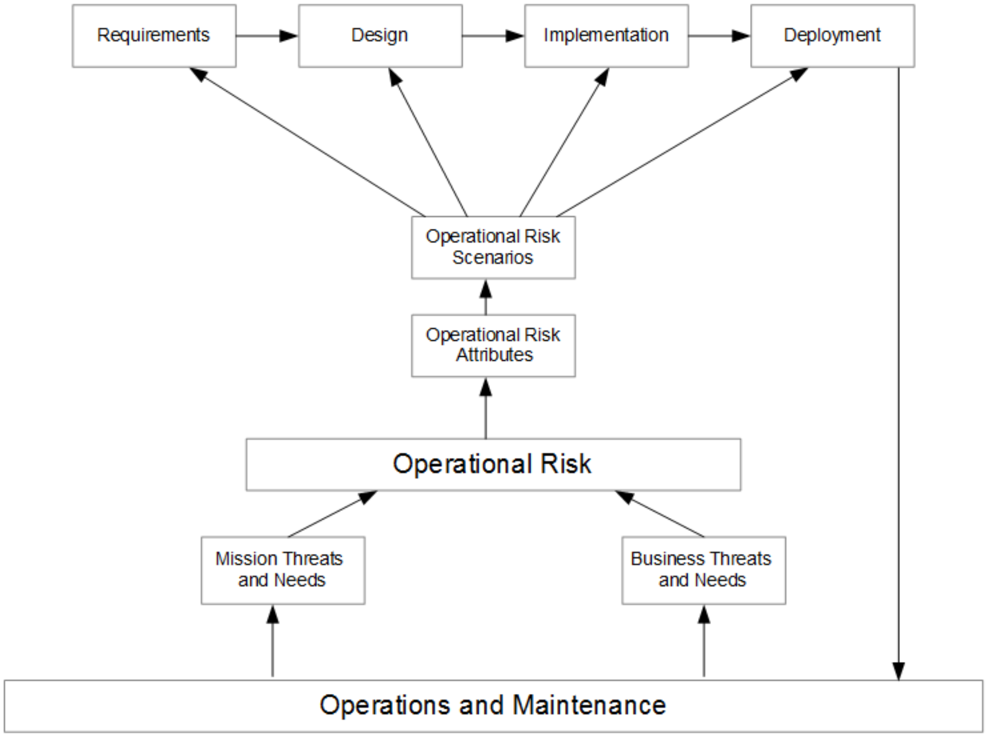

Requirements
Design
Implementation
Deployment
Operational Risk Scenarios
Operational Risk Attributes
Operational Risk
Mission Threats and Needs
Business Threats and Needs
Operations and Maintenance

Figure 1. Operational Risk-Driven Engineering Requirements/Engineering Development (ORDERED).

The ORDERED process starts in Operations and Maintenance whereas most systems engineering lifecycle models end in Operations and Maintenance. Ideally, new systems are developed to mitigate operational threats or needs. These needs arise from exploring both the mission aspects of operations as well as the business aspects of managing the operational organization.

Operational risks are identified that describe the gap between current operations and maintenance activities and the evolving mission and business threats and needs. Operational risks are then analyzed and operational risk scenarios developed.

Scenario-based engineering is a standard approach when developing complex systems to describe expected behavior or outcomes[9], however, operational risk scenarios as used in ORDERED describe unwanted behavior or outcomes. These scenarios are then used to inform systems engineering lifecycle activities to ensure that the capability or system under development mitigates evolving operational risk, increasing the operational acceptability of the capability or system when deployed.

Chapter 2 introduces basic risk management concepts and discusses how operational risk considerations are ignored in traditional risk management approaches. Chapter 3 describes the concept of operational risk, how the concept is considered traditionally in banking and military operations, and proposes a more general definition to apply to a wider set of operational organizations.

Chapter 4 discusses the relationship between operational risk and systems engineering activities and how a failure to consider evolving operational risk during system development may negatively impact program outcomes. Chapter 5 details the ORDERED process and how operational risk may be used to influence systems engineering activities as well as how systems engineering activities may be used to mitigate operational risk.

Chapter 6 illustrates the results of a survey constructed to measure the relationship between a focus on operational risk during the program lifecycle and resulting program outcomes. Chapter 7 introduces a simple model of operational risk and its relationship to technical debt and program cost.

Chapter 8 codifies the characteristics of an effective focus on operational risk during the systems engineering process and evaluates successful and challenged programs against these characteristics to validate the assertion that a focus on operational risk during the systems engineering process has a positive impact on program outcomes. Chapter 9 summarizes the results of the research and recommends areas requiring further exploration.

CHAPTER 2: RISK MANAGEMENT

Managing program risk is not a new concept. Engineers and program managers considered events, activities, processes, systems, and other impediments to success as soon as humankind began undertaking complex solutions to major challenges.

The wonder of an engineering accomplishment such as the Great Pyramids in Egypt stand as a testament to the ability of humankind to overcome great obstacles in building structures that appear to be unachievable given the tools, processes, methods, workforce, and environmental considerations at the time. While the Pyramids themselves have been the focus of restoration and archeological attention, the towns where these planners and workman lived provide insight into the planning, structure, and foresight required to accomplish these great engineering feats.

One particular city, Kahun, was built circa 1895 B.C., and its excavation illustrates the lives of the planners and workers who built the Pyramids. Kahun was part of a pyramid complex and was designed by a single architect, and its construction was purposeful[10], laid out to mitigate many obstacles facing the workers. The study of the process and methods of building pyramids sheds light into the risk mitigation activities applied during design and construction, such as complex irrigation systems employed to allow for ease of construction.

Massive canals were built to re-direct the Nile River to improve the ability to get raw materials close to the build sites, reducing the risk of program failure. In addition, political risks were considered and mitigated.

Similar to modern large-scale programs within the U.S. Department of Defense, where components are designed and developed in geographically disperse locations around the U.S. to garner support for the program, the pyramid builders also needed to collect political support and extend the reach of the Egyptian kings to the outer limits of the Egyptian empire.

The many logistical needs and raw materials required, including cooper, granite, limestone, and food, were transported from great distances within Egypt in order to show power and mitigate the risk of Bedouin warriors disrupting the program[11].

In 1857, Theodore Judah, a civil engineer, developed a detailed plan to build the Pacific Railroad[12]. While Judah's plan was more of a call to action for building the railroad, throughout his plan he introduced risks and proposed mitigation actions to convince financial backers of the viability of his plan. He didn't specifically use the term *risk*, but rather introduced threats to program success and plans of action to overcome these threats.

One threat he identified had to do with the unknowns of completing the program on time within a reasonable cost. To mitigate this threat, he proposed an incremental approach to building the railroad, starting at both ends and measuring actual progress, allowing for incremental decision points to continue the program, discontinue, or adjust the plan.

This concept is also included in the more recent Incremental Commitment Model[13], which uses risk-driven anchor-point milestones rather than traditional systems engineering design reviews to allow for making a feasibility decision about continuing a program.

Another threat to the Pacific Railroad that Judah identified had to do with the lack of infrastructure required along the chosen route. He proposed to mitigate this threat by first building a wagon road along the route to allow for settlement prior to construction. The wagon road with settlements and depots along the route would also mitigate another threat that he identified: the danger posed by hostile Indians destroying the railroad.

He argued that settlement along the wagon route would deter attacks and stated, *What more terrible rod of power we hold over these Indians—the power to concentrate hundreds, ney, thousands of men in a few hours upon any desired point? How much harm could they do before the fighting train would be upon them at* *the rate of fifty miles an hour?* Judah's plan not only proposed the approach to build the Pacific Railroad, but identified threats, or what we would today call risks, to achieving the plan and mitigation actions required to overcome the threats.

These early examples provide insight into the minds of early planners and engineers and how they considered potential negative outcomes and implemented action plans to increase the likelihood of program success.

However, risk management today is a large field of study. It includes research in mathematical notations of probability, finding and quantifying cause and effect relationships between human behavior or environmental influences and their health impact, financial and economic applications, optimizing insurance levels and cost, human safety analysis, supply chain risk, as well as many other applications[14, 15, 16].

Risk management, as a formal program management and engineering process as applied to the engineering of complex systems, emerged after World War II[17]. Mehr and Hedges[18] codified the basic concepts of risk management in 1963, after seven years of research and writing, and included details about analyzing and handling risks to a business enterprise.

Today, risk management as a program management and engineering practice is commonplace[19]. The Project Management Institute's Project Management Body of Knowledge includes project risk management as one of its ten knowledge areas, highlighting its importance as equal to areas such as scope, cost, schedule, and quality management[20].

The Capability Maturity Model Integration (CMMI) includes risk management as a process area, and organizations are required to demonstrate competence in program-level risk management in order to achieve a maturity level 3 rating[21]. The Guide to the Systems Engineering Body of Knowledge includes risk management as a topic within the systems engineering management knowledge area and discusses the overlap between systems engineering and program management within the program's overall risk management process[3].

The Department of Defense requires all program managers to manage risk[22] and has developed a detailed guidebook to assist program managers in the activities required to manage program risk[23].

Even with the evolution of risk management as a standard engineering and management process, not all high-risk and critical programs have effective risk management processes in place. The National Aeronautics and Space Administration (NASA) recently reported that over half of the programs that it examined in a deep-dive assessment had significant weaknesses in their risk assessment processes[24].

Simply having a risk management process in place is not sufficient. Programs need to have a continual focus on the most critical risks to program success. These most critical risks go beyond meeting cost and schedule constraints or overcoming technical challenges.

Some of the most challenging risks facing a systems engineering team are associated with ensuring that the capabilities delivered actually satisfy the real operational need and that as the operational need evolves during the systems engineering lifecycle, the team is able to identify these changes and react to the shift in need. Ignoring these considerations increases operational risk for the end-user of the capability and decreases the likelihood that the end-user would consider the capability operationally effective.

CHAPTER 3: OPERATIONAL RISK MANAGEMENT

Operational risk management is widely practiced in the banking industry and in military operations. While some of the concepts and definitions are common, the purpose and approach are unique depending on the application.

In the banking industry, operational risk management focuses on mitigating catastrophic financial loss at an institution and limiting the propagation of that loss to other banks and across international boundaries. In the military, operational risk has a heavy emphasis on safety hazards and their impact on mission outcomes. Both of these applications of operational risk management form a foundation for a more comprehensive treatment of operational risk.

3.1 OPERATIONAL RISK IN THE BANKING INDUSTRY

Operational risk management within the banking industry is focused on the goal of reducing the probability of loss due to events such as fraud, mismanagement, system failures, failed investments, or legal considerations[25]. Banks estimate their risk exposure, establish mitigation activities, and set aside financial reserves to cover such loss. The banking system is international in that loss and risk aren’t confined to a single bank or country but have broader impacts to the world economy.

In 1930, the Bank for International Settlements (BIS) was established in Basel, Switzerland. It is an international organization with shareholders consisting of central banks and other monetary authorities. The purpose of the BIS is to foster monetary and financial stability and international cooperation among central banks.

Military tensions in the 1930s reduced cooperation between countries, and the BIS was instrumental in moving more than one hundred and forty tons of gold out of the European central banks for safe keeping as part of the goal to ensure international financial stability. After World War II, the BIS became the international forum for the central establishment and control of banking standards[26].

The Group of Ten (G-10) consists of eleven industrialized nations that meet on an annual basis to discuss and cooperate regarding international financial matters[27]. After several high visibility bank failures in 1974, including the collapse of Bankhaus Herstatt in Germany and the Franklin National Bank in the United States, the G-10 asked the BIS to establish the Basel Committee on Banking Supervision. The Basel committee established standards for international banking focused on risks incurred by international banks to limit the spread of financial failure in times of crisis[28].

These standards evolved over years of collaboration and were known as the Basel Accord (1988), Basel II (2004), and Basel III (2010). The term *operational risk* emerged during this time and became the leading approach for managing banking institution risk in the 1990s[29].

The Basel committee established a framework for managing financial risk using operational risk management as the central expectation for banks to implement. It defined operational risk as *the risk of loss resulting from the inadequate or failed internal processes, people, and systems or from external events.* This definition included legal risk and published a set of principles and a framework for managing operational risk[30].

The Basel definition of operational risk is general enough to apply to other industries and applications of operational risk management, however, the principles are focused on the banking industry. They require banks who comply with the framework to establish a robust operational risk management approach with expectations placed on the board of directors and senior management as well as process expectations for continuous operational risk identification, mitigation, and reporting.

The Basel operational risk management principles are shown in **Table 1**. The Basel operational risk management principles emerged to address banking risk and were established in times of crisis to avert future global financial loss. As such, they are

Table 1. Basel Operational Risk Principles

Principle Category	Principle Text
Fundamental Principles Of Operational Risk Management	**Principle 1:** The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behavior. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organization.
	Principle 2: Banks should develop, implement, and maintain a Framework that is fully integrated into the bank’s overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity, and risk profile.
Governance - Board of Directors	**Principle 3:** The board of directors should establish, approve, and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes, and systems are implemented effectively at all decision levels.
	Principle 4: The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.
Governance - Senior Management	**Principle 5:** Senior management should develop for approval by the board of directors a clear, effective, and robust governance structure with well defined, transparent, and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organization policies, processes, and systems for managing operational risk in all of the bank’s material products, activities, processes, and systems consistent with the risk appetite and tolerance.

Risk Management Environment - Identification and Assessment	**Principle 6:** Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes, and systems to make sure that the inherent risks and incentives are well understood.
	Principle 7: Senior management should ensure that there is an approval process for all new products, activities, processes, and systems that fully assesses operational risk.
Risk Management Environment - Monitoring and Reporting	**Principle 8:** Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.
Risk Management Environment - Control and Mitigation	**Principle 9:** Banks should have a strong control environment that utilizes policies, processes, and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.
Business Resiliency and Continuity	**Principle 10:** Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.
Role of Disclosure	**Principle 11:** A bank’s public disclosures should allow stakeholders to assess its approach to operational risk management.

unique to the banking industry. However, the concepts are sound and at a higher level of abstraction apply more broadly.

As financial institutions become more complex through regulation changes or diversification of services offered, operational risk increases, and the need for a broader discussion of operational risk increases as well[31]. The Basel principles are generalized and shown in **Table 2.**

Table 2. Basel Principles Generalized

Basel Principles Generalized
Principle 1: Establish a strong operational risk management culture
Principle 2: Integrate operational risk considerations into overall operations
Principle 3: Ensure that operational risk management is implemented effectively
Principle 4: Define the components of risk exposure based on operational needs
Principle 5: Establish an operational risk management strategy
Principle 6: Continuously identify and assess operational risk based on ongoing operational activities
Principle 7: Identify and assess operational risk when adopting new systems or processes
Principle 8: Monitor and report operational risk exposure to operational leadership
Principle 9: Establish and implement mitigation strategies for the most critical operational risks
Principle 10: Implement resiliency and continuity plans to ensure ongoing operations in the event of severe operational disruption
Principle 11: Ensure that key stakeholders participate in operational risk activities

Power suggests that operational risk management is still a relatively new field of study within the banking industry and states, *Definitions of key concepts are an intimate and central part of the logic of any practice; without a system of concepts and taxonomies, any practice of intervention is blind, disorganised and of questionable legitimacy*[29].

Moving toward a more general application of these concepts may assist any operational organization in establishing and maintaining a comprehensive operational risk management process that focuses on mitigating mission and business risks.

3.2 OPERATIONAL RISK IN THE MILITARY

Military operations involve weighing the risk of taking action against the risk of inaction. Colonel John Boyd, United States Air Force, wanted to understand why U.S. fighter pilots were more successful in combat while flying the F-86 fighter aircraft as opposed to pilots flying the Mig-15, a more technologically advanced aircraft, during the Korean conflict.

His research concluded that U.S. fighters were able to cycle through a four-step decision process more quickly than their adversaries. This cycle of observe, orient, decide, and act became known as the OODA-loop and was adapted beyond Air Force fighter pilots into ground and naval operations[32]. Inherent in the OODA-loop cycle is identification and mitigation of operational risk.

While the fighter pilot's OODA-loop is executed in mere seconds, the process of making decisions using the OODA-loop in a military context applies equally for mission-planning activities and long-term strategic planning and involves identifying and mitigating operational risk. Accommodating uncertainty and allowing flexibility in execution is more conducive to improving mission outcomes and decreasing safety-related risks[33].

The U.S. Marine Corps defines operational risk management as *The process of identifying and controlling hazards to conserve combat power and resources*[34]*.* The U.S. Navy defines operational risk management in OPNAV INSTRUCTION 3500.39B as *The process of dealing with risk associated within military operations, which includes risk assessment, risk decision making and implementation of effective risk controls*[35]*.*

The U.S. Air Force removed the word *operational* from its guidance document and prefers the more generic term *risk management*. Its definition of risk management is *a decision-making process to systematically evaluate possible courses of action, identify risks and benefits, and determine the best course of action for any given situation*[36]*.* While the definition includes *for any given situation*, the emphasis within the guidance document on risk management is on addressing personnel health, safety, and environmental factors.

The U.S. Army includes guidance for the management of risk in operational contexts within ATP 5-19 and defines risk management as *The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits*[37]*.*

The focus of operational risk in the Marine Corps, the Navy, the Air Force, and the Army is on identification and elimination of hazards. The Navy defines a hazard in 3500.39B as

Any real or potential threat that can cause personal injury or death, property damage or mission degradation, *or damage to environment*. The Navy identifies its operational risk management process in four steps: Identify Hazards, Assess Hazards, Make Risk Decisions, and Implement Controls.

The Army includes the same four steps, adding Supervise and Evaluate as a fifth step. The increase of asymmetric threats in combat, that is an unpredictable enemy using unconventional means to attack a more conventional force, increases the emphasis on safety and hazard mitigation on the battlefield[38].

Similar to the approaches found in the military services, NASA uses a Risk-Informed Safety Case approach to support the claim that NASA operations are conducted in a safe manner, free from operational safety-related hazards[97].

This emphasis on hazards rather than on a more general definition of operational risk narrows the handling of potential operational risk to the identification of safety-related risks and ignores other operational attributes that contribute to mission or business degradation.

3.3 OPERATIONAL RISK EXPANDED

The concepts and application of operational risk management in banking and military operations provides a foundation for a more comprehensive treatment of operational risk. The structure and discipline established in a continuous process of identifying risks or hazards and establishing proactive mitigation plans to address these risks is fundamental to addressing operational risk.

However, the narrow focus within both the banking industry on financial risk and within the military on safety hazards decreases the potential effectiveness of operational risk activities. The more inclusive definition of operational risk and operational risk management is shown in **Table 3**.

Table 3. Operational Risk Definitions

Operational Risk	*The possibility of suffering mission or business loss.*
Operational Risk Management	*An operational practice with processes, methods, and tools for managing risks to successful mission and business outcomes.* *It provides a disciplined environment for proactive decision making to:* *- continually assess what could go wrong (operational risks)* *- determine which operational risks are most important to deal with, and* *- implement strategies to address operational risk*

With this more general yet comprehensive definition, operational organizations may explore operational risks[39] beyond those related to financial risk as practiced in the banking industry and safety hazards as explored in military contexts. Any risk to the successful accomplishment of mission or business outcomes may be identified and addressed.

A detailed operational risk taxonomy is presented in Appendix A, with the goal of assisting operational organizations in exploring potential sources of risk to both mission execution and longer-term business viability and continuity.

CHAPTER 4: OPERATIONAL RISK AND ENGINEERING ACTIVITIES

Requirements development and management is one of the earliest and most critical activities in the systems engineering lifecycle. It represents the bridge between the operational need and the potential solution space. Even when the rest of the systems engineering activities are performed with effectiveness, solving the wrong problem will increase the likelihood of rejection of the system by the end-user and late lifecycle cost increases.

In 2008, Carnegie Mellon University and the National Defense Industrial Association developed a study to determine whether systems engineering practices had an impact on program performance (cost, schedule, scope) of defense systems[40]. It was not an easy question to answer, as there were few studies specifically aimed at correlating systems engineering practices and program outcomes.

The authors found that across the defense industry, among contractors who participated in the survey, there wasn't a common definition of the activities included in their respective systems engineering approaches. Some companies included engineering management activities such as risk management and planning in their definition while others had a narrower definition of systems engineering and even excluded later lifecycle activities such as integration and testing in how they defined systems engineering.

In constructing their approach to gathering data, the team decided to focus on the major activities of systems engineering rather than the topic as a whole. They devised a survey instrument that asked systems engineers and program managers about the effectiveness of eleven systems engineering practices within their program and also on program outcomes such as schedule and cost variance. They found sixty-four programs across defense industry companies willing to participate in the survey.

The research continued through 2012 as the team looked to obtain quantitative evidence of the benefit of systems engineering best practices on program performance[2]. It also explored team experience, program challenges, and their relationship to program success. **Figure 2** presents the summary of the team's findings with the systems engineering activity on the y-axis and the correlation, represented by Gamma score, on the x-axis.

Gamma values of zero indicate a non-existence or weak relationship. Gamma values near 1 represent a strong positive relationship, while Gamma values near -1 represent a strong negative relationship. If a systems engineering practice has a positive Gamma value, program performance and the effectiveness

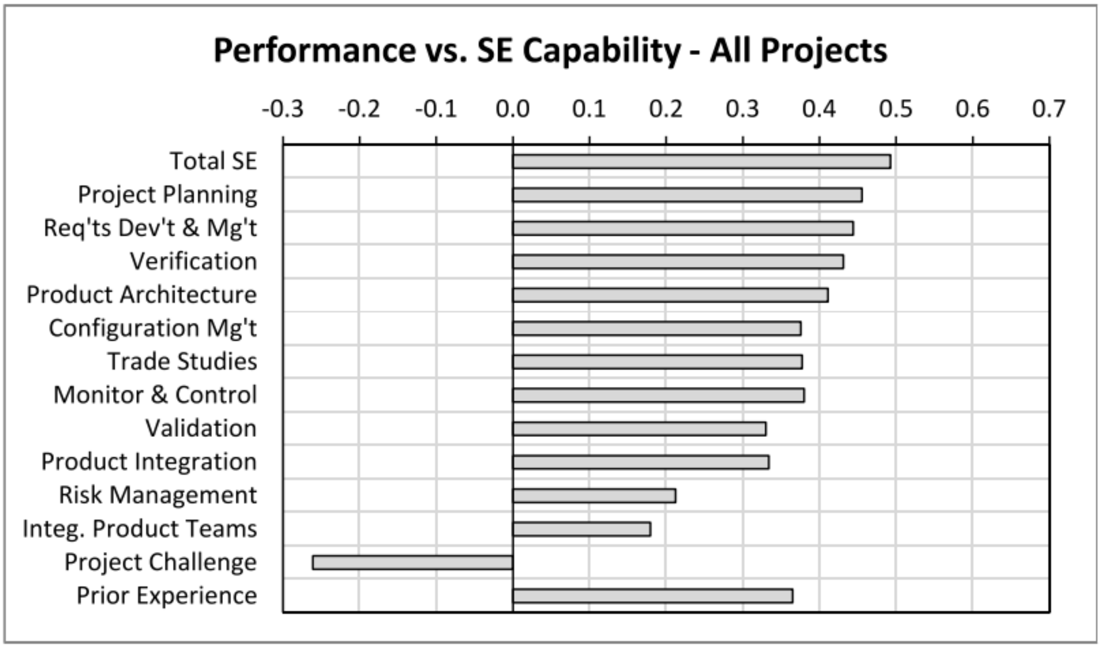


Figure 2. Program Performance versus SE Capabilities and Drivers.

of that practice move in the same direction. While this relationship does not indicate causation, it does support the researcher's conclusion that *projects that properly apply systems engineering best practices perform better than projects that do not*.

Requirements activities represents one of the highest Gamma values, second only to project planning. This supports the argument that requirements development and management is one of the most critical systems engineering activities impacting program outcomes.

As shown in **Figure 3**, the Gamma value of 0.44 indicates a strong supporting relationship between requirements engineering activities and program performance. The percentage of programs

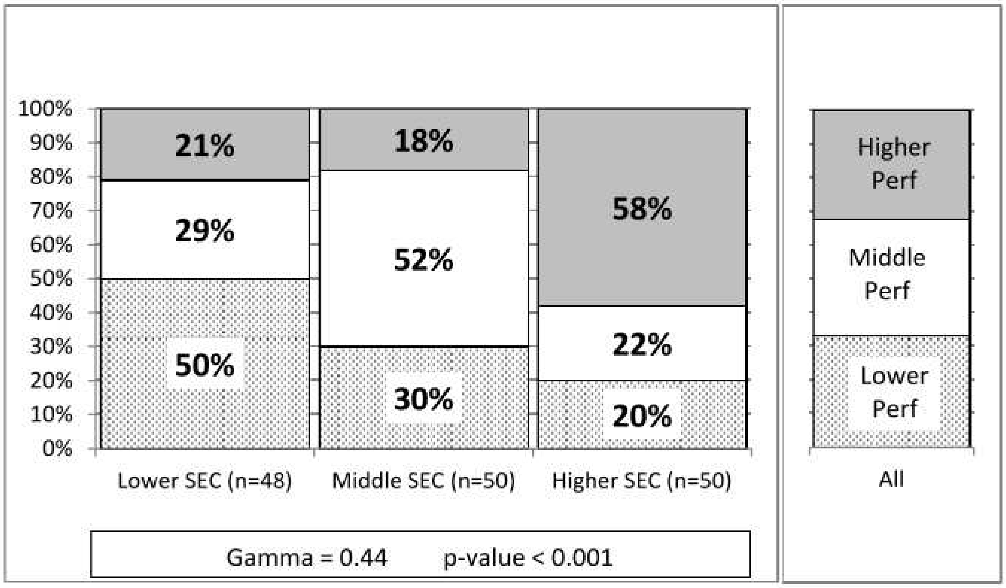


Figure 3. Correlation between Requirements Effectiveness and Program Performance.

delivering higher performance increased from 21 percent to 58 percent as the effectiveness of their requirements engineering practices increased from lower to higher.

While this study highlights the importance of applying systems engineering activities to increase the likelihood of program success, it does not explore the relationship between an operational risk focus and program outcomes. Examining studies of program failures highlights this relationship.

One study by the Rand Corporation explored the relationship between the cost of complex system development and the uncertainty of requirements[41]. The authors of the study argue that operational risks may drive uncertainty and that urgent operational needs might cause a program to be accelerated or more end units produced than planned.

This type of churn in requirements and in funding causes costs to increase and requires re-work in lifecycle engineering activities and artifacts. The Rand study also points out that a lack of participation by operationally focused stakeholders creates disconnects when the system is tested against operational needs.

In several system development programs, the authors recognized that *...requirements and capabilities were set by planners and promised by the acquisition community, but there was great difficulty in testing them during operational test and evaluation*. These difficulties are driven by long acquisition timelines during which operational risks and mission threats influence the operational need.

The real operational need when the system enters operational test and evaluation has evolved, but the operational need statement, which may have been baselined years earlier, remains stagnant. The tension between long-standing engineering methods expecting well-defined and stable requirements and the rapid evolution of operational need requires newer methods for including an ongoing review of operational risk and mission threats and mechanisms for inserting this new understanding into the system baseline to allow systems to remain relevant.

The Nunn-McCurdy Act was a provision in the 1983 defense authorization bill[42] in which the intent was to force a notification of Congress and to initiate a review of major weapon system acquisition programs if they exceeded their Acquisition Program Baseline by certain thresholds. This is commonly referred to as a Nunn-McCurdy breach.

The review is intended to evaluate whether the program is worth continuing or if the program should be canceled. While a Nunn-McCurdy breach is a good mechanism for reviewing the efficacy of a program, the review is late-to-need. As former Senator John Tower, then Chairman of the Senate Armed Services Committee, pointed out during the initial debate of the provision, this is like *closing the gate after the horse has galloped off into the boondocks*[43].

Finding the root cause(s) of a Nunn-McCurdy breach may be challenging. As an old proverb states, *success has many fathers, while failure is an orphan*[44].

Commissioned by the Office of the Secretary of Defense, a Rand study explored the issues that led to such breaches[45]. The study examined the Army’s Excalibur program, a munitions system that provides for precision fires in artillery munitions, and the Navy’s Enterprise Resource Planning (ERP) program, which was designed to serve as the technical backbone for the maintenance, financial, and supply functions of the Navy.

The root causes for breaches identified in the Excalibur program were changes in procurement quantities driven by operational requirements changes and affordability considerations, inaccurate estimates, concept and technological changes, and minor technical issues. The concept and technological changes occurred between the initial solicitation and contract award.

Urgent operational needs to support Operation Enduring Freedom/Operation Iraqi Freedom caused production to be accelerated and more Increment 1A rounds to be produced than initially planned. This is an example of how operational risk and mission threats may drive the need to evolve requirements after programs have baselined requirements.

The Navy's ERP system was initiated in 2003 and fully started in 2004. The program was re-baselined in 2006 at an increase of $400 million. The increase was necessitated by a re-design of the system, a change in business practices, and an improvement in estimates.

Major shifts in the way that the Navy was organized moved intermediate maintenance activities to regional maintenance activities and caused major re-design issues. Identifying operational risk and evolving mission needs during early requirements activities could have highlighted the need to include growth and exploratory scenarios into the requirements engineering process and might have led to a more flexible design that could have withstood this operational change.

After examining the Excalibur and the Navy ERP root causes of failure, the author recommended a framework for thinking about critical program features. *An initial conceptual framework would allow a decision maker to quickly determine what is most critical, complex, or least understood of the list of program features*. He recommends an approach that characterizes technical complexity of functional requirements.

However, he does not look at quality attributes such as evolvability, flexibility, and adaptability to operational risk and mission changes. The author recognizes that operational risk and mission threats influence operational need and even states, *...as the needs of the battlefield evolve, so will the demand for integrated, better, and faster technologies.* But the focus is primarily on technical risk of components already selected or designed, not on assessing evolving operational risk and its impact on system or sub-system requirements or the selection or design of components. Addressing operational risk factors this late in the development lifecycle leads to re-work and cost impacts.

The Space Based Infrared System (SBIRS) is a key part of the future missile alert system for the United States[46]. When fully operational, it will provide monitoring of ballistic missile launches anywhere in the world at any time. It is also one of the most challenging programs undertaken with cost growth estimated at over 400 percent[47].

The cost overruns have been attributed to immature technologies, complex requirements, and unrealistic cost estimates[48]. The program began in 1996 with a contract awarded to Lockheed Martin for $2.3 billion. By 2012, the cost of the program grew to nearly $14 billion, as shown in **Figure 4**, as reported in Program Office Status Reports, and by 2014 costs were estimated at $17 billion[47].

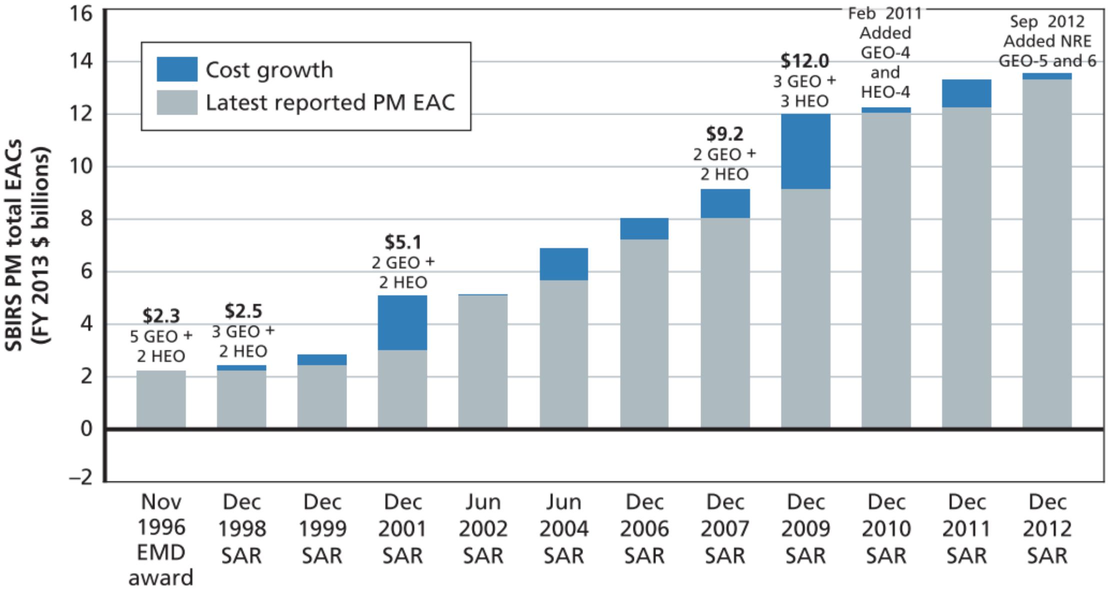


Figure 4. SBIRS Cost Growth as Reported in Program Office Status Reports

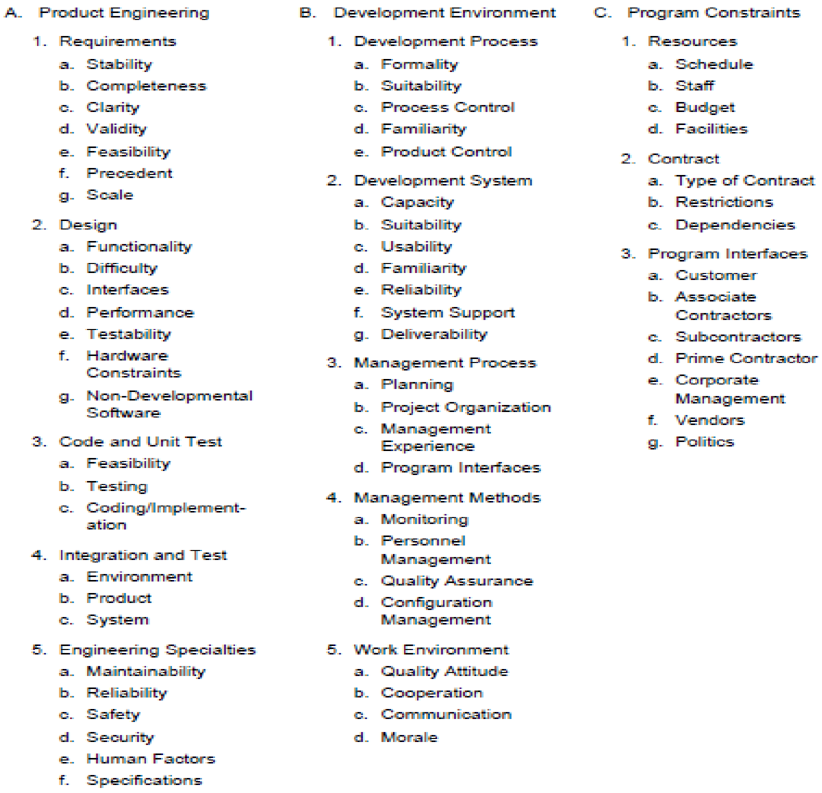
The SBIRS program's first Nunn-McCurdy breach was declared in 2000 when the program failed to meet the initial operational capability date for Increment 1 Ground in late 1999. Brent Collins, then Air Force Program Executive Officer for Space, assembled a team to review the program.

I was asked to lead the technical review team investigating the contractor’s development activities and progress at its primary software development location in Boulder, Colorado, and the operational site at Buckley Air Force Base in Aurora, Colorado.

The team included members from the Software Engineering Institute, Aerospace Corporation, MITRE, Air Force Audit Agency, Defense Contract Management Center, and Lockheed Martin. During a planning meeting before the investigation, I asked Mr. Collins to articulate what success would look like for the program. He stated that achievement would be *successful certification of Increment 1 on the mutually-agreed-upon re-structure date with a subordinate goal of successful entry into Initial Operational Test and Evaluation*[49]. The team decided to conduct a risk assessment following the Software Risk Evaluation (SRE) method developed by the Software Engineering Institute[50].

The SRE method uses a detailed software development risk taxonomy that provides a structure for identifying and classifying risks[51]. While the taxonomy was developed to address risks related to software development programs, the topics and structure are written generically enough to apply more broadly.

Figure 5 shows the overall structure of the taxonomy with three major *classes*: Product Engineering, Development Environment, and Program Constraints. These three categories equate to what the program is building (Product Engineering), how the team chooses to operate (Development Environment), and external forces (Program Constraints).



A. Product Engineering

1. Requirements
   a. Stability
   b. Completeness
   c. Clarity
   d. Validity
   e. Feasibility
   f. Precedent
   g. Scale
2. Design
   a. Functionality
   b. Difficulty
   c. Interfaces
   d. Performance
   e. Testability
   f. Hardware Constraints
   g. Non-Developmental Software
3. Code and Unit Test
   a. Feasibility
   b. Testing
   c. Coding/Implementation
4. Integration and Test
   a. Environment
   b. Product
   c. System
5. Engineering Specialties
   a. Maintainability
   b. Reliability
   c. Safety
   d. Security
   e. Human Factors
   f. Specifications

B. Development Environment

1. Development Process
   a. Formality
   b. Suitability
   c. Process Control
   d. Familiarity
   e. Product Control
2. Development System
   a. Capacity
   b. Suitability
   c. Usability
   d. Familiarity
   e. Reliability
   f. System Support
   g. Deliverability
3. Management Process
   a. Planning
   b. Project 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

C. Program Constraints

1. Resources
   a. Schedule
   b. Staff
   c. Budget
   d. Facilities
2. Contract
   a. Type of Contract
   b. Restrictions
   c. Dependencies
3. Program Interfaces
   a. Customer
   b. Associate Contractors
   c. Subcontractors
   d. Prime Contractor
   e. Corporate Management
   f. Vendors
   g. Politics

Figure 5. SEI's Software Development Taxonomy.

The next level contains *elements* such as Requirements, Design, and Resources. The lower level of the taxonomy structure contains *attributes,* which are the risk concerns associated with each *element*.

For example, the *attributes* to explore for risk identification or classification under the *element* of *Requirements* would be Stability, Completeness, Clarity, Validity, Feasibility, Precedent, and Scale. Discussing the elements of the taxonomy with program team members is a good way to explore possible program risks and may help expand potential sources of risk beyond a team's collective experience. In addition, a taxonomy may help de-personalize risk identification and allow team members to focus on objective definitions of the attributes rather than trying to place blame or argue over word definitions.

During the SBIRS Increment 1 technical review, the taxonomy was useful in exploring areas of program risk with the engineering team in a non-threatening approach. In a five-day period we interviewed thirty-one team members, identified one hundred sixty-nine individual risk statements, and affinity-grouped them into fifteen risk areas[49]. One of the major risk areas was described as Requirements Uncertainty.

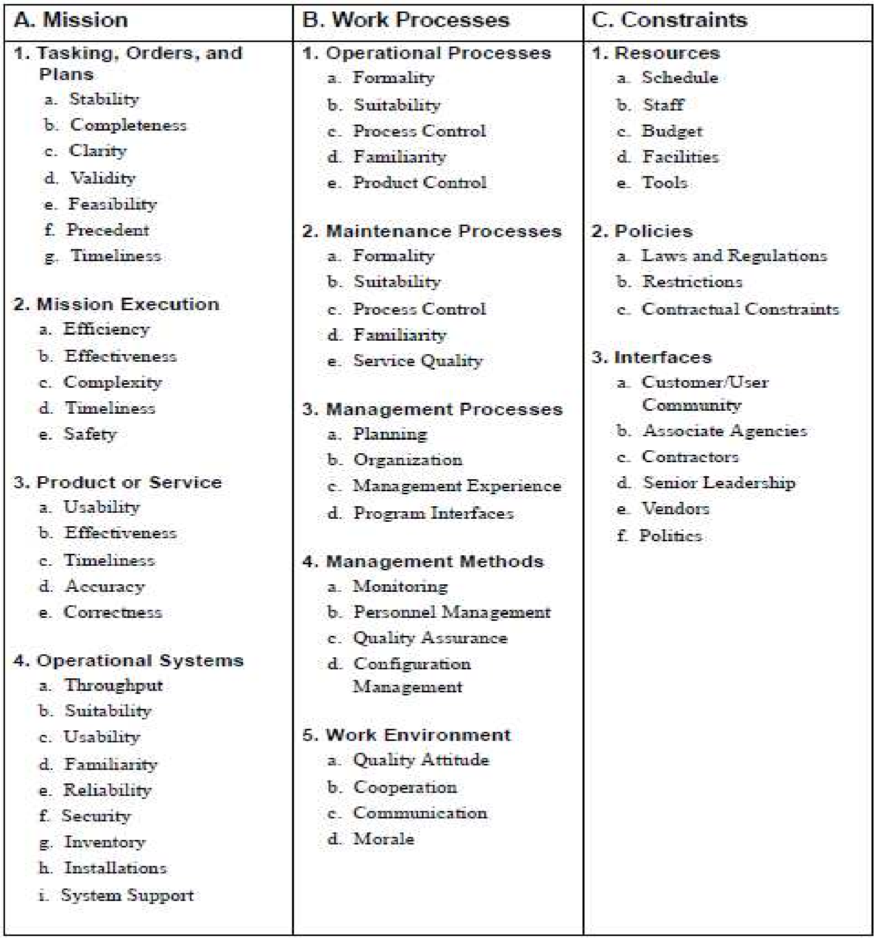
The program was experiencing disconnects between the expectations of the engineering team and the operational team. Disconnects such as these arise when the operational need or mission threat is either not well understood or has evolved during development activities, and the changes were not incorporated into development activities and are not reflected in the deployed system.

The second interview site was the SBIRS operational facility. The facility was located at Buckley Air Force Base, and the end-users were mostly officers and enlisted members of the United States Air Force. The operators were highly-trained and educated men and women, yet most of them were not engineers and didn’t understand the systems engineering activities required to develop a complex system.

One example of this disconnect has to do with defect discovery and removal. The SBIRS development team wanted more test time at the operational site to find and remove defects. Finding and removing defects as the system moves from a development environment through various integration and test environments and finally into the operational environment is a standard systems engineering approach. It allows the development team to grow system reliability and to gain confidence in system performance supporting deployment decisions[52].

SBIRS operators, on the other hand, spent their time operating systems that have to work every time. As one operator stated, *The system has to work, or people will die. I don’t understand why they are finding defects*.

Given this difference in perception, the assessment team decided that using the software development taxonomy wasn’t the right tool for eliciting risks. Having recently taught risk management courses at several overseas operational locations, I sketched the beginnings of what was eventually published as the Taxonomy of Operational Risks[53]. The team tested the operational risk taxonomy during interviews at Buckley Air Force Base, as shown in **Figure 6**.



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	**1. Operational Processes** a. Formality b. Suitability c. Process Control d. Familiarity e. Product Control	**1. Resources** a. Schedule b. Staff c. Budget d. Facilities e. Tools
2. Mission Execution a. Efficiency b. Effectiveness c. Complexity d. Timeliness e. Safety	**2. Maintenance Processes** a. Formality b. Suitability c. Process Control d. Familiarity e. Service Quality	**2. Policies** a. Laws and Regulations b. Restrictions c. Contractual Constraints
3. Product or Service a. Usability b. Effectiveness c. Timeliness d. Accuracy e. Correctness	**3. Management Processes** a. Planning b. Organization c. Management Experience d. Program Interfaces	**3. Interfaces** a. Customer/User Community b. Associate Agencies c. Contractors d. Senior Leadership e. Vendors f. Politics
4. Operational Systems a. Throughput b. Suitability c. Usability d. Familiarity e. Reliability f. Security g. Inventory h. Installations i. System Support	**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	

Figure 6. SEI's Taxonomy of Operational Risks.

Similar to the development taxonomy, the operational risk taxonomy contains *classes*, *elements*, and *attributes*. The classes are organized into areas related to the mission or missions performed by the operational organization (Mission), the way that the operational organization chooses to perform the mission or missions (Work Processes), and external forces (Constraints).

The taxonomy proved to be a good mechanism to elicit risks from operational users, and over a two-day period the team was able to elicit seventy risk statements, which were grouped into eight risk areas[54]. One of the major risk areas identified by the operational users was Requirements. The end-users were concerned that the requirements management process failed to adequately capture system capabilities and expectations.

They were also concerned that some requirements were more stringent than operationally required and that the development contractor would have difficulty achieving these requirements. The practical use of the operational risk taxonomy helped evolve the work to its current state and publication.

These case studies have shown the importance of a continued focus on operational risk and mission threats during the systems engineering lifecycle to ensure that the end product meets the evolving needs of operational users. However, there are few methodologies or approaches that explicitly include operational risk considerations during the systems engineering lifecycle.

Chapter 5 offers one such approach with the goal of using a continual focus on operational risk as a means to improve the effectiveness of the systems engineering process.

CHAPTER 5: OPERATIONAL RISK-DRIVEN ENGINEERING REQUIREMENTS/ENGINEERING DEVELOPMENT

This chapter introduces a repeatable method designed to influence systems engineering activities through exploration and management of operational risk throughout the systems engineering lifecycle. The approach outlined is called Operational Risk-Driven Engineering Requirements/Engineering Development (ORDERED).

5.1 INTRODUCTION

Operational Risk-Driven Engineering Requirements/Engineering Development is a repeatable method designed to influence systems engineering activities throughout the systems engineering lifecycle with the purpose of improving program outcomes and system operability and usability. New or enhanced capabilities are driven by mission and business needs of diverse stakeholders[55].

Mission and business needs increase operational risk when gaps in current capabilities fail to address these needs. As new capabilities are developed, mission and business needs evolve, increasing the operational risk that the new capability will fail to address these changes. The ORDERED method ensures that program requirements and development activities are enacted with a thorough consideration of operational risk concerns.

ORDERED is not intended to replace a program’s current set of engineering methods, but rather to augment the current approach with operational risk considerations. **Figure 7** presents a high-level overview of the ORDERED method.

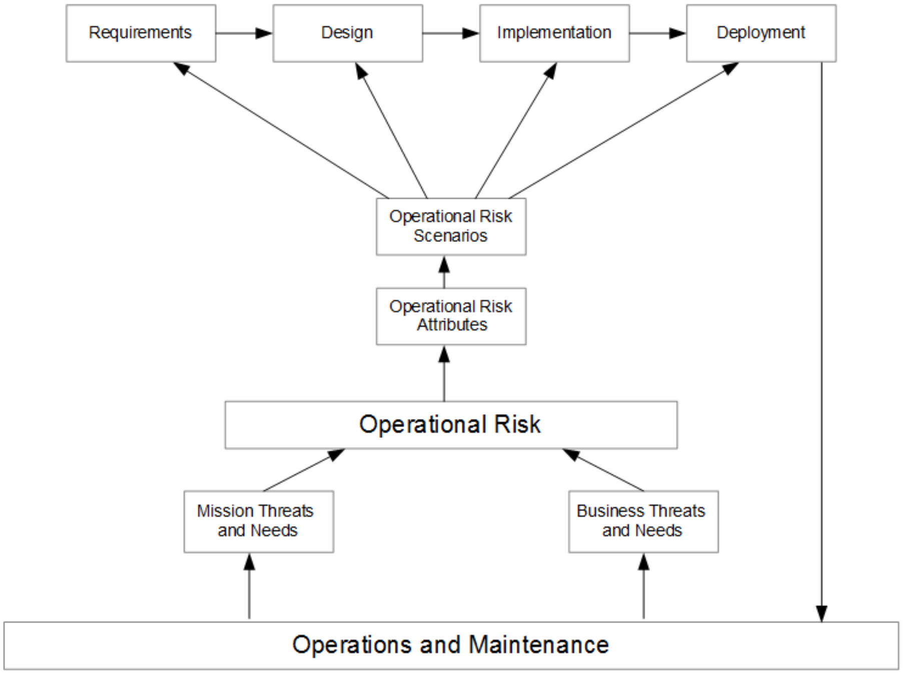

Requirements
Design
Implementation
Deployment
Operational Risk Scenarios
Operational Risk Attributes
Operational Risk
Mission Threats and Needs
Business Threats and Needs
Operations and Maintenance

Figure 7. ORDERED Method.

Mission and business threats and needs are derived from current operations and maintenance activities. The gap between needs and threats and current systems and operational processes generates operational risk. Operational risk is captured in the form of individual risk statements and may be grouped into operational risk areas.

These risks or risk areas define the negative impact of what could go wrong, essentially the mission or business *loss* that may be realized. Operational risk attributes are derived from the risks. These attributes are characteristics of the system or capability.

Operation risk scenarios are developed to further describe the risk in terms of the environment, behavior, and outcomes that would negatively impact mission or business objectives. The scenarios are then used during the systems engineering process to inform activities such as requirements development, architecture and design development, implementation decisions, test and acceptance case development, and deployment strategies and approaches.

As mission and business needs and threats evolve, operational risks are continuously identified, their attributes identified or refined, and scenarios are developed or updated. Mechanisms to incorporate this evolved understanding of mission and business needs into the program baseline should be included into the agreement between the customer and the developer. The shorter time between discovery of new operational risk-driven changes and incorporation of those changes into the program baseline, the more likely systems engineers will be able to influence engineering activities before committing to requirements, design, architecture, or component level decisions.

5.2 BASIC CONCEPTS OF OPERATIONAL RISK

For the purpose of ORDERED, operational risk is defined simply as the *possibility of suffering mission or business loss*. An operational organization is any group of individuals teamed together with a common purpose to carry out a mission. A mission is comprised of a specific task or set of tasks carried out by operational personnel[56]. Tasks may be described as either mission-essential or mission-support[57].

Mission-essential tasks directly contribute to mission execution. For example, if the operational organization was a community fire department, mission-essential tasks could include emergency response, firefighting, and rescue tasks. Mission-support tasks could include equipment maintenance, training, and fire prevention awareness.

Mission risks may be driven by any number of conditions, such as events, activities, processes, and systems that could impact the operational organization’s ability to perform its mission or could negatively impact the full accomplishment of the mission. The impact is tactical in that the mission is impacted directly.

Business risks are also driven by similar conditions, but the impact is more strategic. A flat-tire on a fire truck is a risk to performing the mission task of fighting fires, and therefore, may be described as a mission risk. A lower tax-base in a community may impact the fire department's ability to perform preventive maintenance or hire and train future firefighters, and therefore, could be described as a business risk. This distinction is valuable when identifying operational risk.

When the focus is solely on immediate mission risks, longer-term considerations such as affordability or long-term viability of the organization are ignored. When the focus is solely on business risks, mitigation actions or system solutions may not be operationally effective in the short-term. The balance between mission and business considerations helps ensure that solutions and mitigation actions are both operationally relevant and support the strategic needs of the organization.

5.3 ORDERED APPROACH

The process steps of the ORDERED approach are shown in **Figure 8**.

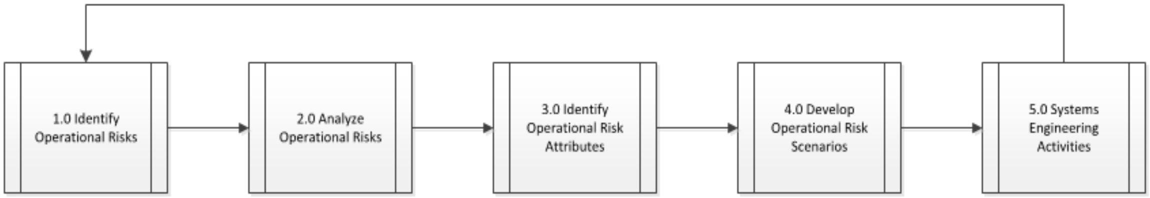

1.0 Identify Operational Risks
2.0 Analyze Operational Risks
3.0 Identify Operational Risk Attributes
4.0 Develop Operational Risk Scenarios
5.0 Systems Engineering Activities

Figure 8. ORDERED Activities.

ORDERED is a continuous process whereby operational risks are identified and analyzed. The risks or risk areas are characterized by identifying operational risk attributes and scenarios to further describe the concern in a manner that helps bridge the gap between operational activities and engineering activities. These scenarios are then evaluated against current and future engineering activities to ensure that requirements and development activities mitigate operational risk.

5.3.1 IDENTIFY OPERATIONAL RISKS

The activities associated with the Identify Operational Risks process step are shown in **Figure 9.**

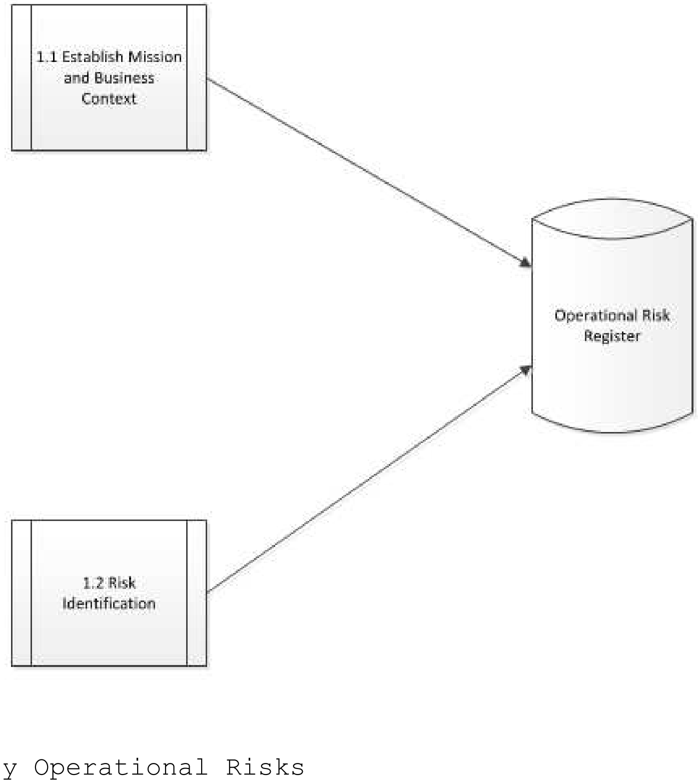

1.1 Establish Mission and Business Context
Operational Risk Register
1.2 Risk Identification

Figure 9. Identify Operational Risks

Risks are identified by having a clear understanding of the mission and business context of the operational organization to include mission-critical and mission-support tasks, objectives, and success criteria and then exploring areas of concern based on potentially failing to achieve, or fully achieve, operational mission success.

5.3.1.1 ESTABLISH MISSION AND BUSINESS CONTEXT

INPUTS: Understanding of mission and business needs.

OUTPUTS: Mission and business objectives and additional context as needed.

Clear articulation of mission and business context helps focus risk identification on areas relevant to mission success. According to Lewis Carrol, *If you don't know where you are going, any road will get you there*[58]. For the purpose of risk identification, knowing what constitutes mission and business success allows operational staff to explore obstacles to achieving success.

For example, a government agency may operate a Cybersecurity Operations Center (CSOC). The purpose of the CSOC is to ensure that cybersecurity incidents do not impact agency operations. The mission and business objectives of the CSOC could be described as shown in **Table 4**.

Depending on the complexity of the mission, further definition may be required to fully understand the mission and

Table 4. CSOC Mission and Business Objectives.

Mission Objectives	Business Objectives
1. Detect, contain, and remediate cybersecurity threats. 2. Analyze trends, determine root causes, and improve system resilience. 3. Educate system operators and maintainers about cybersecurity threats.	1. Reduce cybersecurity-related incidents. 2. Reduce cost of cybersecurity activities. 3. Position for agency organizational consolidation.

business context. Additional details defining specific mission-critical and mission-support tasks, detailed processes, and procedures necessary to perform the mission, as well as quantitative criteria to evaluate mission success, may be provided.

5.3.1.2 RISK IDENTIFICATION

INPUTS: Mission and business objectives and additional context as needed.

OUTPUTS: List of operational risks.

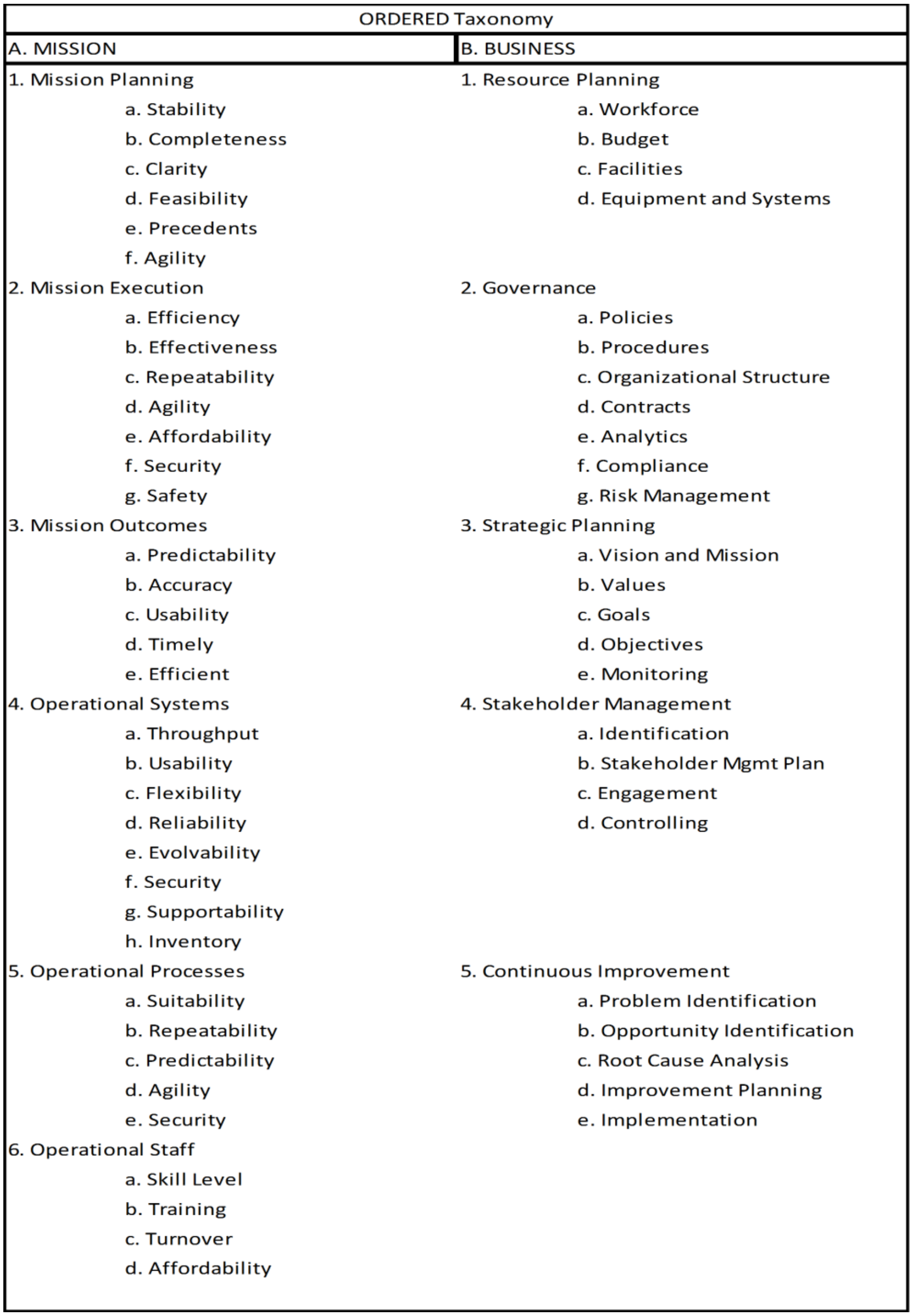
There are many methods for identification of risk to include continuous risk identification by all members of the organization, structure risk identification sessions, and milestone or event-based risk identification[3]. Structured risk identification sessions are facilitated activities with stakeholders and subject matter experts available to help brainstorm operational risks.

Individual risk statements are captured in a structured manner to allow for analysis. Risks may be identified using the *if-then* construct: *if* (an event occurs), *then* (an outcome occurs) or using the *condition; consequence* construct: *condition* (something that exists) leads to an undesirable *consequence* (outcome). The simplified *condition; consequence* structure will be used here.

Regardless of identification method or methods used, sources of risk are explored by operational personnel. ORDERED uses a taxonomy to help with risk identification. A taxonomy is useful both when exploring sources of risk as well as when classifying risks after they are identified to help with the Analyze Operational Risks process. The ORDERED Taxonomy is shown in **Figure 10**. The taxonomy was developed and simplified by considering several source documents[53, 59, 60, 20] and personal experience.

The ORDERED taxonomy consists of two *categories*: Mission and Business. The next level of the taxonomy contains *elements* such as Mission Planning, Operational Systems, and Continuous Improvement. The final level of the taxonomy consists of *attributes*.

Appendix A contains the complete taxonomy with taxonomic definitions for categories, elements, and attributes as well as



ORDERED Taxonomy

A. MISSION	B. BUSINESS
1. Mission Planning	1. Resource Planning
a. Stability	a. Workforce
b. Completeness	b. Budget
c. Clarity	c. Facilities
d. Feasibility	d. Equipment and Systems
e. Precedents	
f. Agility	
2. Mission Execution	2. Governance
a. Efficiency	a. Policies
b. Effectiveness	b. Procedures
c. Repeatability	c. Organizational Structure
d. Agility	d. Contracts
e. Affordability	e. Analytics
f. Security	f. Compliance
g. Safety	g. Risk Management
3. Mission Outcomes	3. Strategic Planning
a. Predictability	a. Vision and Mission
b. Accuracy	b. Values
c. Usability	c. Goals
d. Timely	d. Objectives
e. Efficient	e. Monitoring
4. Operational Systems	4. Stakeholder Management
a. Throughput	a. Identification
b. Usability	b. Stakeholder Mgmt Plan
c. Flexibility	c. Engagement
d. Reliability	d. Controlling
e. Evolvability	
f. Security	
g. Supportability	
h. Inventory	
5. Operational Processes	5. Continuous Improvement
a. Suitability	a. Problem Identification
b. Repeatability	b. Opportunity Identification
c. Predictability	c. Root Cause Analysis
d. Agility	d. Improvement Planning
e. Security	e. Implementation
6. Operational Staff	
a. Skill Level	
b. Training	
c. Turnover	
d. Affordability	

Figure 10. ORDERED Risk Taxonomy

exploratory questions that may be used during a risk assessment to prompt discussion of operational risk.

Using the example of an agency CSOC, during a risk identification workshop, CSOC operators explored business and mission objectives and used the ORDERED taxonomy to examine areas of potential risk. The risk workshop used a structured brainstorm approach and allowed all concerns to be voiced and captured without filtering. The participants collected their concerns in the *condition; consequence* format to allow for analysis in subsequent steps. Shown in **Table 5** are five of the more than sixty risks identified during the session.

Table 5. CSOC Risk Statements

Risk ID	Risk Statement
CSOC001	Incident occurrence is unpredictable; may not have adequate resources to respond during crisis
CSOC002	Heavy compliance and oversight make processes rigid; may not be able to adjust quickly to new events
CSOC003	Current intrusion detection system is proprietary, and vendor is not responsive when changes are needed; system may not detect newer threats; cost of support is high
CSOC004	We hire new operators with little experience; lower mission effectiveness
CSOC005	80 percent of operator time is spent responding to incidents; may not see trends or understand root cause of incidents

Using the *condition; consequence* format keeps the risk statements focused on areas of concern that are relevant to the mission. Risk CSOC004 was identified when exploring Mission Execution, Mission Outcomes, and Operators elements of the

ORDERED taxonomy. The concern raised was that mission effectiveness and ability to meet operational objectives are impacted by inexperienced CSOC operators.

CSOC003 raises concern about the use of a proprietary system and the inability to quickly update the system to meet operational needs. Since the CSOC is dependent on the proprietary system with no alternative source for the capability, CSOC leadership has little leverage with the vendor to reduce costs.

5.3.2 ANALYZE OPERATIONAL RISKS

The activities associated with the Analyze Operational Risks process step are shown in **Figure 11.**

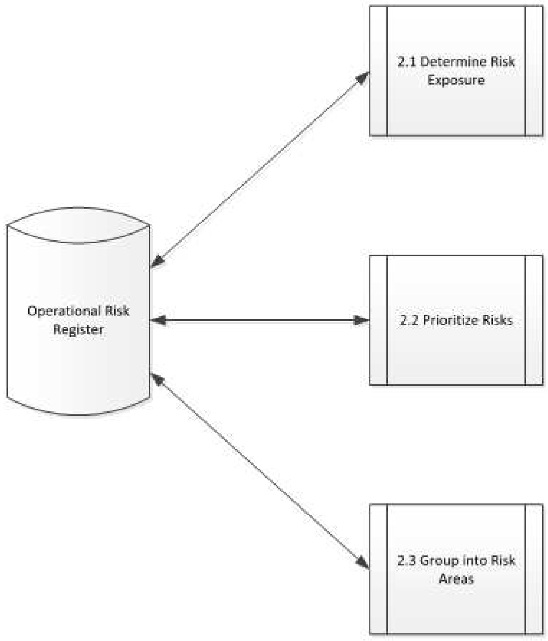

2.1 Determine Risk Exposure
Operational Risk Register
2.2 Prioritize Risks
2.3 Group into Risk Areas

Figure 11. Analyze Operational Risks

Once risks are identified, the next step is to analyze the risks to help understand the exposure that the mission is facing based on each risk, which risks are most critical to mitigate, and to group risks as appropriate when multiple risks address the same risk area.

5.3.2.1 DETERMINE RISK EXPOSURE

INPUTS: List of operational risks.

OUTPUTS: List of operational risks and their risk exposure.

Risk Exposure (RE) is the product of the probability (P) that the risk will occur and the impact (I) to the organization if the risk occurs: RE = P x I. The goal in determining risk exposure is to understand the relative criticality of a given risk in order to help decide which risks should be mitigated, in what order, and the number of resources that the organization is willing to expend on mitigation activities.

Determining risk exposure is not an exact science and relies on the best judgment of individuals. For this reason the ORDERED approach keeps this step simple. The operational organization must decide how to assign a probability and impact score to each risk. ORDERED uses a simple 1 to 5 rating for probability as shown in **Table 6**, with 1 being the lowest probability of occurrence and 5 being the highest probability of occurrence.

Table 6. Probability of Risk Occurrence

Probability	
5	Almost Certain p > 60%
4	Likely 40% < p < 60%
3	Moderate 20% < p < 40%
2	Unlikely 5% < p < 20%
1	Rare p < 5%

While probability of occurrence becomes a simple determination of likelihood of the risk occurring based on best judgment, the impact of occurrence must be taken into consideration with the impact of the risk to the mission or business needs of the organization. Each operational organization will adjust the impact definitions to meet its needs. A generic impact of occurrence table is shown in **Table 7.**

With a list of risks and their risk exposure, an operational organization may begin to understand the relative importance of applying mitigation resources. A simple risk exposure matrix as shown in **Table 8** may help to graphically show

Table 7. Impact of Risk Occurrence

Impact		Risk
5	Extreme	Unacceptable operational failure
4	Major	Loss of operational capability
3	Moderate	Remedial action required
2	Minor	Limited operational impact
1	Insignificant	Minimal operational impact

Table 8. Risk Exposure Matrix

		Insignificant	**Minor**	**Moderate**	**Major**	**Extreme**
		1	**2**	**3**	**4**	**5**
Almost Certain	**5**	**Yellow**	**Yellow**	**Red**	**Red**	**Red**
Likely	**4**	**Green**	**Yellow**	**Yellow**	**Red**	**Red**
Moderate	**3**	**Green**	**Yellow**	**Yellow**	**Yellow**	**Red**
Unlikely	**2**	**Green**	**Green**	**Yellow**	**Yellow**	**Red**
Rare	**1**	**Green**	**Green**	**Green**	**Yellow**	**Yellow**

the risk exposure of each individual risk and its relative exposure as compared to other risks.

Table 9 shows the CSOC risks with their probability of occurrence, impact of occurrence, and risk exposure.

Using the risk exposure matrix and placing the CSOC risks within the matrix produces the result in **Table 10**.

Table 9. CSOC Risks with Risk Exposure

Risk ID	Risk Statement	Prob	Imp
CSOC001	Incident occurrence is unpredictable; may not have adequate resources to respond during crisis	4	2
CSOC002	Heavy compliance and oversight make processes rigid; may not be able to adjust quickly to new events	2	3
CSOC003	Current intrusion detection system is proprietary, and vendor is not responsive when changes are needed; system may not detect newer threats; cost of support is high	4	4
CSOC004	We hire new operators with little experience; lower mission effectiveness	4	4
CSOC005	80 percent of operator time is spent responding to incidents; may not see trends or understand root cause of incidents	4	2

Table 10. CSOC Risk Exposure Matrix

		Insignificant	Minor	Moderate	Major	Extreme
		1	2	3	4	5
Almost Certain	5	🟨	🟨	🟥	🟥	🟥
Likely	4	🟩	🟨 CSOC001 CSOC005	🟨	🟥 CSOC003 CSOC004	🟥
Moderate	3	🟩	🟨	🟨	🟨	🟥
Unlikely	2	🟩	🟩	🟨 CSOC002	🟨	🟥
Rare	1	🟩	🟩	🟩	🟨	🟨

The risk exposure matrix provides a quick and graphical representation of risk exposure and allows decision-makers to allocate resources to mitigate risks. Risks CSOC003 and CSOC004 present the highest risk exposure to mission and business objectives and should be considered first for mitigation activities.

5.3.2.2 PRIORITIZE RISKS

INPUTS: List of operational risks and their risk exposure.

OUTPUTS: Prioritized list of operational risks.

Prioritizing risks provides decision-makers with the ability to allocate scarce resources to mitigate the most important risks to mission success. Simply sorting the risk list by risk exposure, highest to lowest, provides a first look at potential prioritization.

However, since risk probability and risk impact are assigned using best judgment, once the entire list of risks sorted by risk exposure is examined, it may be less practical or urgent to mitigate some risks that sort higher in the list than risks that are further down the risk list. Use the list of risks sorted by risk exposure highest to lowest and examine the top five to ten risks to make sure that the order of the risks makes sense.

Allow for the possibility to move risks up or down based on operational need, urgency, and other operational concerns. Adjust the probability and impact or occurrence as more insight is gained.

In the CSOC example, a simple sort by risk exposure produces the list as shown in **Table 11.** This provides an initial list of the Top N risks.

Table 11. CSOC Initial Prioritized Risk List

Risk ID	Risk Statement	Prob	Imp	Risk Exposure
CSOC003	Current intrusion detection system is proprietary, and vendor is not responsive when changes are needed; system may not detect newer threats; cost of support is high	4	4	16
CSOC004	We hire new operators with little experience; lower mission effectiveness	4	4	16
CSOC001	Incident occurrence is unpredictable; may not have adequate resources to respond during crisis	4	2	8
CSOC005	80 percent of operator time is spent responding to incidents; may not see trends or understand root cause of incidents	4	2	8
CSOC002	Heavy compliance and oversight make processes rigid; may not be able to adjust quickly to new events	2	3	6

After examining the prioritized list of risks, CSOC leadership decided that risk CSOC004 was more urgent to mitigate than CSOC0003, and likewise CSOC005 was more important to mitigate than CSOC001. Given these decisions, the list was re-sorted in accordance with the top five risks presented in **Table 12.**

Table 12. CSOC Final List of Prioritized Risks

Top N	Risk ID	Risk Statement	Prob	Imp	Risk Exposure
1	CSOC004	We hire new operators with little experience; lower mission effectiveness	4	4	16
2	CSOC003	Current intrusion detection system is proprietary, and vendor is not responsive when changes are needed; system may not detect newer threats; cost of support is high	4	4	16
3	CSOC005	80 percent of operator time is spent responding to incidents; may not see trends or understand root cause of incidents	4	2	8
4	CSOC001	Incident occurrence is unpredictable; may not have adequate resources to respond during crisis	4	2	8
5	CSOC002	Heavy compliance and oversight make processes rigid; may not be able to adjust quickly to new events	2	3	6

5.3.2.3 GROUP INTO RISK AREAS (OPTIONAL)

INPUTS: Prioritized list of operational risks.

OUTPUTS: Prioritized list of operational risk areas.

An individual risk may be viewed as a single flashlight illuminating some potential impact in the future. When an organization has a long list of risks, either due to an exhaustive risk identification process or as a result of multiple structured risk identification workshops, it may make sense to group the *flashlights* that appear to point in the same direction together to get a better understanding of the common area of risk that they address.

Risks may be grouped into a pre-defined structure such as the ORDERED taxonomy, a work breakdown structure, by mission tasks, or other structure that helps reason out how the risks relate. Another option is to group the risks by allowing a structure to emerge based on the risks themselves[61].

Once the individual risks are grouped into risk areas, the risk areas are then prioritized by examining the relationship between the risk areas. An inter-relationship digraph is a powerful and simple tool that may be used to examine these relationships[62]. **Figure 12** shows an example inter-relationship digraph illustrating the relationship of six risk areas.

Each risk area is comprised of many individual risk statements. The digraph is constructed by examining each risk area relative to every other risk area to determine if the risk statements associated with the risk area drive or cause the risk statements in the other risk area or vice versa. If there is a relationship, an arrow is drawn to show the primary direction of the relationship. Two-way arrows are not allowed.

Once the digraph is constructed, add the number of arrows coming in to the risk area and the number going out. Risk areas with many arrows coming in indicate that other risk areas are driving or causing the risk statements in this area. Risk areas

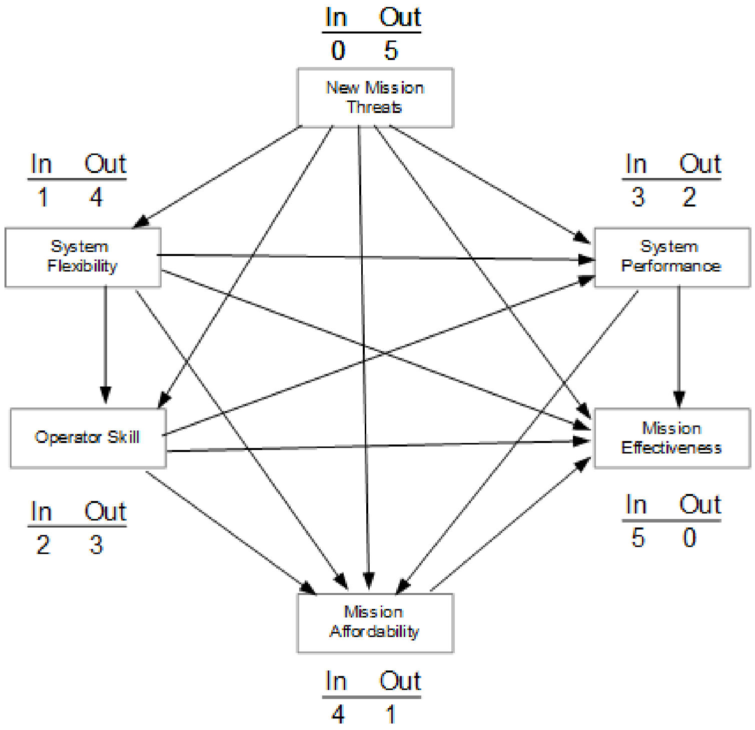


Figure 12. Inter-relationship Digraph

with many arrows going out indicate that risk statements in this risk area are driving risk in the other risk areas.

In this example, the risk area New Mission Threats contains risk statements that drive risk in all other risk areas. Ideally, this is the risk area on which to focus mitigation activities, but realistically, evolving mission threats may be externally driven and may not be within the control of the organization to mitigate.

The risk area System Flexibility may need to be addressed to ensure that systems may respond to new or evolved mission threats. Likewise, the risk area Operator Skill may need to be addressed to ensure that operational personnel are adequately skilled to adjust to changes in mission needs.

Prioritizing mitigation actions on the risk areas with more arrows going out than coming in provides focus and allows the organization to allocate mitigation resources effectively.

5.3.3 IDENTIFY OPERATIONAL RISK ATTRIBUTES

The activities associated with the Identify Operational Risk Attributes process step are shown in **Figure 13.**

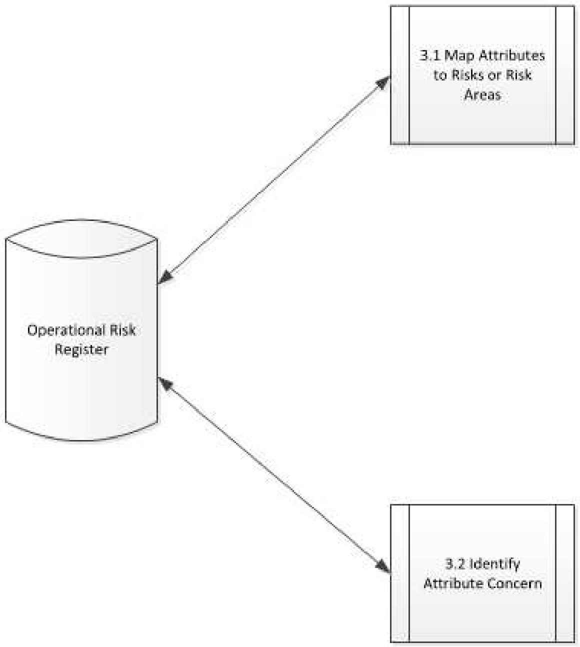

3.1 Map Attributes to Risks or Risk Areas
Operational Risk Register
3.2 Identify Attribute Concern

Figure 13. Identify Operational Risk Attributes

Once risks have been analyzed and their risk exposure determined, and the risks or risk areas are prioritized, the next step is to further explore the risks by identifying the risk attributes that describe the risk’s characteristics and the concerns associated with those characteristics.

5.3.3.1 MAP ATTRIBUTES TO RISKS OR RISK AREAS

INPUTS: Prioritized list of operational risks or risk areas.

OUTPUTS: List of operational risks and risk attributes.

An operational risk attribute is a characteristic of the operational mission or business that will be judged negatively by stakeholders unless the operational risk is mitigated. The purpose of mapping operational risk attributes to risk statements is to further clarify operational concerns and to help when identifying mitigation actions.

A starting point in mapping operational risk attributes is the ORDERED risk taxonomy. The lowest level of the taxonomy contains attributes describing the aspect of risk associated with the elements and categories of the taxonomy. Additional attributes to explore include quality attributes as described in Attribute Driven Design[63] engineering approaches and the Method Framework for Engineering System Architectures[64].

In the CSOC example, the top five risks are shown in **Table 13** with the addition of the risk attributes from the ORDERED taxonomy.

For risk CSOC004, the attributes mapped to the risk statement are Training and Skill Level from the Operator element and Effectiveness from the Mission Execution element. Training

Table 13. CSOC Top Risks with Risk Attributes

Top N	Risk ID	Risk Statement	Prob	Imp	Risk Exposure	Risk Attributes
1	CSOC004	We hire new operators with little experience; lower mission effectiveness	4	4	16	1. Operator: Training, Skill Level 2. Mission Execution: Effectiveness
2	CSOC003	Current intrusion detection system is proprietary, and vendor is not responsive when changes are needed; system may not detect newer threats; cost of support is high	4	4	16	1. Operational Systems: Flexibility 2. Mission Execution: Affordability
3	CSOC005	80 percent of operator time is spent responding to incidents; may not see trends or understand root cause of incidents	4	2	8	1. Operational Systems: Predictability 2. Operational Processes: Suitability
4	CSOC001	Incident occurrence is unpredictable; may not have adequate resources to respond during crisis	4	2	8	1. Resource Planning: Workforce
5	CSOC002	Heavy compliance and oversight make processes rigid; may not be able to	2	3	6	1. Operational Processes: Agility 2. Governance: Policies and Procedures

		adjust quickly to new events				

and skill level of operators will be judged negatively by stakeholders if this risk isn’t mitigated. The effectiveness of the mission will also be judged negatively as the operators who are less skilled and lack training impact mission outcomes.

5.3.3.2 IDENTIFY ATTRIBUTE CONCERN

INPUTS: List of operational risks and risk attributes.

OUTPUTS: List of operational risks, risk attributes, and areas of concern.

In addition to understanding the attributes associated with the operational risk, additional insight into the actual concern is useful when determining mitigation actions. While it helps to understand that a given risk is associated with an ORDERED taxonomic *element* and *attribute*, the additional understanding from eliciting the area of concern from the individual or group who identified the risk provides more definitive focus.

For example, an operator may have identified the following risk: *Current systems were designed using nominal data loads; system may not scale*. The risk could be mapped to the Operational Systems *element* and Throughput *attribute* of the taxonomy.

Simply knowing that Throughput is an attribute may not provide enough detail. The *attribute concern* in this example could be described as *mission stress*. The operator is specifically concerned about how the system will operate when the mission becomes much more intense and the system needs to operate effectively when additional data is processed.

In the CSOC example, **Table 14** shows the top two risks mapped to taxonomic *elements* along with the operator's concern.

Table 14. CSOC Risks with Attribute Concerns

Top N	Risk ID	Risk Statement	Prob	Imp	Risk Exposure	Risk Attributes	Attribute Concern
1	CSOC 004	We hire new operators with little experience; lower mission effectiveness	4	4	16	1. Operator: Training, Skill Level 2. Mission Execution: Effectiveness	Assimilation of new staff and planned growth in mission
2	CSOC 003	Current intrusion detection system is proprietary, and vendor is not responsive when changes are needed; system may not detect newer threats; cost of support is high	4	4	16	1. Operational Systems: Flexibility 2. Mission Execution: Affordability	Mission expansion and attack sophistication

The CSOC operator’s concern with the Skill Level and Mission Execution *attributes* is the inability to perform the mission when assimilating new staff, especially because of planned mission growth, which will require additional staff to be added at a rate higher than previously experienced.

The addition of the attribute concern of *Assimilation of new staff and planned growth in mission* sheds more light on the risk. The addition of the attribute concern enables the construction of more complete risk scenarios.

5.3.4 DEVELOP OPERATIONAL RISK SCENARIOS

The activities associated with the Develop Operational Risk Scenarios process step are shown in **Figure 14.**

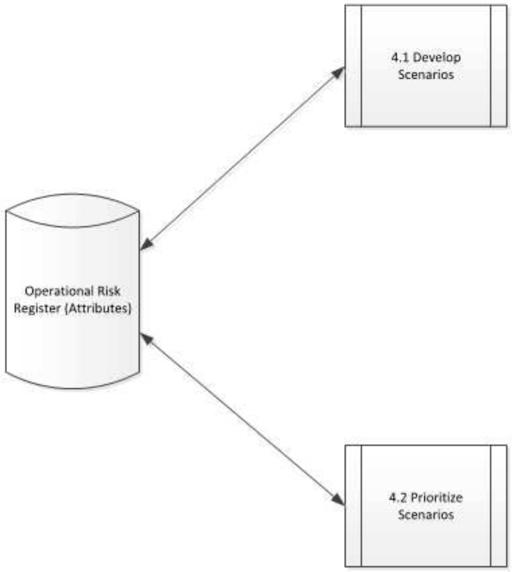


Figure 14. Develop Operational Risk Scenarios

5.3.4.1 DEVELOP SCENARIOS

INPUTS: List of operational risks, risk attributes, and areas of concern.

OUTPUTS: List of operational risks with risk scenarios.

Scenarios are simply expressions of real-world interactions. They may be formal, structured and verbose, or freer form and expressed simply[65]. The purpose of scenarios as used to influence engineering activities is to describe expected results of a system during development in terms of real-world behavior[66]. Scenarios describe how the system should behave under certain conditions when presented with certain stimuli[67].

Operational risk scenarios describe the unwanted behavior of the system that would cause mission or business impact to the operational organization. Similar to the concept of anti-patterns in systems and software engineering[68], operational risk scenarios describe undesirable outcomes that need to be mitigated because they increase operational risk.

The ORDERED method uses a simplified format to describe the risk scenario based on the Architecture Tradeoff Analysis Method[69]. The operational risk scenario should describe a source that provides a stimulus to a system or operational task, the environment or artifact affected by the stimulus, and the unwanted response or outcome. Example operational risk scenarios are listed below:

> *An operator requests fire suppression during a high intensity operation with degraded communications; and the request fails to transmit within five minutes.*
>
> *A resource manager attempts to re-assign a military member while the member is relocating to a new assignment; and the system fails to locate the member*.

The key difference between engineering scenarios and operational risk scenarios is that operational risk scenarios describe negative or unwanted behavior or outcomes while traditional engineering scenarios describe expected behavior or outcomes.

Using the CSOC example, the top two risks are shown in **Table 15**, complete with risk statement, risk attributes and areas of concern, and operational risk scenarios. The scenarios for risk CSOC004 describe the unwanted outcome of new operators failing certification within two weeks and how a change in mission objectives requires a 200 percent ramp-up in operational staff, creating new teams that fail to become mission capable within one month.

CSOC003 scenarios describe both a growth in mission requirements and failure of the existing system to adapt to the change, as well as a new sophisticated attack coupled with the system’s lack of flexibility in evolving easily to address the potential scenario. In all cases, operational risk scenarios describe unwanted behavior or outcomes.

Operational risk scenarios describe the unwanted behavior of a system or outcome of a mission-critical or mission-support task. Some scenarios are more critical to address than others, and some scenarios may already be addressed by operational processes or by existing or planned system capabilities. The

Table 15. CSOC Operational Risk Scenarios

Top N	Risk ID	Risk Statement	Risk Attributes	Attribute Concern
1	CSOC004	We hire new operators with little experience; lower mission effectiveness	1. Operator: Training, Skill Level 2. Mission Execution: Effectiveness	Assimilation of new staff and planned growth in mission
	Operational Risk Scenarios 1. New operator joins organization and fails to be completely certified and capable within two weeks. 2. OPs staff grows by 200 percent, increasing the number of teams performing the mission. New teams not fully capable of supporting operations within one month.			
2	CSOC003	Current intrusion detection system is proprietary, and vendor is not responsive when changes are needed; system may not detect newer threats; cost of support is high	1. Operational Systems: Flexibility 2. Mission Execution: Affordability	Mission expansion and attack sophistication
	Operational Risk Scenarios 1. New mission tasking requires additional intrusion detection across new agency locations. Current system fails to scale, and vendor is unresponsive in making required system changes. 2. A new hacker group uses alternative means to access closed system and uses technology not detected by current system. Complete re-design of detection system required to implement new detection algorithms.			

next step is to prioritize the scenarios based on mission criticality and level of existing plan accommodation.

5.3.4.2 PRIORITIZE SCENARIOS

INPUTS: List of operational risks with risk scenarios.

OUTPUTS: Prioritized operational risk scenarios.

With a list of operational risk scenarios, the next step is to prioritize the scenarios to determine which risk scenarios are the most critical to avoid based on mission and business needs. Some of the risk scenarios might already have mitigation activities in place due to current or planned operational processes or planned activities within the systems engineering lifecycle, such as requirements, design trade-offs, implementation decisions, testing approaches, or deployment strategies that address the scenario to some degree.

Table 16 provides a matrix to score risk scenarios based on criticality and accommodation gap. Scenarios that have a serious mission or business impact are assigned a criticality score of HIGH, scenarios with moderate impact are assigned a score of MEDIUM, and scenarios that have a low mission impact are scored LOW.

The other important aspect in prioritizing scenarios is understanding if current operations or engineering plans accommodate avoidance of the scenario. Scenarios that are not accommodated in current operations or engineering plans are assigned a gap score of HIGH, scenarios that have some accommodation in current operations or engineering plans are assigned a gap scope of MEDIUM, and scenarios that are avoided by current operations or engineering plans are assigned a gap score of LOW.

Table 16. Scenario Criticality and Gap Scoring Matrix

Mission or Business Criticality	
HIGH	Serious mission or business impact
MEDIUM	Moderate mission or business impact
LOW	Low mission or business impact
Plan Gap	
HIGH	No accommodation based on current operations or engineering plan (requirements, design, implementation, testing, deployment)
MEDIUM	Some accommodation based on current operations or engineering plan (requirements, design, implementation, testing, deployment)
LOW	Accommodated in current operations or engineering plan (requirements, design, implementation, testing, deployment)

The criticality and gap score of a scenarios helps those involved to decide which scenarios receive the most attention in the Influence Systems Engineering Activities step of the ORDERED method. Scenarios with HIGH criticality and HIGH gap scores are prioritized over scenarios with LOW criticality and LOW gap scores.

Best judgment is used to prioritize scenarios with scores other than HIGH/HIGH and LOW/LOW. Criticality may be deemed more important than gap given certain mission or business considerations, or gap may be deemed more important.

In the CSOC example, **Table 17** represents the scenarios scored by criticality and gap. Scenario CSOC003-1 has a HIGH mission criticality score and also has no accommodation in current operations or engineering plans to avoid the scenario.

Table 17. CSOC Prioritized Operational Risk Scenarios

Scenario Number	Operational Risk Scenario	Criticality	Gap
CSOC003-1	New mission tasking requires additional intrusion detection across new agency locations. Current system fails to scale, and vendor is unresponsive in making required system changes	HIGH	HIGH
CSOC004-2	OPs staff grows by 200 percent, increasing number of teams performing the mission. New teams not fully capable of supporting operations within one month.	HIGH	MEDIUM
CSOC003-2	A new hacker group uses alternative means to access closed system and uses technology not detected by current system. Complete re-design of detection system required to implement new detection algorithms.	MEDIUM	HIGH
CSOC004-1	New operator joins organization and fails to be completely certified and capable within two weeks.	MEDIUM	MEDIUM

CSOC004-1 and CSOC004-2 both address concerns with training and certification of staff, but CSOC004-1 is less critical as it only addresses the performance of individuals while CSOC004-2 is concerned about performance of teams.

The team felt that CSOC003-2 had a criticality of MEDIUM because the scenario was contained to a single class of intrusion. However, given the lack of accommodation to avoid the scenario, the team may decide to prioritize it above CSOC004-2.

With a list of prioritized operational risk scenarios, systems engineering lifecycle activities are next explored to determine if these scenarios may help improve operational acceptability of systems as they are developed.

5.3.5 INFLUENCE SYSTEMS ENGINEERING ACTIVITIES

Operational risk may be used to inform and influence systems engineering lifecycle activities with the intended outcome of improving the operational acceptability of delivered solutions and services. The activities associated with the Influence Systems Engineering Activities process step is shown in **Figure 15**.

5.3.5.1 INFORM REQUIREMENT ENGINEERING

INPUTS: Requirements and prioritized operational risk scenarios.

OUTPUTS: Validated requirements, change requests, and updated risk register.

Informing requirements with operational risk scenarios is part of a larger requirements validation activity. The process of transforming operational mission and business threats, risks, and needs into a set of requirements that may drive the creation of a system, product, or capability to meet those needs may be a multi-phased process implemented sequentially, iteratively, continuously, in an evolutionary approach, or a combination of approaches[70].

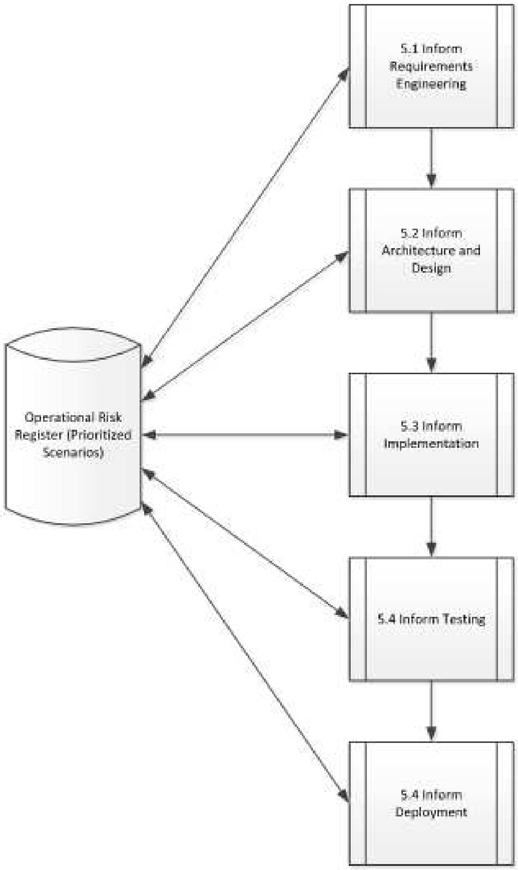

5.1 Inform Requirements Engineering
5.2 Inform Architecture and Design
Operational Risk Register (Prioritized Scenarios)
5.3 Inform Implementation
5.4 Inform Testing
5.4 Inform Deployment

Figure 15. Influence Systems Engineering Activities

This step is not intended to replace the requirements engineering process on a program, but rather to inform the process with operational risk considerations so that the requirements for the system, product, or capability specifies functional and non-functional behavior that avoids high priority operational risk scenarios.

Boehm recommends a requirements approach that includes emphasizing value-driven, shared-vision-driven, change-driven, and risk-driven activities[71]. Central to these approaches is exploration of operational scenarios describing intended behavior.

Risk-driven activities allow engineering leadership to apply resources to mitigate highest risks or to avoid performing activities that increase risk. The addition of operational risk scenarios to expected behavior scenarios allows engineers and operational users to explore behavior that they want the resulting system, product, or capability to help mitigate or avoid.

This step is simply using operational risk scenarios to help define requirements, validate that existing requirements are sufficient, or identify required changes in requirements to address the operational risk scenario. This isn't a one-time activity or only performed during the requirements phase of a program, but rather should be performed continuously as new operational risks are identified and operational risk scenarios are defined.

As requirements are informed by operational risk scenarios, the risk scenario scoring is adjusted as appropriate, which may also require a change in the risk exposure of the original operational risk statement. The operational risk register is updated to reflect new understanding of risk exposure and scenario scoring.

In the CSOC example, after discussing risk scenario CSOC003-1, the engineering team and operational users agreed that the functional requirements were sound but that they had collectively overlooked non-functional requirements of scalability, flexibility, and evolvability. The team decided to issue a program change request authorizing additional architectural trade studies to be performed with the goal of maximizing the non-functional requirements to specifically avoid the operational risk scenario.

Risk scenario CSOC004-2 highlighted the lack of a separate training environment with minimal operational capability to allow multiple teams to train without impacting ongoing operations. The result was a change request to add the requirement for an operationally relevant training environment.

5.3.5.2 INFORM ARCHITECTURE AND DESIGN

INPUTS: Validated requirements, architecture and design, and prioritized operational risk scenarios.

OUTPUTS: Validated architecture and design, change requests, and updated risk register.

Informing architecture and design with operational risk scenarios is part of a larger architecture and design validation activity. Architecture is simply the highest level of design, the first artifact that structures a system, component, or capability into its constituent physical or logical sub-parts. It also represents the first opportunity to ensure that the resulting design and implementation enables desired attributes and avoids undesirable attributes.

The addition of operational risk scenarios during architectural development and validation allows architects and engineers to select or create architectural mechanisms and constructs to avoid operational risk. While all architecture is a design activity, not all design is an architecture activity. Architecture informs, constrains, and influences lower-level design, whereas the lowest level of design describes and influences implementation-level choices[72].

For the purposes of ORDERED, these two activities are treated the same. This step is not intended to replace the architecture and design processes on a program, but rather to inform the processes with operational risk considerations so that architectural and design decisions for the system, product, or capability avoid high priority operational risk scenarios.

As with requirements, this step is simply using operational risk scenarios to help inform architecture and design decisions, to validate that previous architecture and design decisions are sufficient, or to identify required changes in architecture or design artifacts to address operational risk scenarios. This activity should be performed continuously as new operational risks are identified and operational risk scenarios are defined.

As architecture and design activities and artifacts are informed by operational risk scenarios, the risk scenario scoring is adjusted as appropriate, which may also require a change in the risk exposure of the original operational risk statement. The operational risk register is updated to reflect new understanding of risk exposure and scenario scoring.

In the CSOC example, the operational users participated in an architecture evaluation, which included a discussion of the operational risk scenarios and the architectural mechanisms and patterns selected and how they would either avoid the scenario or were deficient in mitigating the risk. When evaluating operational risk scenario CSOC003-1, the engineering team and operational users concluded that the architecture team had failed to consider structural and behavioral patterns that would help avoid the risk scenario.

Since the architecture was still in development, the architecture team revised its approach and selected additional architectural patterns to increase the scalability, flexibility, and evolvability of the solution.

5.3.5.3 INFORM IMPLEMENTATION

INPUTS: Validated requirements, validated architecture and design, implementation details, and prioritized operational risk scenarios.

OUTPUTS: Validated implementation details, change requests, and updated risk register.

Informing implementation with operational risk scenarios is part of a larger systems engineering implementation activity. Implementation is the process of realizing a system that satisfies the validated architecture and design and meets stakeholder requirements. Implementation decisions are made to include make, buy, or re-use tradeoffs as well as resolving detailed implementation choices below the design level.

Operational risk considerations are key in performing engineering trade studies and should be weighted appropriately when selecting implementation-level solutions. This step is not intended to replace the implementation processes on a program, but rather to inform the processes with operational risk considerations so that implementation decisions for the system, product, or capability avoid high priority operational risk scenarios.

This step uses operational risk scenarios to help inform implementation decisions, to validate that previous implementation decisions are sufficient, or to identify required changes in implementation approaches to address operational risk scenarios. This activity should be performed continuously as new operational risks are identified and operational risk scenarios are defined.

As implementation artifacts and activities are informed by operational risk scenarios, the risk scenario scoring is adjusted as appropriate, which may also require a change in the risk exposure of the original operational risk statement. The operational risk register is updated to reflect new understanding of risk exposure and scenario scoring.

In the CSOC example, after discussing risk scenario CSOC003-1, the implementation team decided to de-couple configuration information identifying locations and sites from the intrusion detection system’s compiled software components. This decision allowed end-users to add sites and locations by changing configuration files without needing to go back to the developer to change the software. While this change allowed more operational flexibility, the team also identified an operational security risk and provided guidance regarding additional changes to training and operational procedures to control unauthorized or inadvertent changes to site and location configurations.

5.3.5.4 INFORM TESTING

INPUTS: Validated requirements, validated architecture and design, validated implementation details, testing strategy, and prioritized operational risk scenarios.

OUTPUTS: Validated testing strategy, change requests, and updated risk register.

Informing testing with operational risk scenarios is part of a set of test activities on a program. A program typically has a series of test activities described in a test strategy or test management plan. Verification testing is performed to ensure that the component, sub-system, or system meets all specified requirements. Validation testing is performed to ensure that the delivered capability satisfies an operational need.

The gap between what is specified and what is needed increases operational risk and in turn the likelihood that the end-user rejects the new capability as operationally ineffective. The longer the development lifecycle, the more likely mission and business needs and threats will change. A program may successfully pass all verification testing and still fail validation testing if the delivered capability fails to satisfy the operational need.

Using operational risk scenarios in requirements, architecture, design, and implementation activities helps ensure that the system's specifications, design, and implementation reflect the evolving operational need, thereby decreasing the gap between how the system is specified and realized and the operational need at time of deployment. Test scenarios are use-oriented descriptions of desired function, data, and behavior of a given system[73]. They describe the detailed step-by-step instructions to exercise the system to prove that it behaves as expected.

Testing should also be used to ensure that the system doesn't exhibit unwanted behavior. One of the pitfalls of testing is inadequate user involvement during the planning and execution of test activities[74]. Operational risk scenarios captured from end-users throughout the development process may help test engineers develop comprehensive test scenarios that not only verify and validate expected behavior but also explore the system's ability to prevent unwanted behavior.

This step is not intended to replace the testing processes on a program, but rather to inform the processes with operational risk considerations so that test strategies and scenarios are more comprehensive and include the exploration of the system’s ability to mitigate the user’s most critical operational risks.

In the CSOC example, operational risk scenario CSOC003-2 describes a hacker gaining alternative access to a closed system to avoid detection. Based on this operational risk, the test team developed a set of test scenarios to examine the system’s ability to detect unauthorized access through alternative means.

The results of the testing will either validate that the system as implemented mitigates this operational risk or that additional risk mitigation actions should be considered. These additional actions could include a change request to add detection functionality or they could entail changes in operational processes to mitigate the risk.

5.3.5.5 INFORM DEPLOYMENT

INPUTS: Validated requirements, validated architecture and design, validated implementation details, validated testing strategy, deployment approach, and prioritized operational risk scenarios.

OUTPUTS: Validated deployment approach, change requests, and updated risk register.

Informing deployment with operational risk scenarios is part of a larger deployment strategy defined for the program. A program’s deployment approach needs to account not only for technical aspects of deploying new capabilities but also must account for organizational change issues associated with the operational organization adopting the new capability. These issues may include activities such as training for operations and maintenance staff and changes to operational processes and procedures.

The Capability Maturity Model Integrated Acquisition Model (CMMI-AM) provides guidance on transitioning new capabilities into operations and maintenance[75]. The goals and practices of the CMMI-AM process area Transition to Operations and Support are shown in **Table 18.**

Table 18. CMMI-AM Transition to Operations and Support Goals and Practices

Capability Maturity Model Integrated Acquisition Model – Transition to Operations and Support	
Goals	**Practices**
1. Preparation for transition to operations and support is conducted.	**1.1** Establish and maintain a strategy for transition to operations and support. **1.2** Establish and maintain plans for transitioning acquired products into operational use and support. **1.3** Establish and maintain training requirements for operational and support personnel. **1.4** Establish and maintain initial and lifecycle resource requirements for performing operations and support. **1.5** Identify and assign organizational responsibility for support. **1.6** Establish and maintain criteria for assigning responsibility for enhancements. **1.7** Establish and maintain transition criteria for the acquired products.

2. Transition decisions and actions are executed in accordance with transition criteria.	**2.1** Evaluate the readiness of the acquired products to undergo transition to operations and support. **2.2** Evaluate the readiness of the operational and support personnel to assume responsibility for the acquired products. **2.3** Analyze the results of all transition activities and identify appropriate action.

The practices from CMMI-AM may form the basis of a program's deployment plan. Operational risk scenarios defined throughout the systems engineering process should be used to define the implementation of these activities with the goal of reducing operational risk. This step is not intended to replace the deployment processes on a program, but rather to inform the processes with operational risk considerations so that deployment strategies, approaches, and activities are more robust and include the reduction of operational risk through deployment activities.

In the CSOC example, operational risk scenario CSOC004-2 describes an operational risk associated with standing up new teams to perform operations as mission scope increases. The engineering and operations team decided to deploy new capabilities incrementally, team-by-team, treating each deployment to a team as a new team stand-up. This allowed a low-risk deployment to smaller groups rather than the entire operational staff at once so that deployment activities could be validated and adjusted as needed based on issues found in early deployments.

In addition, treating each team as a new team stand-up allowed development and testing of processes and procedures for expanding mission scope to new teams with the benefit of reducing the risk described in risk scenario CSOC004-2.

5.4 MITIGATING OPERATIONAL RISK THROUGH SYSTEMS ENGINEERING

In addition to using operational risk to influence systems engineering activities, systems engineering processes may also be used to mitigate operational risk. The Defense Acquisition Guidebook describes systems engineering processes in two broad categories: Management Processes and Technical Processes[76]. Each of these categories contains eight processes that describe systems engineering activities as shown in **Table 19**.

Table 19. Defense Acquisition Guidebook Systems Engineering Processes

Defense Acquisition Guidebook Systems Engineering	
Management Processes	Technical Processes
Technical Planning	Stakeholder Requirements Definition
Decision Analysis	Requirements Analysis
Technical Assessment	Architecture Design
Requirements Management	Implementation
Risk Management	Integration
Configuration Management	Verification
Technical Data Management	Validation
Interface Management	Transition

The Management Processes provide a framework for managing the technical activities and identifying processes critical to the success of the program, while the Technical Processes ensure that the solution or service is designed to deliver the capability needed by the stakeholders. Each of these processes is performed to mitigate some amount of risk in which the product under development fails to meet the mission and business needs of the end-user or the end-user’s operational organization.

Table 20 maps the Attributes within the Mission Category of the ORDERED Risk Taxonomy to the Systems Engineering Management Processes of the Defense Acquisition Guidebook.

Table 20. ORDERED Taxonomy: Mission Category Mapped to SE Management Processes

Legend ● = High Mitigation Activity ⊙ = Medium Mitigation Activity ○ = Low Mitigation Activity			**Systems Engineering Technical Management Processes**							
ORDERED Risk Taxonomy			**Technical Planning**	**Decision Analysis**	**Technical Assessment**	**Requirements Management**	**Risk Management**	**Configuration Management**	**Technical Data Management**	**Interface Management**
MISSION	PLANNING	a. Stability	○	●	●	⊙	⊙	○	○	○
		b. Completeness	○	⊙	⊙	⊙	⊙	○	○	○
		c. Clarity	○	⊙	⊙	⊙	⊙	○	○	○

		d. Feasibility	⊙	●	●	●	●	○	○	○
		e. Precedents	●	●	●	●	●	○	○	⊙
		f. Agility	⊙	●	●	●	●	⊙	○	⊙
	EXECUTION	a. Efficiency	○	●	○	⊙	⊙	○	○	○
		b. Effectiveness	○	●	○	⊙	⊙	○	○	○
		c. Repeatability	○	⊙	○	⊙	⊙	⊙	⊙	⊙
		d. Agility	⊙	●	⊙	●	⊙	⊙	⊙	⊙
		e. Affordability	○	●	●	●	●	○	⊙	⊙
		f. Security	⊙	●	●	●	●	⊙	⊙	⊙
		g. Safety	⊙	●	●	●	●	⊙	⊙	⊙
	OUTCOMES	a. Predictability	○	⊙	●	⊙	○	⊙	⊙	○
		b. Accuracy	○	⊙	●	⊙	○	⊙	⊙	○
		c. Usability	⊙	⊙	⊙	⊙	○	○	●	○
		d. Timely	⊙	⊙	⊙	⊙	○	○	○	○
		e. Efficient	○	⊙	⊙	○	○	○	⊙	⊙
	SYSTEMS	a. Throughput	⊙	●	●	⊙	⊙	⊙	○	⊙
		b. Usability	⊙	●	●	⊙	⊙	⊙	●	⊙
		c. Flexibility	○	●	●	⊙	⊙	●	●	●
		d. Reliability	⊙	●	●	⊙	●	⊙	●	⊙
		e. Evolvability	⊙	●	●	⊙	⊙	●	●	●

	f. Security	●	●	●	⊙	⊙	●	●	●
	g. Supportability	⊙	●	⊙	⊙	⊙	●	●	⊙
	h. Inventory	○	⊙	○	○	○	⊙	●	⊙
PROCESSES	a. Suitability	○	⊙	○	○	⊙	○	⊙	⊙
	b. Repeatability	○	○	○	○	⊙	○	●	⊙
	c. Predictability	○	○	○	○	⊙	○	⊙	⊙
	d. Agility	⊙	⊙	○	○	⊙	⊙	⊙	⊙
	e. Security	⊙	⊙	⊙	○	⊙	●	●	⊙
STAFF	a. Skill Level	○	⊙	⊙	○	⊙	⊙	●	○
	b. Training	○	○	○	○	⊙	⊙	●	○
	c. Turnover	○	○	○	○	⊙	⊙	●	○
	d. Affordability	⊙	●	⊙	○	⊙	⊙	●	○

The relationship is characterized as HIGH if the systems engineering process may be substantially used to mitigate risks within an attribute, MEDIUM if there are aspects of the systems engineering process that may be used to mitigate risks within an attribute, or LOW if there is little direct ability of the systems engineering process to mitigate risks within an attribute.

For example, if there are high operational risks mapped to the Affordability attribute of the Mission Execution element, the Systems Engineering Management processes of Decision Analysis, Technical Assessment, Requirements Management, and Risk Management should be considered as risk mitigation activities. The Technical Data Management and Interface Management processes may also help mitigate the risks. Technical Planning and Configuration Management may be of less value when mitigating risks mapped to the Affordability attribute of the Mission Execution Element.

This is intended to be a starting point when considering which systems engineering activities may help mitigate operational risk. These relationships are generalized and would need to be adjusted when considering a specific program.

Table 21 maps the Attributes within the Mission Category of the ORDERED Risk Taxonomy to the Systems Engineering Technical Processes of the Defense Acquisition Guidebook.

Table 21. ORDERED Taxonomy: Mission Category Mapped to SE Technical Processes

Legend ● = High Mitigation Activity ⊙ = Medium Mitigation Activity ○ = Low Mitigation Activity			**Systems Engineering Technical Processes**							
ORDERED Risk Taxonomy			Stakeholder Requirements Definition	Requirements Analysis	Architecture Design	Implementation	Integration	Verification	Validation	Transition
M I	P L	a. Stability	⊙	●	●	●	○	○	⊙	⊙

SSION	ANNING	b. Completeness	○	⊙	●	●	○	○	⊙	○
		c. Clarity	○	⊙	●	●	○	○	⊙	○
		d. Feasibility	⊙	●	●	●	⊙	⊙	●	⊙
		e. Precedents	●	●	●	●	⊙	●	●	●
		f. Agility	●	●	●	●	○	●	●	⊙
	EXECUTION	a. Efficiency	○	●	●	●	○	○	⊙	⊙
		b. Effectiveness	●	●	●	●	○	○	⊙	⊙
		c. Repeatability	⊙	●	●	●	⊙	⊙	⊙	⊙
		d. Agility	⊙	●	●	●	⊙	⊙	●	⊙
		e. Affordability	⊙	●	●	●	⊙	⊙	●	●
		f. Security	⊙	●	●	●	●	●	●	●
		g. Safety	⊙	●	●	●	●	●	●	⊙
	OUTCOMES	a. Predictability	⊙	●	●	●	⊙	●	●	⊙
		b. Accuracy	⊙	●	●	●	⊙	●	●	⊙
		c. Usability	●	●	●	●	⊙	⊙	●	●
		d. Timely	⊙	●	●	●	⊙	⊙	●	⊙
		e. Efficient	⊙	⊙	●	●	○	○	⊙	○
	SYSTEMS	a. Throughput	⊙	●	●	●	●	●	●	⊙
		b. Usability	●	●	●	●	○	⊙	●	⊙
		c. Flexibility	●	●	●	●	⊙	⊙	●	⊙
		d. Reliability	⊙	●	●	●	●	●	●	⊙

		e. Evolvability	●	●	●	●	⊙	⊙	●	⊙
		f. Security	⊙	●	●	●	●	●	●	●
		g. Supportability	⊙	⊙	●	●	⊙	⊙	⊙	⊙
		h. Inventory	⊙	⊙	⊙	⊙	○	○	○	⊙
	PROCESSES	a. Suitability	⊙	⊙	○	○	○	○	⊙	⊙
		b. Repeatability	⊙	⊙	○	○	○	○	●	⊙
		c. Predictability	⊙	⊙	○	○	○	○	●	⊙
		d. Agility	⊙	⊙	⊙	⊙	○	○	●	⊙
		e. Security	●	●	⊙	⊙	○	○	●	●
	STAFF	a. Skill Level	●	●	●	●	○	○	●	●
		b. Training	●	⊙	⊙	⊙	○	○	●	●
		c. Turnover	⊙	⊙	○	○	○	○	⊙	●
		d. Affordability	●	●	⊙	⊙	○	○	⊙	●

Similarly, if there are high operational risks mapped to the Affordability attribute of the Mission Execution element, the Systems Engineering Technical processes of Requirements Analysis, Architecture Design, Implementation, Validation, and Transition should be considered as risk mitigation activities. The Stakeholder Requirements Definition, Integration, and Verification processes may also help mitigate the risks.

Table 22 maps the Attributes within the Business Category of the ORDERED Risk Taxonomy to the Systems Engineering Management Processes of the Defense Acquisition Guidebook.

For example, if the operational organization has difficulty engaging relevant stakeholders, there may be high operational risks mapped to the Engagement attribute of the Stakeholder Involvement element. The Systems Engineering Technical process of Risk Management should be employed to mitigate these risks.

Table 22. ORDERED Taxonomy: Business Category Mapped to SE Management Practices

Legend ● = High Mitigation Activity ⊙ = Medium Mitigation Activity ○ = Low Mitigation Activity			**Systems Engineering Technical Management Processes**							
ORDERED Risk Taxonomy			Technical Planning	Decision Analysis	Technical Assessment	Requirements Management	Risk Management	Configuration Management	Technical Data Management	Interface Management
BUSINESS	RESOURCES	a. Workforce	○	⊙	⊙	○	⊙	○	●	○
		b. Budget	●	●	●	⊙	⊙	○	⊙	⊙
		c. Facilities	⊙	⊙	⊙	⊙	⊙	○	⊙	⊙
		d. Equipment and Systems	⊙	●	●	⊙	●	⊙	⊙	⊙
	GOV	a. Policies	○	○	○	⊙	●	○	○	○
		b. Procedures	○	⊙	○	⊙	●	⊙	●	○

	ERNANCE	c. Organizational Structure	⊙	⊙	○	●	●	○	○	○
		d. Contracts	⊙	⊙	⊙	⊙	●	⊙	●	●
		e. Analytics	○	○	○	○	⊙	⊙	●	○
		f. Compliance	○	○	○	○	○	○	⊙	○
		g. Risk Management	⊙	⊙	⊙	⊙	●	○	○	⊙
	STRATEGY	a. Vision and Mission	○	⊙	○	⊙	●	○	○	○
		b. Values	○	⊙	○	○	⊙	○	○	○
		c. Goals	⊙	⊙	⊙	⊙	●	○	○	○
		d. Objectives	⊙	⊙	⊙	⊙	●	○	○	○
		e. Monitoring	○	○	○	○	⊙	○	○	○
	STAKEHOLDERS	a. Identification	⊙	⊙	○	⊙	●	○	○	●
		b. Stakeholder Management Plan	⊙	○	○	⊙	⊙	○	○	○
		c. Engagement	⊙	⊙	○	⊙	●	○	○	⊙
		d. Controlling	⊙	○	○	●	●	○	○	⊙
	IMPRO	a. Problem Identification	○	⊙	⊙	⊙	●	○	⊙	⊙
		b. Opportunity Identification	○	⊙	⊙	⊙	●	○	⊙	○
		c. Root Cause Analysis	○	⊙	●	⊙	⊙	⊙	⊙	⊙
		d. Improvement Planning	⊙	○	○	○	⊙	⊙	⊙	⊙

	VEMENT	e. Implementation	⊙	⊙	○	⊙	●	⊙	●	○

The Technical Planning, Decision Analysis, Requirements Management, and Interface Management processes may also help mitigate the risks. Technical Assessment, Configuration Management, and Technical Data Management may be of less value when mitigating risks mapped to the Affordability attribute of the Mission Execution Element.

Table 23 maps the Attributes within the Business Category of the ORDERED Risk Taxonomy to the Technical Processes of the Defense Acquisition Guidebook.

Table 23. ORDERED Taxonomy: Business Category Mapped to SE Technical Processes

Legend ● = High Mitigation Activity ⊙ = Medium Mitigation Activity ○ = Low Mitigation Activity			**Systems Engineering Technical Processes**							
ORDERED Risk Taxonomy			Stakeholder Requirements Definition	Requirements Analysis	Architecture Design	Implementation	Integration	Verification	Validation	Transition
BUSIN	RESOU	a. Workforce	●	⊙	⊙	⊙	○	○	⊙	⊙
		b. Budget	●	●	●	●	⊙	⊙	●	●

ESS	RCES	c. Facilities	⊙	⊙	⊙	○	○	○	⊙	⊙
		d. Equipment and Systems	●	●	●	●	⊙	○	⊙	⊙
	GOVERNANCE	a. Policies	●	⊙	○	○	○	○	⊙	○
		b. Procedures	●	●	●	●	○	○	●	●
		c. Organizational Structure	●	⊙	⊙	○	○	○	●	●
		d. Contracts	⊙	⊙	⊙	⊙	○	○	○	●
		e. Analytics	⊙	○	○	○	○	⊙	●	●
		f. Compliance	⊙	○	○	○	○	⊙	●	●
		g. Risk Management	⊙	⊙	⊙	⊙	○	⊙	●	●
	STRATEGY	a. Vision and Mission	●	●	○	○	○	○	●	⊙
		b. Values	⊙	⊙	○	○	○	○	⊙	⊙
		c. Goals	●	●	⊙	○	○	○	⊙	⊙
		d. Objectives	●	●	⊙	○	○	○	⊙	⊙
		e. Monitoring	○	○	○	○	○	○	○	○
	STAKEHOLDERS	a. Identification	●	⊙	⊙	○	○	○	●	●
		b. Stakeholder **Management** Plan	⊙	⊙	⊙	○	○	○	⊙	⊙
		c. Engagement	●	⊙	⊙	○	○	○	●	●
		d. Controlling	●	⊙	⊙	○	○	○	●	●
	IMPROVEMENT	a. Problem Identification	●	●	⊙	⊙	○	⊙	●	●
		b. Opportunity Identification	●	●	⊙	⊙	○	○	⊙	⊙
		c. Root Cause Analysis	●	⊙	⊙	⊙	○	○	⊙	○
		d. Improvement Planning	●	⊙	○	○	○	○	⊙	●
		e. Implementation	●	●	⊙	⊙	⊙	⊙	●	●

Similarly, if there are high operational risks mapped to the Engagement attribute of the Stakeholder Involvement element, the Systems Engineering Technical processes of Stakeholder Requirements Definition, Validation, and Transition should be considered as risk mitigation activities. The Requirements Analysis and Architecture Design processes may also help mitigate the risks. Implementation, Integration, and Verification processes may be of less value when mitigating risks mapped to the Engagement attribute of the Stakeholder Involvement Element.

5.5 ORDERED SUMMARY

This chapter introduced ORDERED, a repeatable method designed to influence systems engineering activities throughout the systems engineering lifecycle with the purpose of improving program outcomes and system operability and usability. Key to the process is a thorough operational risk identification and analysis process that results in operational risk scenarios. The operational risk scenarios are continually identified and evolved throughout the systems engineering lifecycle and used to influence systems engineering decisions from requirements through deployment.

In addition, systems engineering processes themselves may be used to mitigate operational risk, and the ORDERED taxonomy was mapped to the Defense Acquisition Guidebook systems engineering processes to highlight this relationship. The ORDERED process is not intended to replace the systems engineering processes and methods used on a program, but rather it is intended to augment those activities with operational risk considerations.

CHAPTER 6: SURVEY RESULTS

To understand the relationship between operational risk considerations and program outcomes, a survey instrument was developed (see Appendix B). The survey approach followed a recent survey on systems engineering effectiveness conducted by the National Defense Industrial Association Systems Engineering Division, the Institute of Electrical and Electronics Engineers Aerospace and Electronic Systems Society, and the International Council on Systems Engineering[77].

Using a Likert scale consisting of *Not At All*, *A Little*, *Moderately*, *Considerably*, *To A Great Extent*, and *Unknown*, participants were asked to indicate how strongly they supported the statements shown in **Table 24.** Operational risk considerations were defined as actively eliciting operational risk from end-user during the early solution development stages of a program as well as actively and continuously involving end-user perspectives during development to identify and mitigate evolving operational risk throughout the program lifecycle (Questions 6 and 8).

Program performance was defined as meeting cost and schedule expectations, delivering a system that satisfies the end-user’s most critical quality attribute requirements, and

Table 24. Risk Survey Questions

Question Number	Question
1	My program team has a documented risk management process.
2	My program team has an active risk register that reflects the team’s most critical current risks.
3	My program team has a robust, continuous risk identification process.
4	My program team actively mitigates the program’s top risks.
5	The leadership above my program actively elicits risks and helps mitigate risks to my program.
6	My program team actively elicited operational risks and mission threats from customers and end-users during the capture phase.
7	My program team actively elicited quality attributes (responsiveness, adaptability, evolvability, agility, scalability, etc.) during the capture phase.
8	The customer actively participates with the program team during execution to identify and mitigate operational risk.
9	The customer actively participates with the program team during execution to prioritize quality attributes (responsiveness, adaptability, evolvability, agility, scalability, etc.) and evaluate the ability of the solution or service to satisfy critical quality attributes during development.
10	The customer interaction with the program team is positive.
11	My customer would say that the solution or service we deliver mitigates operational risk or mission threats.
12	My customer would say that the solution or service we deliver meets all critical quality attributes (affordability, agility, scalability, etc.).
13	The program team consistently meets all customer cost and schedule objectives.

delivering a system or service that mitigates operational risk (Questions 11, 12, and 13).

In addition, the survey instrument was designed to enable the exploration of the relationship between the existence of an effective risk management process on the program and program outcomes (Questions 1, 2, 3, and 4). Additional questions in the list were asked for purposes other than stated above.

The survey was administered to 104 program managers on October 14, 2015. The programs were classified as solution development, service delivery, and professional services as shown in **Figure 16**.

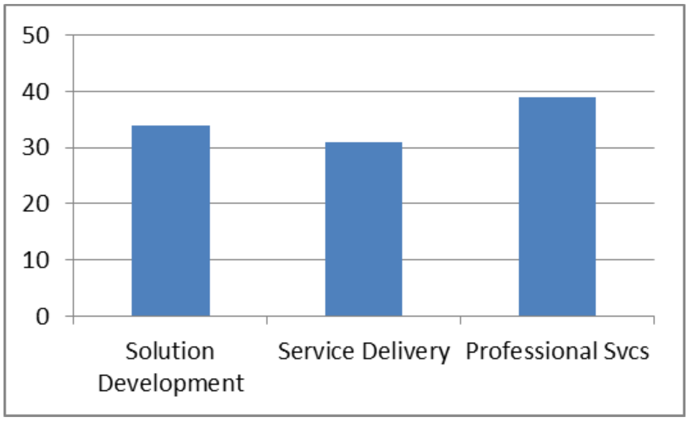


Figure 16. Program Type

A solution development program was defined as a program where the team is responsible for developing and delivering a solution (typically a tangible product such as a software/hardware system) to a customer. A service delivery program was defined as a program where the team is responsible for developing and delivering a service to the customer and is expected to meet customer outcomes, such as service level agreements. A professional services program was defined as a program where the program team is responsible for delivering

qualified staff that provides expertise and works at the direction of the customer to support the customer's mission.

The programs ranged in size from small (under $5 million in annual revenue) to large (over $50 million in annual revenue) as shown in **Figure 17.**

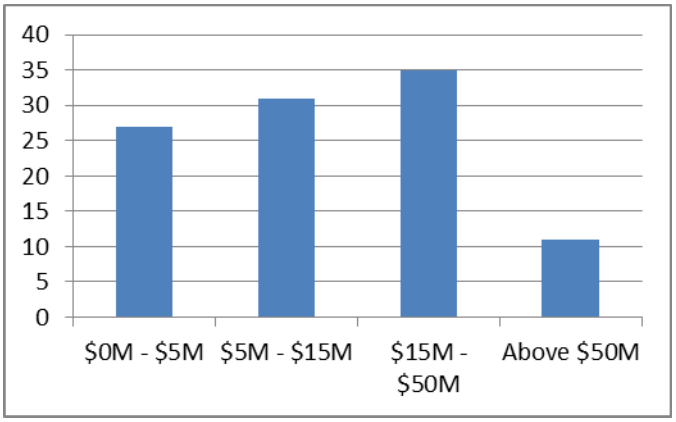


Figure 17. Program Revenue

The results were analyzed by first examining the variation in the responses to the thirteen questions to determine if enough variation existed to allow further analysis. The analysis of the distribution of results shown in **Figure 18** indicates enough variation within and between questions to allow further analysis[78].

The two areas explored here are first the relationship between the existence of an effective risk management process and program performance and second the relationship between an operational risk focus and program performance. Questions 1, 2, 3, and 4 were combined to provide an aggregate score of risk

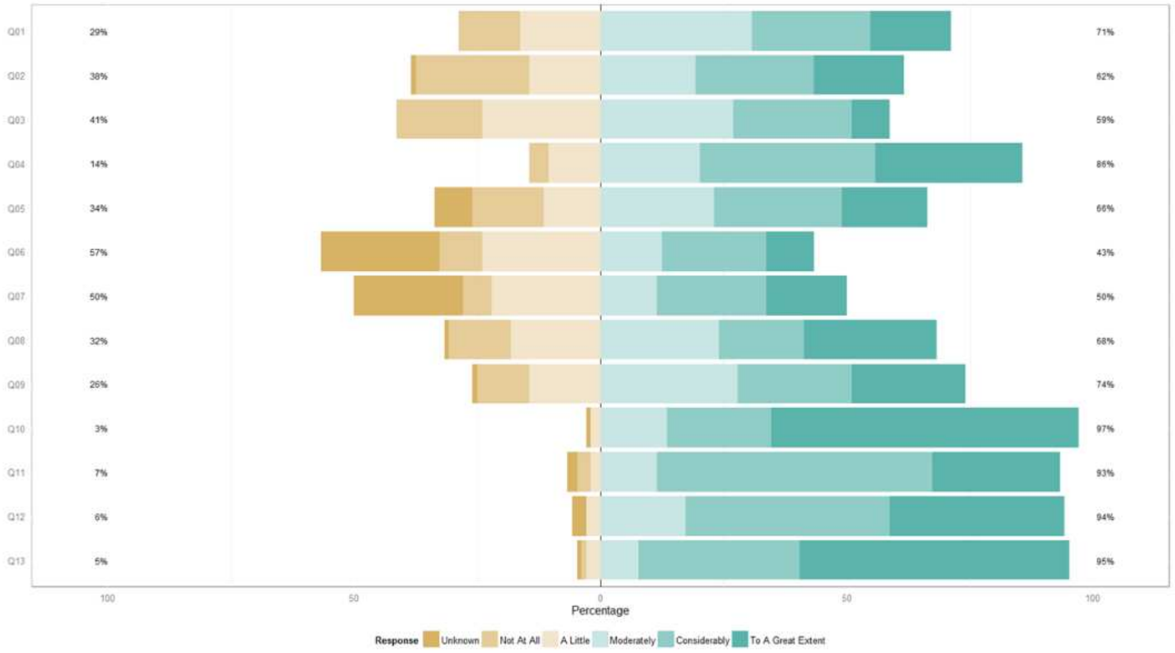


Figure 18. Likert Analysis

process effectiveness. They measure the existence of a documented risk process, the use of a risk register, an active and continuous risk identification and mitigation process, and the program mitigating its most critical risks.

Questions 6 and 8 were combined to provide an aggregate score of operational risk effectiveness. They measure active elicitation of the customer’s operational risks during the program’s capture phase (where early lifecycle solution activities occur) and elicitation and mitigation of operational risk during program execution.

Questions 11, 12, and 13 were combined to provide an aggregate score of program performance. They measure the customer’s perspective of the program meeting cost and schedule objectives, mitigating their most critical operational risks, and delivering a service or solution that meets all expected quality attributes.

Each program's aggregate measure for the three areas, risk process effectiveness, operational risk effectiveness, and program performance, were then divided into three categories indicating the lower third of effectiveness or performance, the middle third of effectiveness or performance, and the top third of effectiveness or performance. **Figure 19** shows the result of risk process capability compared to program performance.

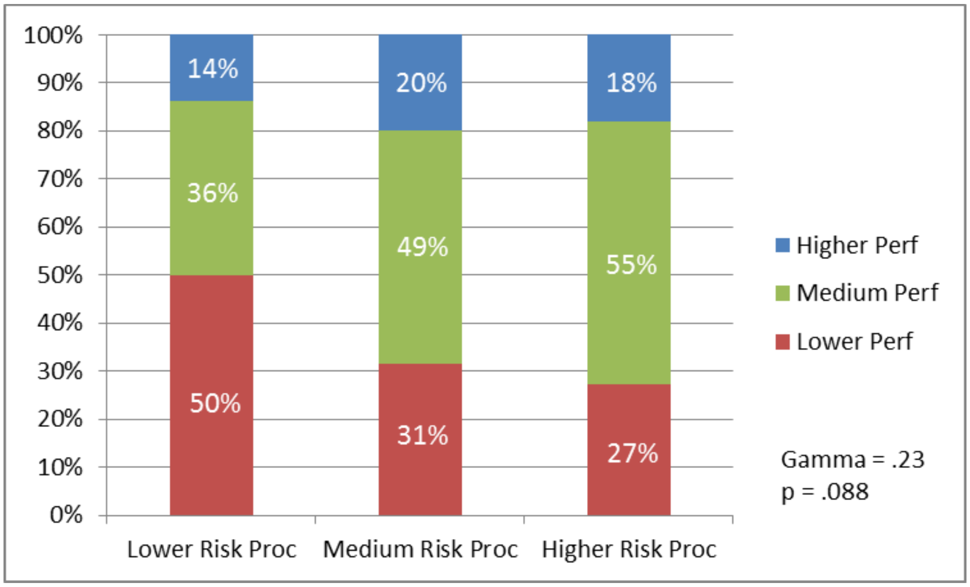


Figure 19. Risk Process Capability and Program Performance

Simply looking at the chart, one might conclude that programs with a more effective or capable risk process perform better than programs with an ineffective risk process. Fifty percent of the programs with lower risk process capability exhibited lower program performance. That number decreased to 31 percent for programs with medium risk process capability and to 27 percent for programs with higher risk process capability.

The number of programs exhibiting higher program performance across the low, medium, and high risk process capability stayed roughly the same, while the programs exhibiting medium program performance increased from 36 percent to 49 percent to 55 percent across the three groups. Performing ordinal logistic regression analysis of the data reveals a Gamma score of .23 and p-value of .088. Gamma is a measure of association that expresses the strength of relationship between two ordinal variables[79] as represented by the equation below.

$$G = \frac{N_s - N_d}{N_s + N_d}$$

N_s is the number of pairs of cases ranked in the same order on both variables, and N_d is the number of pairs of cases ranked in reverse order on both variables. Where there is a tie, the relationship is dropped from the equation. Gamma values of less than 0.2 may be considered as weak, values around 0.3 may be thought of as moderately strong, values near 0.5 are considered strong, and values over 0.6 are very strong.

P-values measure the probability that the observed relationship in the sampled data occurs by chance alone. Values of $p < 0.05$ are used as a basis for rejecting the null hypothesis, that is having confidence that the relationship is not specious[40].

The Gamma score of .23 indicates a weak relationship between the two variables, and a high p-value of .088 decreases our confidence that the relationship observed is valid. In other words, it would be difficult to conclude with certainty using this data that programs with an effective risk process outperform programs with a less effective risk process.

Figure 20 shows the results of comparing the operational risk process capability and program outcomes.

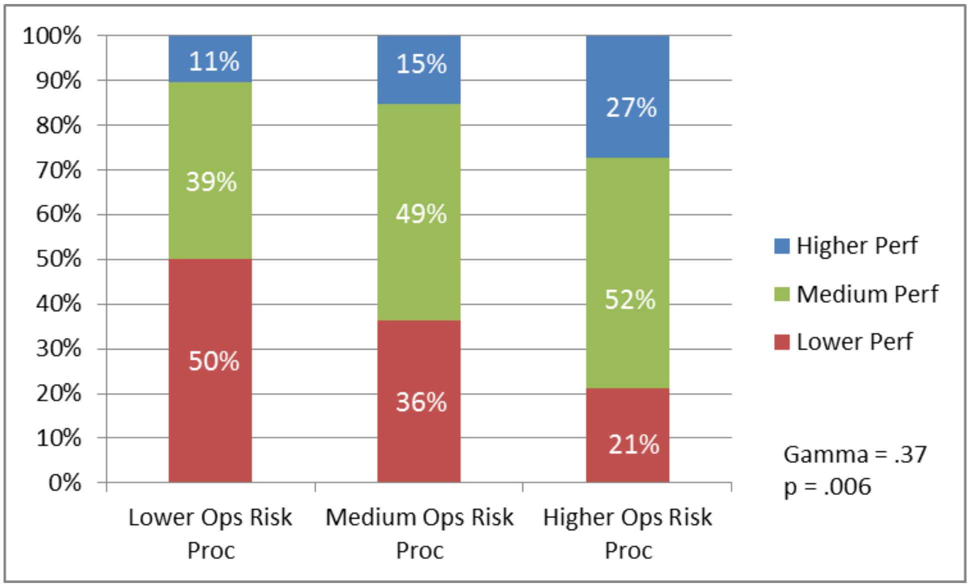


Figure 20. Operational Risk Process Capability and Program Performance

Once again, simply looking at the chart, one might conclude that programs that focus on identifying and mitigating operational risk throughout their lifecycle perform better than programs that don't focus on operational risk. The number of programs exhibiting lower program performance decreased from 50 percent for programs with low operational risk process capability to 36 percent for programs with medium operational risk process capability and to 21 percent for programs with higher operational risk process capability.

Programs exhibiting medium program performance increased from 39 percent for programs with low operational process performance to 49 percent for programs with medium operational process performance and to 52 percent for programs with higher operational risk process performance. Programs exhibiting high program performance increased from 11 percent for programs with lower operational risk process performance to 15 percent for programs with medium operational risk process capability to 27 percent for programs with higher operational risk process capability.

The Gamma score shows a moderately strong to strong positive relationship between the two variables, and the p-value of .006 provides confidence that the relationship is valid.

The above analysis includes all three program types: Solution Development, Service Delivery, and Professional Services. Because systems engineering activities are performed more heavily on Solution Development programs, the analysis was performed excluding the Service Delivery and Professional Services programs.

Figure 21 shows risk process capability compared to program performance. Interestingly, the relationship when looking only at Solution Development programs results in a weak Gamma score and a high p-value. The conclusion is that there is not a valid relationship between risk process effectiveness and program performance for Solution Development programs within the sample.

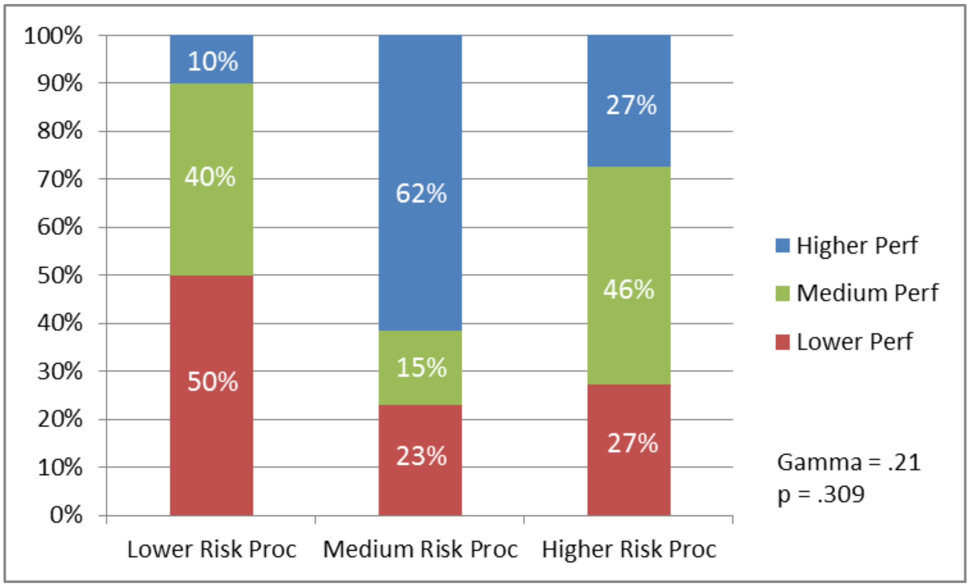


Figure 21. Risk Capability and Program Performance: Solution Development Programs

Figure 19 included all programs and indicated a questionable relationship. However, when evaluating risk process effectiveness and program performance for just Solution Development programs, one could conclude that increasing risk process performance alone would have little or no effect on program outcomes.

Figure 22 shows the results of comparing the operational risk process capability and program outcomes for Solution Development programs only. This comparison results in the strongest relationship of the data analyzed. The number of Solution Development programs exhibiting lower program performance decreased from 46 percent for programs with low operational risk process capability to 36 percent for programs with medium operational risk process capability and to 17 percent for programs with higher operational risk process capability.

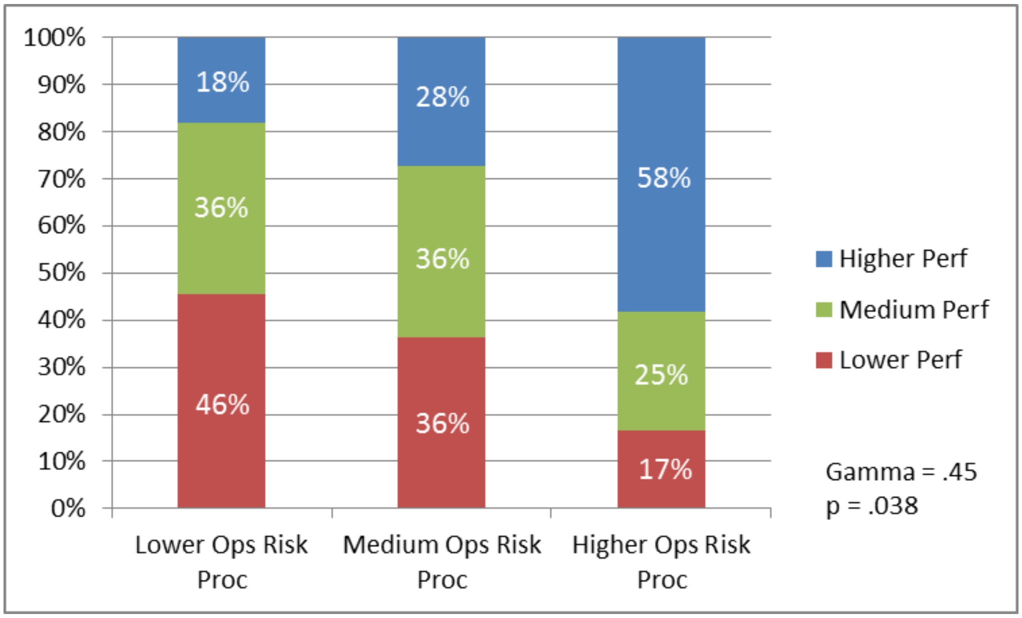


Figure 22. Operational Risk Capability and Program Performance: Solution Development Programs

Solution Development programs exhibiting medium program performance remained steady at 36 percent for programs with low and medium operational process performance and decreased to 25 percent for programs with higher operational risk process performance. Solution Development programs exhibiting high program performance increased from 18 percent for programs with lower operational risk process performance to 28 percent for programs with medium operational risk process capability and jumped to 58 percent for programs with higher operational risk process capability.

The Gamma score shows a strong positive relationship between the two variables, and the p-value of .038 provides confidence that the relationship is valid.

The caution here is that the ordinal logistic regression analysis performed provides only confidence that there is a correlation between an operational risk focus and program performance and an indication of the strength of that relationship. It does not provide a causal relationship. In other words, from the data alone, one cannot conclude that an operational risk focus causes improved program performance or that higher program performance causes higher operational risk process capability. One may only conclude that there is a positive correlation between the variables: they move in the same direction.

Given the strength of the relationship and the low p-value, one may confidently conclude that programs within the sample that focus on operational risk during the program lifecycle also have better program performance than programs that focus less on operational risk during the program lifecycle. This relationship holds and is even stronger when only Solution Development programs are examined.

Further analysis may provide additional insights. Revenue or team size may influence the outcomes of the analysis. Larger programs may have a more formal risk process in place or may have lower program performance due to the inherently higher risk of larger programs.

Service Delivery programs may require stronger risk practices than Professional Services programs, and the influence of operational risk considerations may weigh heavier in program outcomes. This is a first step in the analysis of the relationships between risk, operational risk, and program outcomes, and the results are promising and indicate that more exploration with additional survey instruments may provide even more valuable insights.

CHAPTER 7: MODELING OPERATIONAL RISK

Many factors impact the outcomes of an engineering program, including the complexity of the problem space, the precedents of solutions to address the problem, and the skill and ability of the team solving the problem, among others. Several other measures of success include total cost, user acceptance, and operational effectiveness.

Total cost is a convenient surrogate for the success of a program. If the capability delivered is not acceptable to the user or is deemed operationally ineffective, total cost increases as additional development and re-work is performed to address the user or operability issues.

Operational risk increases when end-user or operability issues exist in a product or capability. If the operational risk is not addressed in a given release, re-work is deferred to subsequent releases. If it is not addressed in subsequent releases, it is deferred into operations and maintenance.

Deferring re-work increases the technical debt of a program[80]. Technical debt is defined by McConnell as *A design or construction approach that's expedient in the short term, but that creates a technical context in which the same work will cost more to do later than it would cost to do now*[81].

In the simplest terms, the total cost of a program is a sum of the total cost of each development release, plus the cost to resolve any residual technical debt not addressed during development, plus the nominal operations and maintenance cost for the life of the capability.

$$TC_p = (\sum_r TC_r) + \ C_{td} + C_{om}$$

The total cost for any given release is the cost for developing features allocated to the release, plus the cost of any operational risk mitigation activities (additional features) performed during the release, plus the cost of the technical debt addressed during the release.

$$TC_r = C_r + C_{or} + C_{td}$$

C_r is the cost for developing each feature of a release.

$$C_r = \sum_k C_r(F_k)$$

C_{or} is the cost for any operational risk mitigation actions performed for a release.

$$C_{or} = \sum_{k} C_{or}(F_k)$$

C_{td} is the cost of technical debt mitigated in this release.

$$C_{td} = \sum_{k} C_{td}(F_k)$$

The dilemma facing most engineering program teams is the trade-off between needing to deliver capability early versus addressing longer-term issues such as supportability and evolvability of the delivered products. Most programs have stakeholders who want to see progress and ensure that the payoff from the program is worth the investment. This creates pressure to keep the program *sold* by demonstrating and delivering value early.

There may also be a pressing operational need that places pressure on the engineering team to deliver capabilities sooner rather than spend time considering longer-term operational attributes such as maintainability. Engineering a solution that is more operationally flexible and adaptable impacts early systems engineering lifecycle activities such as requirements, architecture, and design.

Delaying the engineering activities that allow a more complete infrastructure results in re-working these engineering artifacts later when it is more costly to make changes. These delayed decisions increase technical debt and operational risk.

To simplify and explore the relationship between addressing operational risk by reducing technical debt and the impact on cost and schedule, the simplified model shown in **Figure 23** below was developed using the Vensim system dynamics modeling tool developed by Ventana Systems Inc.

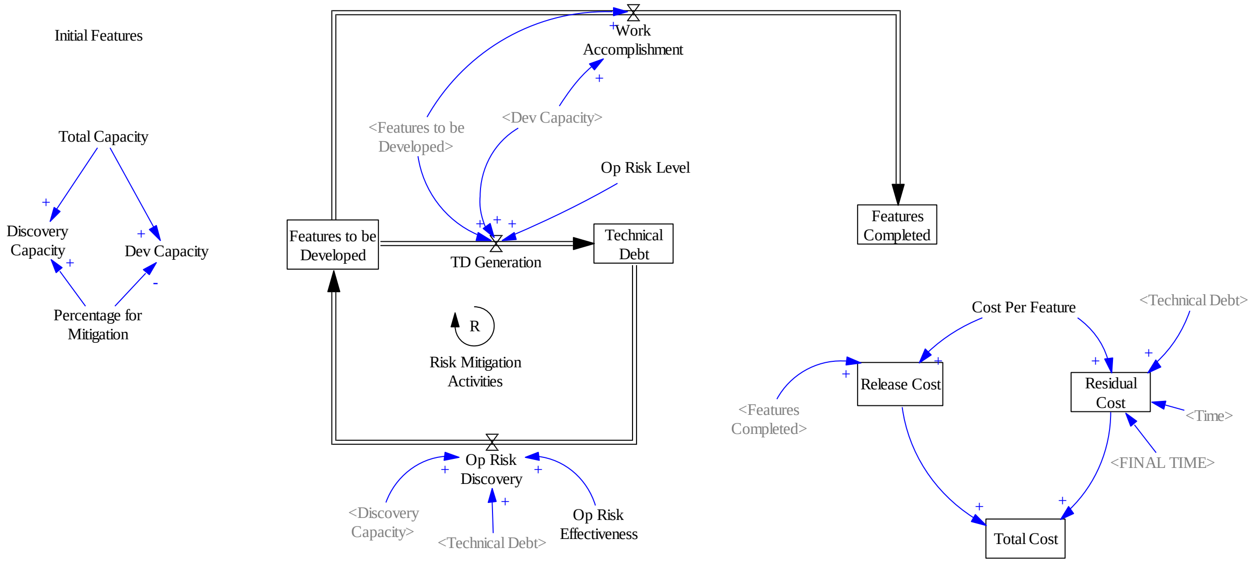


Figure 23. Simplified Operational Risk Model

This model simplifies the interaction during the development phase of a program and simulates a single release. In this model, the initial set of features (Initial Features) represent the development work to be done during the release and becomes the starting point for the work to do (Features to be Developed). Features are normalized so that each feature has the same cost to implement (Cost Per Feature) and the same amount of effort required to complete them.

Capabilities may be comprised of one or more features. A more complex capability would have more features and more cost. For the purpose of this model, the collection of features into capabilities is assumed and not modeled. The program team has a set amount of capacity in terms of features that they may complete in a month (Total Capacity). Some percentage of that capacity may be assigned to develop the planned features (Dev Capacity), and some percentage may be assigned to discover and mitigate operational risk discovered during development (Discovery Capacity).

Depending on the development capacity, a certain amount of work may be performed per month (Work Accomplished), and developed features are moved to the completed state (Features Completed). Technical debt (Technical Debt) grows during development. This debt may grow from deferred decisions, poor quality, and a variety of other causes.

For this model, technical debt increases based on the level of operational risk (Op Risk Level). The level of operational risk represents a disconnect between mission and business needs and the current set of features under development. If mission and business needs have shifted, a certain amount of re-work is required to the features under development.

For example, an operational shift impacting 20 percent of the features would require additional work performed on 20 percent of the features. This re-work is captured as technical debt. Technical debt is discovered based on the program’s ability to recognize operational risk (Op Risk Effectiveness) as well as the amount of resources allocated to discover risk (Discovery Capacity).

As technical debt is discovered, additional work is added to the work to do (Features to be Developed) variable. Some programs elect to ignore technical debt while others allocate some number of resources to discover and address technical debt. Features added because of technical debt that are addressed in a release cost the same to address as other features in the release, however, schedule is impacted, and the cost of the release increases (Release Cost).

Technical debt that is not addressed during the release is much more costly to address. For software systems, addressing technical debt post-deployment may be more than one hundred times more costly than if addressed during development[71].

A NASA study determined that for software systems, the cost to fix problems after deployment ranged from one hundred to one thousand times more than if fixed during development. For systems (integrated hardware and software systems), the cost was twenty-nine to about sixteen hundred times more[82].

For the purposes of this model, the lower value of twenty-nine times more costly is used for technical debt not addressed during the release. The total cost for the program then is the cost of the release plus the cost to address technical debt in operations.

The model was run with all variables fixed with the exception of the number of resources allocated to mitigate operational risk (Percentage for Mitigation). **Table 25** indicates the initial values of all other variables.

Table 25. Initial Model Variables

Initial Model Variables	
Variable	**Value**
Initial Features	648
Completed Features	0
Total Capacity	30
Operational Risk Level	0.2
Operational Risk Effectiveness	0.5
Cost Per Feature	$1,000
Technical Debt	0
Release Cost	0
Residual Cost	0
Total Cost	0

The initial features to be developed was set at six hundred forty-eight features. The capacity of the program team was set at thirty features per month. The operational risk level represents the gap in the system under development and the evolving business and mission needs of the end-user. This was set at 20 percent, reflecting a need to re-work 20 percent of the features to address the operational risk.

Operational risk effectiveness represents the ability of the development team to recognize and translate the growing technical debt into work to be done. This was set at 50 percent, indicating that the development team had a fairly healthy ability to recognize operational risk. The cost of a feature was set at $1,000, and the cost of addressing technical debt during operations was assigned a multiplier of twenty-nine.

The program was simulated with zero, 10 percent, 20 percent, 25 percent, and 30 percent of the program capacity allocated to mitigate operational risk and address technical debt during the release. A value of zero indicated that the program team decided to ignore evolving needs of the end-user as represented by operational risk and deferred all technical debt reduction post-deployment. **Table 26** shows the output of the simulations.

Table 26. Model Outputs

	Model Outputs						
Percentage for Mitigation	**Features Completed**	**Release Months**	**Technical Debt (features) Addressed in the Release**	**Release Cost**	**Residual Technical Debt (features)**	**Residual Cost**	**Total Cost**
0%	648	22	0	$648,000	129.6	$3,758,400	$4,406,400
10%	684	26	36	$684,000	99.3	$2,879,700	$3,563,700
20%	735	31	87	$735,000	57	$1,653,000	$2,388,000
25%	765	34	117	$765,000	29.25	$848,250	$1,613,250
30%	798	38	150	$798,000	4.2	$121,800	$919,800

Ignoring operational risk in order to deliver the initial features allows the program to complete at twenty-two months with a development cost of $648,000. This decision defers the resolution of technical debt into the operations phase where it is much more costly to address. The total cost for this option is $4,406,400.

At the other extreme, allocating 30 percent of development capacity to identify and mitigate operational risk and thereby reducing technical debt stretches the schedule to thirty-eight months. The residual technical debt is the lowest, and the total cost is $919,800, dramatically lower than delivering early. This tradeoff between cost and schedule is shown in **Figure 24** as a Pareto Front allowing decision-makers the ability to explicitly select how much operational risk and technical debt they are willing to mitigate during development at the expense of schedule, versus delivering early and ignoring operational risk at the expense of total lifecycle cost.

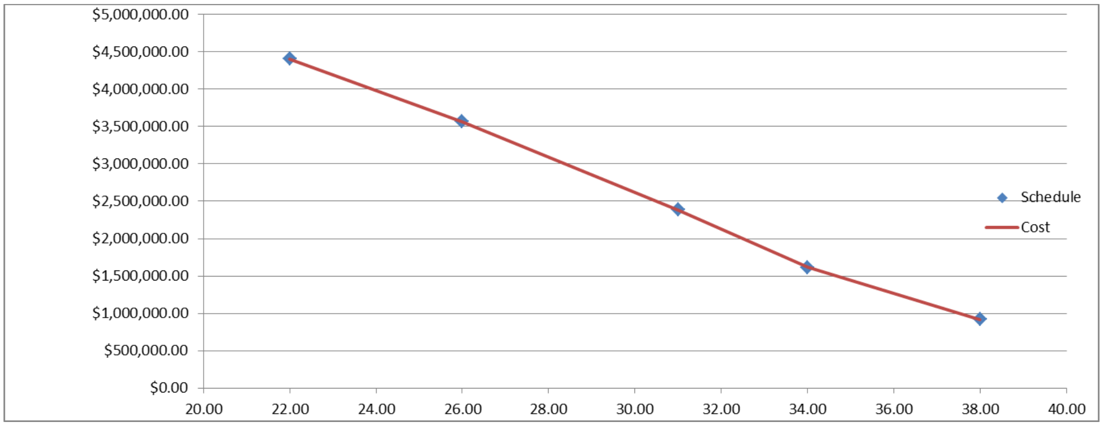


Figure 24. Pareto Front Showing Cost and Schedule Tradeoff

Urgent operational needs may drive decision-makers to ignore operational risk and defer technical debt. They may also not be aware of the impact of ignoring operational risk during development on total cost and opt for the shorter schedule to reduce development costs. Either way, a model such as the one described here could help decision-makers understand the dynamics involved in addressing operational risk and technical debt during development using an explicit approach such as ORDERED.

CHAPTER 8: EVALUATING OPERATIONAL RISK EFFECTIVENESS

The ORDERED approach presented in Chapter 5 describes how the systems engineering activities on a program could be adjusted to ensure that operational risk considerations are addressed throughout a program’s lifecycle. Because ORDERED is a proposed approach, no programs are actively using it, and therefore, evaluating its effectiveness or viability on a program is not possible.

As an alternative, codifying the outcomes as expected characteristics from implementing a comprehensive operational risk management approach such as ORDERED is presented in this chapter, and case studies of completed programs are used to determine if those characteristics were observed in the case study.

Standards have emerged by community consensus and are one way to describe expected characteristics of materials, products, processes, or services. There are several standards organizations and constructs to disseminate characteristics of best practice.

One such set of standards is the Capability Maturity Model Integration initially developed by a joint Government, Industry, and Academia working group with Carnegie Mellon University as the original steward of the models, which are currently maintained by the CMMI Institute[21]. The CMMI model uses a construct that includes both normative material and informative material.

Normative parts of a standard are required or expected in order to be compliant with the standard. Informative material is explanatory material and is used to further define the intent of the standard and provide implementation guidance.

The architecture of the CMMI model includes process areas consisting of goals, practices, and guidance. The goals are required, the practices are expected, and the guidance is informative.

A process area defining the normative and informative characteristics of an Operational Risk Management (ORM) process would need to address areas such as the generalized Basel principles described in Chapter 3 and provided in Table 2. An ORM process area could then be implemented by a variety of users, including banking and military organizations, to establish and evaluate the effectiveness of a general ORM process.

However, ORDERED is a narrow application of operational risk considerations as applied to the systems engineering process of an engineering program. Rather than a general ORM process area, **Table 27** provides a look at goals and practices using the CMMI process area construct defining the

Table 27. Systems Engineering Operational Risk Characteristics

Goal 1	**Engineering Plans Mitigate Operational Risk**	
	Specific Practice 1.1	**Manage Operational Risks** *Operational risks, driven by requirements prioritization decisions, are explicitly captured as risk statements and mitigation plans are developed.*
	Specific Practice 1.2	**Engineering plans mitigate operational risk** *Engineering plans (methodologies, lifecycles, etc.) are developed to mitigate both development and operational risk.*
	Specific Practice 1.3	**Engineering plans are influenced by evolving operational risk** *Engineering plans are evolved when mission or business needs evolve.*
	Specific Practice 1.4	**Transition to operations and support plans mitigate operational risk** *Operational risk considerations influence transition to operations and support plans that are developed or adjusted to mitigate operational risk.*
Goal 2	**Lifecycle engineering activities mitigate operational risk.**	
	Specific Practice 2.1	**End-users participate in systems engineering activities by identifying operational risk** *End-users participate continuously during the systems engineering process by identifying and prioritizing operational risk, taking into consideration evolving mission and business needs.*
	Specific Practice 2.2	**Operational risk considerations validate system requirements** *System requirements are developed and validated based on an analysis of mission and business*

		threats, needs, and operational risk.
	Specific Practice 2.3	**System requirements balance mission and business needs** *Validated system requirements balance short-term mission needs and longer-term business needs.*
	Specific Practice 2.4	**Operational risk considerations influence systems engineering artifacts** *Derived and sub-system requirements, architecture, designs, and technical decisions are influenced by operational risk considerations.*
	Specific Practice 2.5	**Technical solutions are influenced by evolving operational risk** *Technical solutions are evolved when mission or business needs evolve.*
	Specific Practice 2.6	**Operational risk considerations influence technical decisions** *Technical decisions to defer or accelerate capabilities during development are made based on a thorough consideration of operational risk.*

characteristics that should be present if a program is actively addressing operational risk concerns as part of its systems engineering process.

The goals presented represent the required outcomes of actively considering operational risk during development. Engineering plans, such as a Systems Engineering Management Plan, a Software Development Plan, and a Test and Evaluation

Master Plan; the program’s selected methodology such as single-step, incremental, or evolutionary; and the program Work Breakdown Structure, Integrated Master Plan, transition to operations and support plans, and other planning documents are all developed by considering how planning decisions may mitigate operational risk.

To achieve this goal, a program would need to continuously identify operational risk and develop mitigation plans to address the risk. Planning activities and program plans would be developed to mitigate operational risk and evolve when operational risk evolves.

In addition to engineering plans, operational risk should influence systems engineering artifacts and decisions. This would require active participation by operational end-users during engineering activities, analysis of operational risk to develop and validate requirements, and the need to balance near-term mission needs with longer-term business needs when defining and prioritizing requirements.

Technical artifacts such as derived requirements, architecture, design, and engineering trade studies are influenced by operational risk. When mission and business needs evolve, operational risk changes, and engineering artifacts are evaluated for impact and changes incorporated as appropriate to mitigate the evolving operational risk. Decisions to defer or accelerate capabilities are made to either mitigate operational risk or are evaluated to determine if these decisions increase operational risk and whether additional mitigation actions are required.

Publicly available case studies provide a rich set of descriptions of completed programs and the successes or challenges that the programs experienced. Case studies provide an opportunity to evaluate actions, decisions, and outcomes against the practices described in Table 27 to determine if the practice was considered during the program.

The programs evaluated against the practices defined in Table 27 include those that are successful as well as programs that are challenged. This is a subjective evaluation because a program may be described as successful or challenged differently based on the stakeholder.

A program that delivers on time and on schedule but lacks certain quality attributes deemed important to the operational user may be viewed as successful by the program office responsible for managing the program, yet the end-user may view the program as challenged because it fails to meet the operational need. Another program may cost more than planned or take longer or encounter technical challenges during development.

However, the added cost or schedule may have been required to address changes in operational risk or mission threats. Additionally, the way that the program overcame technical challenges may have allowed operational flexibility and better addressed operational needs. This program could be viewed as challenged by the program office yet successful by the end-user. For the case studies presented here, the rationale for whether the program was successful or challenged is presented.

Practices are evaluated as to the level of implementation present in the case study description and assigned a value of High, Medium, or Low based on the criteria defined in the Standard CMMI Appraisal Method for Process Improvement (SCAMPI) Class C[83] as shown in **Table 28.**

Table 28. SCAMPI C Practice Characterization Definitions

Label	**Meaning**
LOW	The intent of the model practice is judged absent or inadequately addressed in the approach. Goal achievement is judged unlikely because of this absence or inadequacy.
MEDIUM	The intent of the model practice is judged to be partially addressed in the approach, and only limited support for goal achievement is evident.
HIGH	The intent of the model practice is judged to be adequately addressed in the set of practices (planned or deployed) in a manner that supports achievement of the goal in the given process context.

The first set of programs evaluated are described as successful programs and are presented in **Table 29.**

Table 29. Case Studies of Successful Programs

Case 1: Business Transformation within a Russian Information Technology Company[3]			Transforming the business through the following activities: • mission analysis and capabilities decomposition • business architecting • planning of the program • implementation of the new business model **Successful** program because the organization recognized a shift in threats to the long-term viability of the organization and implemented a business transformation program to position itself to take advantage of the shift.
	SP 1.1	H	Shifts in external risks threatened the current operational model. The company recognized these threats and developed plans to mitigate them.
	SP 1.2	H	Decisions to select engineering methods (Agile) were based on unknowns associated with a shift in operational needs.
	SP 1.3	H	Early in development, expenditures exceeded resources, delivery of capability took longer than expected, and higher than planned re-work was experienced. A set of principles was established to address these issues based on Agile practices, resulting in disciplined delivery and cost containment.
	SP 1.4	M	Use of a multi-level integrated program team addressed roll-out risks.
	SP	H	Use of a multi-level integrated program team identified changes in

	2.1	🟩	operational needs, found a new solution, generated changes, and updated the plan.
	SP 2.2	H	Entire transformation was undertaken to address perceived shifts in business threats and requirements derived to address these shifts.
	SP 2.3	L	System developed to address long-term business needs, little evidence that short-term mission risks were considered.
	SP 2.4	H	Used capability-based development and selected a system of systems architectural pattern based on business threats.
	SP 2.5	M	Some changes were made based on lack of progress, but there was little evidence that technical solutions were re-evaluated or evolved.
	SP 2.6	L	The need for corporate knowledge capture was identified as a risk but not addressed until after the system was deployed.
Case 2: The Hubble Space Telescope[84]	The Hubble Space Telescope (HST) was launched into low Earth orbit in 1990 and remains in operation. With a 2.4-meter mirror, Hubble's four main instruments observe in the near ultraviolet, visible, and near infrared spectra. **Successful** program because the telescope is well known as a marvel of science fulfilling critical operational needs and because of engineering design decisions that accommodated operational risk during the life of the program, allowing evolution post-deployment after a critical design flaw was detected.		
	SP 1.1	H	Extensive operational mission analysis was conducted with outcomes influencing plans based on technical and operational risk, including

		🟩	decisions to allow on-orbit modification of components.
	SP 1.2	H	Plans were developed to include program phases designed to accommodate discovery and mitigation of risk through the program lifecycle. Trade-studies, independent review teams, simulations, laboratory experiments, and ground testing activities were designed to reduce engineering and operational risk.
	SP 1.3	M	While many plans were clearly adjusted based on evolving operational risk, verification plans were not adjusted when testing of the mirror indicated. Additional analysis was required.
	SP 1.4	M	Operations and support plans were developed and adjusted based on operational risk scenarios. Specifically, the original plan to retrieve and re-launch the HST every five years was abandoned for on-orbit maintenance. These plans, however, assumed the continuation of the Space Shuttle program, and on-orbit maintenance is on hold until a robotic alternative is developed.
	SP 2.1	H	NASA created an Institute to ensure that the astronomer-scientist customer had a direct say in what the HST would actually be able to do. The Institute had direct influence over initial requirements, design, development, and on-orbit operations and maintenance.
	SP 2.2	H	Extensive operational mission analysis activities were performed and influenced system requirements.
	SP 2.3	M	Cost considerations appeared to influence requirements over technical or operational considerations.

		🟨	However, most decisions impacting requirements went through exhaustive trade studies and analysis.
	SP 2.4	H	Due to the known operational risk associated with potential problems detected post-launch, engineers had designed the system specifically for on-orbit servicing to upgrade instruments and change out degradable components. Instruments were designed for ease of removal and replacement.
	SP 2.5	H	Once the error in the mirror was detected, engineers developed a solution to correct the problem on-orbit.
	SP 2.6	L	Due to schedule and cost pressures, NASA ignored indicators that there were problems from at least two tests used to align the test apparatus and check the correct radius of the primary mirror. At the conclusion of the testing activities, management abandoned the review of all data for the final report and re-assigned the team as a cost-cutting measure.
Case 3: Mission Integration and Development[85, 86]	The Mission Integration and Development (MIND) program is a complete lifecycle contract to develop, integrate, operate, and maintain the National Reconnaissance Office's (NRO's) Future Imagery Architecture system, integrating core ground common services and numerous space and ground-based systems and providing a state-of-the-art intelligence infrastructure. The MIND contract was awarded in April 1999 to a multi-company team under the leadership of the Raytheon Company. **Successful** program because the MIND program accomplished all major milestones on schedule and continually exceeded the operational availability specification of 98 percent (averaging over 99.5 percent) since the first transition to operations in December 2003. This initial delivery into operations was performed		

	on cost and on schedule (to the day) as established four and a half years earlier in the original proposal.		
	SP 1.1	H	The initial development was completed in seven increments. The initial increments established the infrastructure and tested high-risk designs and operational concepts. This strategy later enabled MIND to accept major changes driven by operational risk evolution without baseline delivery schedule changes.
	SP 1.2	H	The program used incremental development, event-based reviews, and Integrated Product Teams with customer representation to ensure operational risks were accommodated. They also used proven process technology as recognized by Malcolm Baldridge awards, CMMI, and International Organization for Standardization (ISO) 9001:2000/AS9100:2001 compliance.
	SP 1.3	H	Incremental development and delivery of system in blocks provided opportunities for customer feedback, incorporation of new requirements, and changes to existing requirements based on operational considerations.
	SP 1.4	H	Implementation of incremental deployment of the system in blocks performed to mitigate operational risk. The transition occurred so smoothly that it received special recognition from the NRO.
	SP 2.1	H	MIND developed a series of Early Interface Tests as a risk reduction technique. The contractor employed a full-time staff at the Government operational sites to perform operational integration activities, facilitate end-user feedback, and

			address problems or issues immediately. The customer was an active member of the MIND team, participating in a wide range of planning, review, and decision activities to include risk identification and mitigation.
	SP 2.2	H	The initial increments established the infrastructure and tested high-risk designs and operational concepts.
	SP 2.3	M	A series of Engineering Review Boards and the Program Control Board, which is the controlling authority for risk and management reserves, approved all technical baseline changes after considering operational need and cost impacts.
	SP 2.4	M	The program used a structured architecture-based development approach, which allowed the customer to participate in the engineering process and ensured that the requirements derived for the program supported the design and that the design was appropriate for the mission needs.
	SP 2.5	H	The engineering approach (incremental) and architectural approach (separation of concerns) allowed the MIND program to accept major changes without baseline delivery schedule changes.
	SP 2.6	M	Additional block updates occurred after deployment, but it is unclear if technical capability was deferred or accelerated.
Case 4: Enterprise Resource Planning Systems	Implementation of an Enterprise Resource Planning (ERP) system at a manufacturing subsidiary of a multinational pharmaceutical firm deploying a single instance of specific technical skills across a large number of sites		

Implementation at Pharma Inc.[87]	worldwide. **Successful** program because the system went live as expected, on time and within budget, and the program team was able to achieve a rapid ramp-up to full production earlier than planned (seven weeks instead of the predicted nine weeks after going live).		
	SP 1.1	H	Planning decisions were driven by the business threat of failing a Food and Drug Administration audit, which would have long-term impacts on the financial viability of the company. This operational risk was clearly articulated and communicated as the driving need for the program.
	SP 1.2	H	The implementation team selected a negotiated engineering process rather than a standard plan-driven process. This allowed a dialogue between end-users, ERP integrators, and ERP product vendors as they negotiated needs, extension capabilities, and ERP configurability as they converged within the solution space.
	SP 1.3	H	Legacy data integrity issues were discovered after initial planning, and in response, the program team created a dedicated data maintenance team of seventeen full-time equivalents and ensured that data going into the new system was clean, valid, and in the right format.
	SP 1.4	M	Local end-users participated in the program work streams, and integration specialists were charged with mitigating the anticipated impact to business and mission tasks during transition.
	SP 2.1	M	End-users were encouraged to voice uncertainty during development and raised concerns about the ERP transition impacting customer

			satisfaction and their ability to distinguish their work from competitors. Because this was a global implementation, some end-users at remote sites weren't as engaged in identifying mission and business impacts of the new system.
	SP 2.2	H	The exploration/negotiation process used by the company allowed for influence of the requirements based on operational risk.
	SP 2.3	M	Requirements were sub-optimized to mitigate longer-term business needs and tended to ignore more urgent mission needs of end-users. However, this decision was explicit and well-communicated throughout the implementation.
	SP 2.4	H	This implementation of the ERP system was in the highly-regulated pharmaceutical sector, which requires operational risk considerations to influence detailed implementation decisions, such as quality, safety, traceability, and transactional integrity.
	SP 2.5	M	The company used a dual cycle of exploration/negotiation, allowing the resulting implementation to produce a stable corporate template acceptable to most site requirements. This enabled product evolution based on changing user needs. While most of the interaction between development team and end-user was positive, there was some evidence that when end-users requested changes that were required based on operational need, their requests were ignored, and they were told to use the system as is and to absorb the operational impact.

	SP 2.6	L	Schedule pressure influenced the team to defer planned tasks rather than evaluate the impact of the deferral decision on operational risk.

The second set of programs evaluated are described as challenged programs and are presented in **Table 30**.

Table 30. Case Studies of Challenged Programs

<table>
<tr><td rowspan="4"><b>Case 1: Titan Survey portion of the NASA/ESA Cassini-Huygens Mission to Saturn[3]</b></td><td colspan="3">The Titan survey portion of the Cassini-Huygens mission involved the Huygens lander separating from the Cassini orbiter and commencing a one-way, two and a half-hour descent into Titan's atmosphere. Its modest transmitter sent data back to the orbiter, which relayed the information to Earth.

<b>Challenged</b> program because the program team ignored operational risks associated with the design of the communication link between the orbiter and the lander not accounting for Doppler shift. These issues were identified during development and ignored due to cost and schedule pressures, forcing the team to address the issues after launch at greater expense and the risk of mission failure.</td></tr>
<tr><td>SP 1.1</td><td>M</td><td>Operational risk of communication issues between the lander and the orbiter were identified but not addressed due to cost and schedule pressure.</td></tr>
<tr><td>SP 1.2</td><td>L</td><td>A traditional development approach was selected. The decision to divide the work between the European Space Agency (ESA) and NASA was made based on political motivation, not on desire to mitigate operational risk associated with interface complexity.</td></tr>
<tr><td>SP</td><td>L</td><td>Plans were not adjusted when risks of inter-operability issues were</td></tr>
</table>

	1.3		raised. Testing did not reflect operational environment, and requests for high-fidelity radio testing between the orbiter and the lander were ignored due to budget constraints.
	SP 1.4	L	The launch date was held even though scientists raised concerns about potential Doppler shift phenomenon.
	SP 2.1	H	Scientists participated during development and identified the risk of ignoring the Doppler shift between the orbiter and the lander.
	SP 2.2	L	No evidence requirements were adjusted based on operational risk of inter-operability between the orbiter and the lander.
	SP 2.3	L	The program team appeared to prioritize development cost and schedule and ignored both mission and lifecycle cost considerations.
	SP 2.4	L	Architectural and design decisions did not account for interface issues between the orbiter and the lander.
	SP 2.5	L	The component selected by the ESA vendor did not address operational risk of Doppler shift.
	SP 2.6	L	The program team ignored operational risk during development and deferred further analysis until after launch. Although the travel time would be approximately seven years from Earth to Saturn, less costly changes to components or designs were impossible after launch. Heroic engineering activities saved the mission at higher cost using sub-optimal solutions.
Case 2: Denver International	Implementation of an airport-wide, information technology-based baggage handling system at		

Airport Baggage Handling System[88]	Denver International Airport (DIA) intended to dramatically improve the efficiency of luggage delivery. The system composed of fifty-five networked computers, five thousand electric eyes, four hundred radio frequency receivers, and fifty-six barcode scanners was to orchestrate the safe and timely arrival of every suitcase and ski bag at DIA. **Challenged** program because by the time the airport opened in late February 1995, it was sixteen months behind schedule and close to $2 billion over budget, causing DIA to abandon its previous commitment to build an airport-wide automated baggage handling system to support the airport when initially opened.		
	SP 1.1	L	Only three firms bid on the contract, and Denver's consulting firm recommended against all three submitted designs on the grounds that the configurations would not meet the airport's operational needs. The contract was awarded to BAE, who originally declined to bid on the program because of the complexity and the lack of time to complete the program.
	SP 1.2	L	Based on schedule constraints, the system was initially deployed without thorough engineering studies performed.
	SP 1.3	L	When the system failed its first operational test, the program wasn't re-planned, rather more pressure was placed on the program team to deliver as planned to support the opening of the airport.
	SP 1.4	M	The opening of the airport was delayed based on the results of operational testing and lack of progress developing a baggage handling system.

	SP 2.1	L	DIA management relied on BAE to understand the operational environment and mitigate operational risk.
	SP 2.2	L	The BAE system was described as highly advanced and theoretically capable of living up to its promised capabilities, but lack of validation of the requirements and designs in an operational environment caused the system to not be able to achieve stable and reliable operations.
	SP 2.3	L	Schedule considerations drove the lack of engineering trade studies and modeling that could have improved system design.
	SP 2.4	L	BAE did not perform validation of the designs and technical solutions selected based on operational need.
	SP 2.5	M	The fully automated system was too complex and unable to meet the operational need, causing DIA to abandon the design due to operational risk.
	SP 2.6	M	Operational risk drove DIA to abandon the airport-wide computerized baggage handling system and instead opted to support two concourses with a manual baggage system and one concourse with a scaled-down semi-automated system.
Case 3: The Air Force's Expeditionary Combat Support System[89]	The Expeditionary Combat Support System (ECSS) program was intended to transform how the Air Force manages its global logistics and supply chain network in support of its operations worldwide. Part of the effort was to overhaul or retire hundreds of legacy computer systems. **Challenged** program because the result after eight years of development was an abandoned system, a waste of $1.1 billion in taxpayer money, and the need to maintain multiple,		

	inadequate logistics systems far inferior to the promise of ECSS.		
	SP 1.1	M	The Air Force identified cultural resistance to change and lack of leadership as potential problems in 2004, yet it failed to mitigate these operational risks.
	SP 1.2	L	The program failed to follow the required Business Process Re-engineering (BPR) approach required of major information technology programs. This lack of adherence to the BPR process meant a failure to examine operational processes and risks and to develop plans based on the assessment.
	SP 1.3	L	The program failed to follow appropriate change management processes during program execution.
	SP 1.4	L	High levels of resistance to change within the end-user community was allowed to fester without addressing transition into operations plans.
	SP 2.1	L	The Air Force failed to clearly communicate with ECSS end-users or allow them to adequately participate in program development activities. This lack of participation decreased buy-in and acceptance from end-users.
	SP 2.2	L	The Air Force failed to follow acquisition best practices and did not establish a set of validated and stable requirements for the program.
	SP 2.3	L	The Air Force failed to highlight the expected improvements to long-term operations of the new system. Cost avoidance was prioritized over mission impact.

	SP 2.4	L	Lack of end-user participation, program delays, and cost pressure caused the design team to forego appropriate operational risk considerations.
	SP 2.5	L	Early in the program, requirements changes due to operational need changes was identified as a high risk that would increase costs and cause scheduling delays. However, this risk was never addressed and served as a contributing cause of the program's failure.
	SP 2.6	L	Decisions to add, decrease, or remove capabilities were made without regard to impact on cost, schedule, and usability. Contributing to this lack of consideration was the fact that the program had six different program managers during the program's eight years, who weren't always privy to decision rationale.
Case 4: The Marine Corps' Expeditionary Fighting Vehicle[90, 91, 92, 93]	The Expeditionary Fighting Vehicle (EFV) was planned to be an armored amphibious vehicle that was initiated in 1988 to replace the 1970s-era Amphibious Assault Vehicle. The EFV was an armored, fully-tracked infantry combat vehicle operated by a three-person crew designed to carry seventeen combat-equipped Marines. It was designed to roll off a Navy amphibious assault ship, move under its own power to the beach, and cross the beach and operate inland. **Challenged** program because of cost growth and changing requirements driven by mission threats that evolved since the program was originally conceived. Improvised Explosive Devices (IEDs) were not prevalent in 1988, and the design had the EFV too close to the ground and vulnerable to an IED taking out the vehicle and its occupants. Also, advances in longer-ranged, shore-based, anti-ship cruise		

	missiles put the Navy's amphibious ships disembarking EFVs at their twenty-five-mile operating limit vulnerable to attack requiring a change in operational concepts and designs. Program delays, rising costs, and a decrease in the number of vehicles ordered drove the cost of each vehicle to over $24 million each. As a result, the EFV program requested an additional $11.163 billion in 2011 and was subsequently cancelled with only five prototype vehicles delivered after twenty-three years of sunk development cost.		
	SP 1.1	🟥 L	The Expeditionary Fighting Vehicle was designed to mitigate the risks of a World War II enemy requiring U.S. Marines to conduct assaults on the shores of an enemy. While it was recognized that the threat evolved, little was done to mitigate mission evolution risks.
	SP 1.2	🟥 M	Plans included traditional long development lifecycles with system delivery at the end. No evolution was built into the engineering plans, but plans did include operational readiness testing where many issues were uncovered.
	SP 1.3	🟥 L	When mission threats changed, the program was slow to react and required major, costly re-designs and eventually was canceled because it couldn't meet the evolving threats.
	SP 1.4	🟥 M	Transition plans included operational readiness testing with prototypes, which allowed the end-user to express concerns about the lack of effectiveness of the vehicle.
	SP 2.1	🟨 L	The Expeditionary Fighting Vehicle was a model acquisition program that won numerous awards early in its lifecycle. As an acquisition reform

		🟨	program, the prime contractor was given more leeway and less government oversight. End-user involvement began in earnest during operational readiness testing in 2006, at which time the prototype was viewed as operationally ineffective with concerns that the vehicle would wear out under normal operating conditions.
	SP 2.2	L	Requirements were developed based on the last war, and little validation of requirements was conducted.
	SP 2.3	L	System requirements were not balanced. The desire to specify a vehicle for both amphibious landing as well as over-land operations resulted in requirements that were sub-optimized for both needs.
	SP 2.4	M	The program was forced to repeat the System Design and Development phase to address operational risks such as better protection against sea water, a strengthened gun turret, and trim tabs to make the vehicle more stable in the water. This added $143 million in development costs and a schedule slip of four years.
	SP 2.5	L	The program was slow to react to changes in mission threats, and changes in technical solutions became too costly to allow the program to continue.
	SP 2.6	L	Decisions to relax requirements and subsequent decisions to decrease the number of vehicles acquired were based on cost rather than operational risk.
CASE 5: New York Subway Communications	In 1999, officials in New York City hired contractors to develop a new communications system to allow law enforcement personnel to communicate both underground and above ground		

<table>
<tr><td rowspan="5"><b>System</b>[94, 95]</td><td colspan="3">during emergency situations. The goal of the program was to develop a network that would make it possible for law enforcement personnel to talk across department and organizational lines. Program completion would be in 2004 at a cost of $115 million.

<b>Challenged</b> because government and contractor program managers ignored technical issues associated with operability of the system that could cause interference when they were raised in 2001. Schedule and political pressure caused the team to continue with a failed design rather than re-design the transmission components of the system.

Police users said in 2004 that they would not use the system unless the interference issues were fixed. The decision was made in 2005 to fix the problems after delivery. The program was completed three years late in October of 2007 after spending $140 million, a 22 percent cost overrun.

However, because of interference issues, the implementation was halted due to lack of operational effectiveness. At the time, fixing the problem was expected to increase the cost of the program to $210 million, an 83 percent budget overrun.</td></tr>
<tr><td>SP 1.1</td><td>L</td><td>Program managers ignored operational risk of frequency interference even though the concern was widely known and communicated.</td></tr>
<tr><td>SP 1.2</td><td>L</td><td>The program team did not plan for operational risk mitigation actions such as prototype development or early operational testing.</td></tr>
<tr><td>SP 1.3</td><td>L</td><td>Plans were not adjusted when operability issues were raised.</td></tr>
<tr><td>SP 1.4</td><td>L</td><td>Operational risk was ignored, and deployment plans were held even though technical debt was</td></tr>
</table>

			increasing.
	SP 2.1	M	The police department raised the issue of interference and lack of operability, but the program team actively ignored its input.
	SP 2.2	L	Operational risk concerns were ignored and requirements held even though the concerns were known early.
	SP 2.3	L	Cost considerations outweighed mission needs.
	SP 2.4	L	Operational risks were ignored, and a failed design was allowed to continue.
	SP 2.5	L	The technical solution selected failed to meet the operational need.
	SP 2.6	L	The program team decided to delay addressing known operational risks based on cost and schedule. The resulting system was unusable.

Table 31 provides a summary of the successful and challenged programs along with the evaluation of those programs against the systems engineering operational risk characteristics described in Table 27. In addition, each program was scored numerically by simply assigning a value of 1 for each Low, 3 for each Medium, and 5 for each High characterization. This provides the ability to quickly compare scores across programs.

Programs identified as successful had a higher score than programs identified as challenged. The results would imply that the successful programs addressed operational risk

Table 31. Summary of Successful and Challenged Programs

Successful Programs										
	SP 1.1	SP 1.2	SP 1.3	SP 1.4	SP 2.1	SP 2.2	SP 2.3	SP 2.4	SP 2.5	SP 2.6	Score
Case 1	H	H	H	M	H	H	L	H	M	L	38
Case 2	H	H	M	M	H	H	M	H	H	L	37
Case 3	H	H	H	H	H	H	M	M	H	M	44
Case 4	H	H	H	M	M	H	M	H	M	L	38
										Average	39.25
Challenged Programs											
	SP 1.1	SP 1.2	SP 1.3	SP 1.4	SP 2.1	SP 2.2	SP 2.3	SP 2.4	SP 2.5	SP 2.6	Score
Case 1	M	L	L	L	H	L	L	L	L	L	16
Case 2	L	L	L	M	L	L	L	L	M	M	16
Case 3	M	L	L	L	L	L	L	L	L	L	12
Case 4	L	M	L	M	L	L	L	M	L	L	16
Case 5	L	L	L	L	M	L	L	L	L	L	11
										Average	14.2

considerations, either explicitly or inadvertently, more than challenged programs. However, given the subjective nature of this evaluation technique, additional research may be required to convince a program team to implement an approach that allows operational risk considerations to influence systems engineering activities during program execution.

Several practices defined in Table 27 did not score well in either successful of challenged programs. Neither set of programs as a group did well in managing the balance between short-term mission needs and longer-term business needs (SP 2.3). Cost and schedule drivers tended to drive decisions over mission and business needs.

Similarly, when capabilities were deferred or accelerated, cost and schedule played a key role in these decisions over the consideration of the operational risk impacts of the decision (SP 2.6). Of the practices related to planning, few programs considered operational risk when developing transition and deployment plans (SP 1.4). While these practices seem important to program success based on experience and judgment, their lack of presence in successful programs indicates that further exploration is required before including them in a standards-like description of systems engineering operational risk.

CHAPTER 9: CONCLUSIONS AND FUTURE RESEARCH

The purpose of this research was first to define the activities that could be used by systems engineers to ensure that engineering activities are influenced by operational risk considerations. Secondly, to determine if a focus on operational risk during the systems engineering lifecycle has a positive impact on program outcomes.

A structured approach to addressing operational risk during the systems engineering process, Operational Risk-Driven Engineering Requirements/Engineering Development (ORDERED), was introduced, and an exhaustive operational risk taxonomy was developed to allow systems engineers to incorporate the end-user’s evolving operational risk considerations into systems engineering activities.

To examine the relationship between operational risk considerations during the systems engineering process and program outcomes, a survey instrument was developed and administered, a system dynamics model developed, and case studies of successful and challenged programs were evaluated against characteristics of successfully implementing an operational risk focus. These activities led to the conclusion that a focus on operational risk during the systems engineering lifecycle has a positive impact on program outcomes.

This research focused primarily on program-level activities, those activities within the systems engineering lifecycle from user needs analysis through deployment and support of a given system, component, or capability. The results of identifying and applying operational risk considerations within the program systems engineering activities as shown in this research were promising. Additional work is required to institutionalize operational risk thinking within existing systems engineering lifecycle activities based on the ORDERED approach described here or other similar approaches.

Another area of further research would be applying these concepts at an enterprise level. Programs within a portfolio are typically linked by a common mission set and are funded through the same or similar sources.

As operational risk evolves, priorities change. An enterprise may need to re-direct attention and resources to expedite some programs, slow others down, or cancel some programs altogether. They may find that they need to initiate new programs to address the evolving risk if existing programs are unable to accommodate change.

In a study by the National Academy of cost growth of NASA missions, the authors note that ...*cost growth in one mission may induce organizational re-planning that delays other missions in earlier stages of implementation, further amplifying overall* *cost growth. Effective implementation of a comprehensive, integrated cost containment strategy, as recommended herein, is the best way to address this problem*[96]. An integrated strategy would benefit from operational risk considerations to balance cost containment considerations.

REFERENCES

1. Wiley, *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. 2015: Wiley.

2. Elm, J.P. and D.R. Goldenson, *The Business Case for Systems Engineering Study: Results of the Systems Engineering Effectiveness Survey*. 2012, DTIC Document.

3. Pyster, A., et al., *Guide to the Systems Engineering Body of Knowledge (SEBoK) v. 1.0. 1.* Guide to the Systems Engineering Body of Knowledge (SEBoK). 2012.

4. Wrubel, E. and Jon Gross, *Contracting for Agile Software Development in the Department of Defense: An Introduction (CMU/SEI-2015-TN-006)*. 2015. Retrieved August 22, 2015, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=442499.

5. *Performance of the Defense Acquisition System 2015 Annual Report,* Under Secretary of Defense, Technology, and Logistics (USD[AT&L]), Editor. 2015.

6. Ellis, R.F., R.D. Rogers, and B.M. Cochran, *Joint Improvised Explosive Device Defeat Organization (JIEDDO): Tactical Successes Mired in Organizational Chaos; Roadblock in the Counter-IED Fight*. 2007, DTIC Document.

7. Aronin, B.S., et al., *Expeditionary Combat Support System: Root Cause Analysis*. 2011, DTIC Document.

8. McCain, J., *Floor Remarks by Senator John McCain on the Air Force's ECSS Program*. 2014, Available from: http://www.mccain.senate.gov/public/index.cfm/2014/7/floor-remarks-by-senator-john-mccain-on-the-air-force-s-ecss-program.

9. Egyed, A. and I. Schaefer, *Fundamental Approaches to Software Engineering: 18th International Conference, FASE 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015, Proceedings*. Vol. 9033. 2015: Springer.

10. David, A.R., *The pyramid builders of ancient Egypt: a modern investigation of pharaoh's workforce*. 2002: Routledge.

11. Stille, A., *The World's Oldest Papyrus and What It Can Tell Us About the Great Pyramids*, in *Smithsonian Magazine*. 2015, Smithsonian Institute. p. 26-37.

12. Judah, T.D., *A Practical Plan for Building the Pacific Railroad: San Francisco, January 1, 185*7. 1857: H. Polkinhorn, printer.

13. Boehm, B. and J.A. Lane, *Using the incremental commitment model to integrate system acquisition, systems engineering, and software engineering.* CrossTalk, 2007. 19(10): p. 4-9.

14. Covello, V.T. and J. Mumpower, *Risk Analysis and Risk Management: An Historical Perspective.* Risk Analysis, 1985. 5(2): p. 103-120.

15. Chavez-Demoulin, V., P. Embrechts, and M. Hofert, *An extreme value approach for modeling operational risk losses depending on covariates.* Journal of Risk and Insurance, 2015.

16. Ho, W., et al., *Supply chain risk management: a literature review.* International Journal of Production Research, 2015. 53(16): p. 5031-5069.

17. Dionne, G., *Risk Management: History, Definition, and Critique.* Risk Management and Insurance Review, 2013. 16(2): p. 147-166.

18. Mehr, R.I. and B.A. Hedges, *Risk management in the business enterprise*. 1963: RD Irwin.

19. Teller, J., A. Kock, and H.G. Gemünden, *Risk management in project portfolios is more than managing project risks: a contingency perspective on risk management.* Project Management Journal, 2014. 45(4): p. 67-80.

20. PMI, *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*. 2013, Project Management Institute, Incorporated.

21. Chrissis, M.B., M. Konrad, and S. Shrum, *CMMI for development: guidelines for process integration and product improvement*. 2011: Pearson Education.

22. Department of Defense, *DoD Instruction 5000.02*, in *Operation of the Defense Acquisition System*, January. 2015.

23. Department of Defense, *Department of Defense Risk Management Guide for Defense Acquisition Programs*. 2014, Office of the Deputy Assistant Secretary of Defense for Systems Engineering.

24. NASA, *2015 Report on NASA's Top Management and Performance Challenges*, N.O.O.I. GENERAL, Editor. 2015.

25. Jarrow, R.A., *Operational risk. Journal of Banking & Finance*, 2008. 32(5): p. 870-879.

26. BIS. *BIS history, overview*. 2016 [cited 2016 17 January], Available from: http://www.bis.org/about/history.htm.

27. Investopedia. *Group of Ten, G-10*. 2016 [cited 2016 17 January]; Available from: http://www.investopedia.com/terms/g/groupoften.asp.

28. Curti, F., et al., *Benchmarking Operational Risk Models.* Available at SSRN 2741179, 2016.

29. Power, M., *The invention of operational risk.* Review of International Political Economy, 2005. 12(4): p. 577-599.

30. BIS, *Principles for the Sound Management of Operational Risk*. 2011, Basel, Switzerland: Bank for International Settlements Communications.

31. Chernobai, A., A.K. Ozdagli, and J. Wang, *Business Complexity and Risk Management: Evidence from Operational Risk Events in US Bank Holding Companies.* Available at SSRN, 2016.

32. Curts, R.J. and D.E. Campbell, *Avoiding information overload through the understanding of OODA loops, a cognitive hierarchy and object-oriented analysis and design.* Annapolis, MD: C4ISR Cooperative Research Program (CCRP), 2001.

33. Grote, G., *Promoting safety by increasing uncertainty–Implications for risk management.* Safety science, 2015. 71: p. 71-79.

34. MCI, *ORM 1-0: Operational Risk Management*. 2002, United States Marine Corps: Headquarters Marine Corps, Washington DC.

35. OPNAV, *3500.39 B.(2004).* Operation risk management, 2004.

36. USAF, *Pamphlet 90-803 - Risk Management (RM) Guidelines and Tools*, U.S.A. Force, Editor. 2013.

37. Army, *ATP 5-19.* Risk Management, 2014.

38. Lin, J., et al., *Risk management in asymmetric conflict: using predictive route reconnaissance to assess and mitigate threats*, in *Social Computing, Behavioral-Cultural Modeling, and Prediction*. 2015, Springer. p. 350-355.

39. Wing, L.C. and Z. Jin, *Risk management methods applied to renewable and sustainable energy: a review. Journal of Electrical and Electronic Engineering*, 2015. 3(1): p. 1-12.

40. Elm, J.P., et al., *A Survey of Systems Engineering Effectiveness-Initial Results (with detailed survey response data)*. 2008, DTIC Document.

41. Arena, M.V., et al., *Impossible certainty: cost risk analysis for Air Force systems*. 2006, Santa Monica, CA: RAND. xxvi, 166 p.

42. Schwartz, M., *Nunn-McCurdy Act: Background, Analysis, and Issues for Congress*. 2010: DIANE Publishing Company.

43. *Congressional Record*. May 14, 1981. p. S5012.

44. *The Oxford Dictionary of Proverbs (5 ed.)*. 2008, Oxford University Press.

45. Blickstein, I., et al., *Root cause analyses of Nunn-McCurdy breaches. Vol. 2: Excalibur artillery projectile and the Navy Enterprise Resource Planning program, with an approach to analyzing program complexity and risk*. Rand Corporation monograph series. 2012, Santa Monica, CA: RAND. xxiii, 89 p.

46. *Space Based Infrared System (SBIRS)*. [cited 2015 7 July], Available from: http://www.lockheedmartin.com/us/products/sbirs.html.

47. *Budget Busters: The USA's SBIRS-High Missile Warning Satellites*. [cited 2015 26 July]; Available from: https://www.defenseindustrydaily.com/despite-problems-sbirs-high-moves-ahead-with-3rd-satellite-award-05467/.

48. Kim, Y., et al., *Acquisition of Space Systems.* Volume 7. *Past Problems and Future Challenges*. 2015, DTIC Document.

49. Gallagher, B.P., *Boulder Software Risk Evaluation Report for SBIRS*. 2000, Software Engineering Institute: Unpublished report.

50. Williams, R., Sandra Behrens, and George Pandelios, *SRE Method Description (Version 2.0) & SRE Team Members Notebook (Version 2.0) (CMU/SEI-99-TR-029)*. 1999, Retrieved July 26, 2015, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=13557.

51. Carr, M.J., et al., *Taxonomy-based risk identification*. 1993, DTIC Document.

52. Huang, C.Y., *Performance analysis of software reliability growth models with testing-effort and change-point. Journal of Systems and Software*, 2005. 76(2): p. 181-194.

53. Gallagher, B.P., et al., *A Taxonomy of Operational Risks.* 2005.

54. Gallagher, B.P., *Buckley mini Software Risk Evaluation Preliminary Report for SBIRS*. 2000, Software Engineering Institute: Unpublished report.

55. Susnienė, D. and P. Vanagas, *Means for satisfaction of stakeholders' needs and interests.* Engineering economics, 2015. 55(5).

56. Gallagher, B.P., *Interpreting Capability Maturity Model Integration (CMMI) for Operational Organizations.* 2002.

57. *Air Force Instruction 90-1 102, Performance Management.* 2000.

58. BrainyQuote.com. Xplore Inc. *Lewis Carroll.* 2015 [15 August, 2015]; Available from: http://www.brainyquote.com/quotes/quotes/l/lewiscarro165865.html.

59. Gallagher, B., et al., *CMMI for Acquisition: Guidelines for Improving the Acquisition of Products and Services*. 2011: Addison-Wesley Professional.

60. ISO, *31000: 2009 Risk management-Principles and guidelines*, in *International Organization for Standardization*, Geneva, Switzerland. 2009.

61. Dorofee, A.J., et al., *Continuous Risk Management Guidebook*. 1996, DTIC Document.

62. Doggett, A.M., *Root cause analysis: A framework for tool selection.* Quality Management Journal, 2005. 12(4): p. 34.

63. Wojcik, R., et al., *Attribute-Driven Design (ADD), Version 2.0*. 2006, DTIC Document.

64. Firesmith, D.G., et al., *The method framework for engineering system architectures*. 2008: CRC Press.

65. Sutcliffe, A., *Scenario-based requirements engineering* in *Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International.* 2003.

66. Mylopoulos, J., L. Chung, and E. Yu, *From object-oriented to goal-oriented requirements analysis.* Communications of the ACM, 1999. 42(1): p. 31-37.

67. Bass, L., Mark Klein, and Gabriel Moreno, *Applicability of General Scenarios to the Architecture Tradeoff Analysis Method (CMU/SEI-2001-TR-014)*. 2001, Retrieved August 22, 2015, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=5637.

68. Brown, W.H., R.C. Malveau, and T.J. Mowbray, *AntiPatterns: refactoring software, architectures, and projects in crisis.* 1998.

69. Kazman, R., Mark Klein, and Paul Clements, *ATAM: Method for Architecture Evaluation (CMU/SEI-2000-TR-004)*. 2000, Retrieved August 22, 2015, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=5177.

70. Kossiakoff, A., et al., *Systems engineering principles and practice*. Vol. 83. 2011: John Wiley & Sons.

71. Selby, R.W., *Software engineering: Barry W. Boehm's lifetime contributions to software development, management, and research*. Vol. 69. 2007: John Wiley & Sons.

72. Len, B., C. Paul, and K. Rick, *Software architecture in practice.* Boston, Massachusetts Addison, 2003.

73. Weidenhaupt, K., et al., *Scenarios in system development: current practice.* Software, IEEE, 1998. 15(2): p. 34-45.

74. Firesmith, D.G., *Common System and Software Testing Pitfalls: How to Prevent and Mitigate Them: Descriptions, Symptoms, Consequences, Causes, and Recommendations*. 2014: Addison-Wesley Professional.

75. Bernard, T., et al., *CMMI Acquisition Module (CMMI-AM) Version 1.1.* 2005.

76. Department of Defense, *Defense Acquisition Guidebook*, in *Chapter 4: Systems Engineering*. 2015.

77. Elm, J.P. and D.R. Goldenson. *Quantifying the effectiveness of systems engineering*. in *Systems Conference (SysCon), 2013 IEEE International*. 2013. IEEE.

78. Joshi, A., et al., *Likert scale: explored and explained. British Journal of Applied Science & Technology*, 2015. 7(4): p. 396.

79. Freeman, L.C., *Elementary applied statistics: for students in behavioral science*. 1965: John Wiley & Sons.

80. Nord, R.L., et al. *In search of a metric for managing architectural technical debt* in *Software Architecture (WICSA) and European Conference on Software Architecture (ECSA)*, 2012 Joint Working IEEE/IFIP Conference in 2012. IEEE.

81. McConnell, S. *Managing Technical Debt*. 2011 Available from: https://www.youtube.com/watch?v=lEKvzEyNtbk.

82. Stecklein, J.M., et al., *Error cost escalation through the project life cycle.* 2004.

83. Hayes, W., et al., *Handbook for conducting Standard CMMI Appraisal Method for Process Improvement (SCAMPI) B and C appraisals,* version 1.1. 2005.

84. Mattice, J.J., *Hubble Space Telescope systems engineering case study.* Air Force Institute of Technology, Wright-Patterson AFB, OH, 2005.

85. Smith, M., *Department of Defense and National Defense Industrial Association Top 5 DoD Program Awards 2005 Nomination Form: Mission Integration and Development (MIND)*. 2006, National Defense Industrial Association.

86. Raytheon. *Raytheon Program Selected As One Of The Dod's Top 5 Programs*. 2006. Available from: http://investor.raytheon.com/phoenix.zhtml?c=84193&p=irol-newsArticle&ID=937745.

87. Carton, F., F. Adam, and D. Sammon, *Project management: a case study of a successful ERP implementation. International Journal of Managing Projects in Business*, 2008. 1(1): p. 106-124.

88. Montealegre, R. and M. Keil, *De-escalating information technology projects: Lessons from the Denver International Airport. Mis Quarterly*, 2000: p. 417-447.

89. Congress, *The Air Force's Expeditionary Combat Support System (ECSS): A Cautionary Tale on the Need for Business rocess Reengineering And Complying with cquisition Best Practices*. 2014.

90. Kelly, T.K., et al., *Results from the Congressionally Mandated Study of US Combat and Tactical Wheeled Vehicle.* 2011.

91. Hooper, C. *A Poster Child for Next-War-Itis*. 2008. Available from: http://www.usni.org/magazines/proceedings/2008-11/poster-child-next-war-itis.

92. Feickert, A. *The Marines' Expeditionary Fighting Vehicle: Background and Issues for Congress*. 2010. DTIC Document.

93. Mak, M.A., et al., *Amphibious Combat Vehicle Acquisition: Marine Corps Adopts an Incremental Approach*. 2015, DTIC Document.

94. Neuman, W., *Police Won't Use $140 Million Radio System*, in *New York Times*. 2007.

95. Shore, B., *New York Subway Communications System.* 2009.

96. Council, N.R., *Controlling Cost Growth of NASA Earth and Space Science Missions*. Washington, DC: The National Academies Press. 2010.

97. NASA, *NASA System Safety Handbook: System Safety Framework and Concepts for Implementation, Version 1*. NASA/SP-2010-580. 2011.

APPENDIX A – ORDERED TAXONOMY

A. MISSION

The mission category consists of potential sources of risk to the operational mission. The sources of risk in this category focus on the mission timeline from mission tasking and planning through evaluation of mission outcomes. In addition, the operational systems, processes, and people used to perform the mission are potential sources of risk to mission performance and are included in this category.

1. Mission Planning

The mission planning element includes sources of risk associated with planning the mission. It includes how the mission is tasked, planned, and re-planned during execution of the mission.

a. Stability

The stability attribute includes sources of risk associated with mission tasking and planning. Areas of risk include the frequency and magnitude of changes to mission tasking and the impact on operational planning and re-planning activities as well as stability of operational plans themselves.

Exploratory Questions

- *How often does mission tasking change?*

- *Do operational plans need adjustment during execution?*

b. Completeness

The completeness attribute includes sources of risk associated with the thoroughness and maturity of mission tasking and operational plans. Areas of risk include tasking with missing details required to plan the mission and operational plans lacking detail required to perform the mission.

Exploratory Questions

- *Is mission tasking detailed enough to plan the mission?*
- *Are operational plans detailed enough to allow operators to perform their assigned tasks?*

c. Clarity

The clarity attribute includes sources of risk associated with the certainty of the mission tasking as well as the operational plans. Areas of risk include level of confusion or misinterpretation that may arise from mission tasking or operational plans that lack clear and unambiguous definition.

Exploratory Questions

- *Is mission tasking ambiguous?*
- *Are operational plans of sufficient detail to avoid*

confusion or ambiguity in execution?

d. Feasibility

The feasibility attribute includes sources of risk associated with how likely mission outcomes are to be achieved given current people, processes, and systems. Areas of risk include probability of mission success and ability of current operational resources to perform the mission task or execute the operational plans.

Exploratory Questions

- *Can the operational organization achieve the mission tasking?*
- *Are operational plans sufficient to achieve mission outcomes given available resources?*

e. Precedents

The precedents attribute includes sources of risk associated with whether the mission tasking or the approach defined in the operational plans have been successfully performed in the past. Areas of risk include mission tasking specifying outcomes never achieved previously or implementation choices within operational plans that are unproven.

Exploratory Questions

- *Have the mission outcomes defined in the tasking ever* *been achieved before? If so, has this organization achieved these outcomes previously?*

- *Do operational plans define methodologies, approaches, or tactics new to the organization?*

f. Agility

The agility attribute includes sources of risk associated with how quickly the tasking and plans may be adjusted to meet evolving operational needs. Areas of risk include rigid change control processes for mission tasking and plans or the inability to adjust quickly when mission threats evolve.

Exploratory Questions

- *How often does the mission change from the original tasking?*
- *How quickly can the operational organization adjust to mission changes?*
- *How much authority do operational leaders have in deviating from tasking or plans?*

2. Mission Execution

The mission execution element includes sources of risk associated with performing the mission. It includes the effectiveness and efficiency of execution, the ability to repeatedly perform the mission, to adjust as needed, and to execute while meeting cost constraints in a safe and secure manner.

a. Efficiency

The efficiency attribute includes sources of risk associated with the ability of the operational organization to execute mission requirements with the least amount of resources needed. Areas of risk include resource waste during execution, performing unnecessary tasks that don’t contribute to mission success, or under-utilization of resources.

Exploratory Questions

- *Are there mission execution steps performed that don’t contribute to mission outcomes?*
- *Are execution steps as streamlined as they could be while still meeting mission outcomes?*
- *Are all mission resources (people, processes, systems) used without waste?*

b. Effectiveness

The effectiveness attribute includes sources of risk associated with the efficacy of the operational mission to achieve desired outcomes. Areas of risk include ability to achieve mission outcomes during performance of the mission and the effectiveness of people, processes, and systems working together to meet mission objectives.

Exploratory Questions

- *Do operational personnel, process, and systems meet mission objectives during execution?*
- *Does the operation achieve desired outcomes?*

c. Repeatability

The repeatability attribute includes sources of risk associated the operational organization's ability to execute the mission multiple times in a similar, if not the same, fashion. Areas of risk include ability to predict resources, effort, and outcomes based on past performance.

Exploratory Questions

- *Are the mission steps performed similarly each time?*
- *How much variation is observed in mission execution? Does that cause concern?*
- *Can operational leaders and personnel rely on past mission execution to predict resources and effort required to achieve mission outcomes?*

d. Agility

The agility attribute includes sources of risk associated the ability of the mission during execution to adjust quickly to respond to changes in operational risk or mission needs/threats. Areas of risk include ability to adjust quickly and allow flexibility in mission execution while still performing the mission with discipline to meet mission outcomes.

Exploratory Questions

- *During execution, are new threats and mission risks quickly identified?*
- *Can operational personnel, processes, and systems quickly adjust during execution to meet mission challenges, threats, or risks?*
- *As mission execution adjusts to meet unexpected execution needs, does mission discipline deteriorate?*

e. Affordability

The affordability attribute includes sources of risk associated with the cost effective performance of the mission. Areas of risk include ability to meet all mission objectives while meeting cost constraints, including keeping cost growth at a minimum and the ability to recognize cost savings over time.

Exploratory Questions

- *Are mission objectives met within all cost constraints?*
- *Do mission execution costs decline over time?*

- *Are there aspects of the mission driving cost increases over time?*
- *Is the operational organization able to continue to execute within budget?*
- *Are labor, raw material, or supplier costs rising unacceptably?*

f. Security

The security attribute includes sources of risk associated with the ability to execute the mission while maintaining all security requirements. Areas of risk include ability to maintain operational, information, system, and personnel security.

Exploratory Questions

- *Are there operational security concerns associated with mission execution?*
- *Does the operational organization maintain information and data security during mission execution?*
- *Does mission execution endanger personnel security?*

g. Safety

The safety attribute includes sources of risk associated with the ability of the operational organization to guarantee safe operations during mission execution. Areas of risk include ability to maintain operational, information, system, and personnel security.

Exploratory Questions

- *Are safety hazards identified and mitigated during mission execution?*
- *Does the operational organization continually assess the adequacy of controls in place to ensure that acceptable levels of safety risk are not exceeded?*
- *Do safety incidents impact mission execution or degrade mission outcomes?*
- *Are contingency plans in place to address potential safety incidents?*

3. Mission Outcomes

The mission outcomes element includes sources of risk associated with the product or services that result from the execution of the mission. It includes being able to provide mission outcomes that predictably meet expectations in terms of the accuracy, timeliness, efficiency, and usability of the product or service provided as a result of executing the mission.

a. Predictability

The predictability attribute includes sources of risk associated with the ability to provide results that predictably meet all expectations. Areas of risk include how well mission outcomes observed align with planned outcomes and the uniformity of results from multiple execution of the same or similar mission tasks.

Exploratory Questions

- *Do mission results routinely match planned results?*
- *Is there variation in the product or service provided as a result of executing mission tasks?*
- *Can mission planners rely on mission task outcomes to produce the results expected?*

b. Accuracy

The accuracy attribute includes sources of risk associated the accuracy of mission outcomes. Areas of risk include the correctness, exactness, and authenticity of the outcomes, products, or services provided through mission execution.

Exploratory Questions

- *Is it important that the mission produces accurate results?*
- *Can mission results be verified as accurate?*
- *How is the authenticity of mission outcomes, products, or services ensured through mission execution?*

c. Usability

The usability attribute includes sources of risk associated with the operational usability of mission outcomes. Areas of risk include a mismatch between operational need and results provided, the appropriateness of the results, and ease of use of mission outcomes.

Exploratory Questions

- *Do the outcomes, products, and services resulting from executing the mission meet the operational need?*
- *Are operators able to quickly and easily understand the outcomes, products, and services resulting from mission execution?*
- *Are the mission execution outcomes appropriate to fulfill mission and business needs?*

d. Timely

The timely attribute includes sources of risk associated with the suitability of the timeliness of mission outcomes. Areas of risk include mission outcomes, products, or services that are late-to-need or are produced too soon so that they become less effective once needed.

Exploratory Questions

- *How important is it that mission outcomes are* *produced in a timely fashion?*

- *Are mission outcomes routinely late-to-need?*
- *Are mission outcomes, products, or services produced too soon, and therefore, are less relevant or effective due to staleness of the outcome?*

e. Efficient

The efficient attribute includes sources of risk *associated with the ability* of the mission to produce efficient outcomes. Areas of risk include waste in execution, lack of ability to execute economically, and tasks that exhibit excessive administrative overhead.

Exploratory Questions

- *Are mission-critical and support tasks executed as streamlined as needed?*
- *Is there waste in execution that drives mission cost higher than necessary?*
- *Is the mission executed with minimal administrative overhead?*

4. Operational Systems

The operational systems element includes sources of risk associated with the systems used by operational personnel to execute the mission. It includes the ability of the systems to enable the performance of mission-critical and mission-support tasks effectively and efficiently. Systems are able to respond appropriately when necessary and to evolve when shifts in mission need occur.

a. Throughput

The throughput attribute includes sources of risk associated the ability of operational systems to process the amount of material or data required to perform the mission and to respond when shifts in mission need occur. Areas of risk include the inability of operational systems to process raw materials or information at a rate that supports current or future operational needs.

Exploratory Questions

- *How critical is it that operational systems keep up with mission demands for the processing of raw materials or information?*
- *Do current systems meet operational throughput needs?*
- *Are there planned or expected changes in mission execution requiring higher levels of throughput that may be met with current operational systems?*
- *Are the systems used by mission partners able to keep up with processing demands?*

b. Usability

The usability attribute includes sources of risk associated with the ease of use of operational systems. Areas of risk include operational systems that are not intuitive to use, that confuse operators, or that induce a high rate of operator errors.

Exploratory Questions

- *How quickly can new operators master operational systems?*
- *Are operational systems easy to use?*
- *Is how to get desired results from operational systems intuitive for operators?*
- *Is there a high rate of operational incidents traced to operator error?*
- *When operations scale in volume or intensity, do operational systems decrease or increase uncertainty and confusion?*

c. Flexibility

The flexibility attribute includes sources of risk associated with the ability of operational systems to meet changes in mission demands. Areas of risk include operational systems that have rigid operational concepts embedded in their design, systems that fail to recognize deviation in mission needs, and systems that require extensive or awkward operational workarounds to perform the mission.

Exploratory Questions

- *Are operational systems designed to easily meet changes in mission expectations?*
- *When mission needs deviate from expectations, do systems support these changes during execution?*
- *Do operators employ extensive or awkward workarounds for system inadequacies in order to meet mission objectives?*

d. Reliability

The reliability attribute includes sources of risk associated with the ability of operational systems to perform their required functions under known and planned conditions for a specified period of time. Areas of risk include operational systems that fail to produce results consistently as expected under normal and planned stress conditions and systems or system components that break or fail earlier or more frequently than expected or modeled.

Exploratory Questions

- *Are there high-reliability requirements for operational systems?*
- *Are there detailed reliability models predicting*

failure modes or that analyze reliability growth or deterioration over time?

- *Do the operational systems perform as expected under normal and planned stress conditions?*
- *Do operational systems or their components fail too often or earlier than expected?*

e. Evolvability

The evolvability attribute includes sources of risk associated with the ability of operational systems to evolve with relative ease to meet changes in mission threats or needs. Areas of risk include operational systems that require extensive or expensive re-design to support evolving mission changes or that require original manufacturer involvement in system evolution.

Exploratory Questions

- *How often do mission threats and risks change and cause the need for mission execution changes?*
- *Are operational systems architected and designed to allow quick evolution without extensive or expensive re-design activities?*
- *Do operational systems require the original manufacturer to effect change?*
- *Does the system design require a large contingent of*

engineers to deploy the systems in order to configure them for operations or changes in operational tactics?

f. Security

The security attribute includes sources of risk associated with the ability of operational systems to enable secure operations. Areas of risk include operational systems that fail to ensure data, system, network, inter-system, or personnel security.

Exploratory Questions

- *How critical or sensitive is the data processed by operational systems or the system itself to operational outcomes?*
- *Are adequate controls in place to ensure that data is free from intentional or unintentional unauthorized manipulation or degradation?*
- *Are adequate controls in place to ensure that only authorized users have access to operational systems?*
- *Are operational networks monitored for unauthorized access or activity?*
- *Are there adequate controls in place to ensure that inter-system interactions are authorized and appropriate?*
- *Do operational systems have controls to detect and*

thwart unauthorized insider threats?

- *Do operational systems protect sensitive personal information of users and operators?*

g. Supportability

The supportability attribute includes sources of risk associated with the ability to support operational systems during use. Areas of risk include operational systems without adequate raw materials available to operate, limited access to routine or preventive maintenance, and lacking post-deployment support strategies.

Exploratory Questions

- *Do operational systems deploy with all required raw materials and spare parts to support normal and expected operations?*
- *Are operational systems subject to routine or preventive maintenance actions?*
- *Is there a well-defined and tested strategy in place to obtain support from the original manufacturer or other source when systems require more than routine maintenance?*

h. Inventory

The inventory attribute includes sources of risk associated with managing and using raw materials to produce operational outcomes, products, or services during mission execution or to store intermediate or final mission outcomes before use. Areas of risk include having to store unplanned amounts of raw or processed materials or not having materials when needed.

Exploratory Questions

- *Is there a well-defined strategy for the management of inventory that includes raw materials, intermediate products, and final mission outcomes prior to use?*
- *Are adequate raw materials or system inputs available when needed?*
- *Is there a plan for re-use or re-purposing of excess raw materials or inventory?*

5. Operational Processes

The operational processes element includes sources of risk associated with the processes used by operational personnel to perform the mission. It includes the suitability of operational processes to perform required mission-critical and support tasks and the ability of those processes to provide repeatable, predictable outcomes while being agile enough to support mission changes without impacting secure mission outcomes.

a. Suitability

The suitability attribute includes sources of risk associated with the appropriateness of operational processes and their level of formality to support mission-critical and support tasks. Areas of risk include having operational processes that impede rather than enable the mission and not having processes that appropriately balance discipline and agility as required by unique mission needs.

Exploratory Questions

- *Are operational activities guided by documented processes?*
- *Do operational processes enable successful mission outcomes?*
- *Are operational processes optimized to the right mix of formality and agility as dictated by mission needs?*
- *Are operators empowered to adjust operational processes to ensure that mission objectives are achieved?*

b. Repeatability

The repeatability attribute includes sources of risk associated with the ability to ensure that process execution is repeatable and results in expected outcomes. Areas of risk include lack of process documentation, ownership, training, and evaluation of effectiveness and compliance.

Exploratory Questions

- *Is operational process documentation adequate to ensure repeatable execution?*
- *Is responsibility assigned for process execution and evolution?*
- *Is adequate and current training provided to operational personnel?*
- *Are operational processes objectively evaluated to ensure that they meet the needs of the mission and that they are executed as documented?*

c. Predictability

The predictability attribute includes sources of risk associated with the ability to predict mission outcomes based on a quantitative understating of process performance. Areas of risk include lack of understanding of process behavior typically characterized by a central tendency and dispersion as well as the inability to model and predict outcomes by analyzing process behavior.

Exploratory Questions

- *Is operational process or critical sub-process* *behavior quantitatively understood?*

- *Is the behavior of critical processes or sub-processes understood in terms of central tendency (mean) and dispersion (standard deviation)?*
- *Does the operational organization use process performance models to understand process interaction, expected outcomes, and to test assumptions and what-if scenarios prior to execution?*
- *Are quantitative mission objectives established based on historic process performance?*

d. Agility

The agility attribute includes sources of risk associated with the ability to quickly plan, execute, re-plan, and adjust as needed during operations. Areas of risk include processes that are so rigid and onerous that they fail to meet operational needs and processes that are inflexible during execution so as to not support adjustments as needed.

Exploratory Questions

- *How quickly can the operational organization plan a new mission with confidence in outcomes?*
- *Are multiple and redundant approvals required to finalize operational plans?*

- *Are operational processes flexible enough to allow re-planning during execution when operational risks or threats change?*
- *Does every operator understand how they personally, and how their teams, contribute to the mission and their pre-approved level of authority to deviate from plan to achieve mission outcomes?*

e. Security

The security attribute includes sources of risk associated with maintaining the integrity, availability, and confidentiality of operational processes, plans, and expected outcomes. Areas of risk include the inability of the operational organization to identify critical process assets that need protection, lack of analysis of process vulnerabilities, failure to identify operational security risks, and the lack of focus on applying mitigation approaches to address security threats.

Exploratory Questions

- *How vulnerable are operational processes to security breaches?*
- *Does the operational organization understand which process assets have security vulnerability implications and require protection?*

- *Are operational security risks and process vulnerabilities continually assessed and analyzed?*
- *Are the most critical process risks mitigated?*

6. Operational Staff

The operational staff element includes sources of risk associated with the people who perform operational activities. It includes ensuring that operational staff maintain proper skill levels, are effectively trained, are replaced in a timely fashion to address attrition, and that the cost of staff remains affordable to perform the required mission.

a. Skill Level

The skill level attribute includes sources of risk associated with a mismatch between the skill levels required for mission execution using existing or planned systems and the current skill level of assigned staff. Areas of risk include the inability of the operational organization to staff positions adequately with skilled staff when needed and mismatches that arise when shifts in mission needs evolve or new systems deployed requiring different skills.

Exploratory Questions

- *Does operational staff have the required skills and* *experience to perform current mission operations?*

- *Does operational staff have the required skills to support planned mission changes or to operate new or planned systems?*
- *Are individuals with required skills available in the current market?*

b. Training

The training attribute includes sources of risk associated with the operational organization’s ability to provide adequate training and experiences to allow staff to perform the current and planned mission with the systems employed and envisioned in the future. Areas of risk include the inability of the operational organization to train staff quickly and realistically and to get them fully qualified to perform operations today and to support planned mission and system evolution.

Exploratory Questions

- *Is current operational staff adequately trained to support mission needs?*
- *Is staff adequately prepared for planned mission and operational system changes?*
- *Is current training realistic and comprehensive enough to allow qualification of operational staff*

prior to mission execution?

c. Turnover

The turnover attribute includes sources of risk associated with the level of operational staff turnover. Areas of risk include the inability of the operational organization to fill positions quickly with adequately skilled and trained staff prior to the need date and the ease with which new staff are integrated into operational systems and processes without mission impact.

Exploratory Questions

- *Is there a high turnover rate within operational staff?*
- *How easily can the operational organization find skilled staff, provide training, and qualify them to perform operational tasks?*
- *Are operational systems and processes intuitive to new operational staff?*
- *How long does it take to fully qualify new operational staff members?*

d. Affordability

The affordability attribute includes sources of risk associated with the cost of the operational staff required to perform mission-critical and support tasks. Areas of risk include operational staff cost growth associated with changes in mission growth, operational system or process complexity, or the inability to find qualified operational staff at reasonable salaries.

Exploratory Questions

- *Are operational staffing needs increasing or becoming more difficult to fill?*
- *Are the costs of hiring skilled operational staff increasing at an unreasonable rate?*
- *Does mission growth or tempo require a large increase in operational staff?*
- *Does the complexity of operational systems or processes drive more-skilled or higher-cost staff?*

B. BUSINESS

The business category consists of potential sources of risk to the longer-term viability of the organization's proficiency in conducting business and executing its assigned mission. The sources of risk in this category focus on activities such as resource planning, governance, strategic planning, stakeholder management, culture, and continuous improvement.

1. Resource Planning

The resource planning element includes sources of risk associated with the resources that the operational organization uses to plan and perform mission activities. It includes the available workforce, funding, facilities, and the tools and systems available to carry out mission tasking.

a. Workforce

The workforce attribute includes sources of risk associated with the strategic management of the workforce required to perform mission activities. Areas of risk include availability of a qualified workforce to perform future mission activities, affordability of the workforce, and the organization's ability to attract and retain a highly skilled workforce.

Exploratory Questions

- *Does the operational organization plan for the management of the workforce long-term?*
- *Can the operational organization attract qualified staff to meet workforce needs?*
- *Can the operational organization retain the staff required to fulfill mission needs?*

b. Budget

The budget attribute includes sources of risk associated with funding constraints to perform mission activities. Areas of risk include lack of long-term viability of the organization to perform mission activities, funding shortfalls requiring degraded operations, growth in mission costs over time, and the inability to acquire new systems to support mission needs or maintain existing systems.

Exploratory Questions

- *Are there budget constraints that impact mission performance?*
- *Will future mission tasks suffer from budget shortfalls?*
- *Are costs growing to an extent that mission performance is negatively impacted?*
- *Can the operational organization afford to acquire and field enhanced capabilities to keep up with mission threats and needs?*
- *Are current systems maintained to ensure mission readiness?*

c. Facilities

The facilities attribute includes sources of risk associated with the permanent or temporary facilities used to conduct mission operations. Areas of risk include facilities that are inadequate, deteriorating, or unable to scale to meet future mission demands.

Exploratory Questions

- *Are current facilities adequate to perform mission operations?*
- *Do facilities support planned growth or mission expansion?*
- *Has facility maintenance kept up with operational needs?*

d. Equipment and Systems

The equipment and systems attribute includes sources of risk associated with having the appropriate tools and systems to perform mission operations. Areas of risk include equipment or systems that fail to support operational needs, fail to scale, are obsolete, or are unable to support shifts in mission needs.

Exploratory Questions

- *Do operational equipment and systems meet current operational needs?*
- *Can operational equipment and systems scale to meet future mission demands?*
- *Are the designs or components that make up equipment and systems obsolete and difficult to maintain?*
- *Are operational equipment and systems flexible enough to support shifts in operational risk or mission needs?*

2. Governance

The governance element includes sources of risk associated with the mechanisms in place to govern mission and business activities. It includes the policy and process architecture to effectively guide activities, organizational structures, contracts with suppliers, and the ability to analyze data, how the operational organization ensures compliance, and how it identifies and mitigates operational risk.

a. Policies

The policies attribute includes sources of risk associated with the operational organization's policies that govern mission activities. Areas of risk include lack of written policies, policies that are inflexible, policies that haven't evolved with changes in mission need, or policies that incentivize unwanted behavior.

Exploratory Questions

- *Does the operational organization have a set of written policies?*
- *Are operational personnel aware of the content of organizational policies?*
- *Do policies drive unwanted behavior?*
- *Do operational personnel need to employ workarounds*

to avoid inflexible policies?

- *Is there a clear process in place to change policies?*
- *When mission and business threats evolve, are policies changed appropriately?*
- *Are mission activities evaluated for compliance with policies?*

b. Procedures

The procedures attribute includes sources of risk associated with the operational organization’s procedures used to perform mission-critical and mission-support tasks. Areas of risk include lack of written procedures, procedures that are either too detailed or too abstract, procedures that are incomplete or inflexible, or the lack of guidance regarding when and how to deviate from procedures to support mission needs.

Exploratory Questions

- *Does the operational organization have a set of written procedures?*
- *Are operational procedures defined for both mission-critical and mission-support tasks?*
- *Are procedures too detailed and inflexible?*
- *Are procedures too abstract and allow too much variation in mission execution?*

- *When mission needs necessitate deviation from procedures, is clear guidance available to direct staff about when and how to deviate?*

c. Organizational Structure

The organizational structure attribute includes sources of risk associated with the structure that the operational organization has in place to execute mission tasks. Areas of risk include organizational structures that inhibit collaboration, increase command and control confusion, contain too many layers, or do not support how the mission is executed.

Exploratory Questions

- *Does the operational organizational structure inhibit cross-unit collaboration?*
- *Are there excessive layers of management between those executing the mission and decision-makers?*
- *Does the organizational structure cause mission execution confusion?*
- *Are command and control structures clear?*
- *Does the static organizational structure mimic and enable the mission execution structure?*

d. Contracts

The contracts attribute includes sources of risk associated with contracts that the operational organization enters into with external suppliers for products and services. Areas of risk include technical performance of acquired products and services, supplier cost and schedule performance, supply chain assurance, obsolescence of acquired products and services, availability of products and services from alternative sources, and flexibility of contracts and suppliers when mission needs change.

Exploratory Questions

- *Do acquired products and services meet mission needs?*
- *Do suppliers meet cost and schedule objectives?*
- *Is the supply chain free of vulnerabilities that may impact the mission?*
- *Does the operational organization have the ability to detect and remediate defective or counterfeit parts?*
- *Are acquired products and services obsolete when needed for mission tasks?*
- *Does the operational organization have access to alternative sources for mission-critical products and services?*
- *Are contracts and suppliers flexible when mission needs change?*

e. Analytics

The analytics attribute includes sources of risk associated with the ability of the operational organization to use data effectively to manage the work and make decisions. Areas of risk include having too much or too little data, not having an analytics capability, or having indicators that are late-to-need, are misleading, are unused, or drive unwanted behavior.

Exploratory Questions

- *Does the operational organization use historical and fact-based data when making critical decisions?*
- *Does the operational organization collect the appropriate amount of data to support tactical and strategic decision-making?*
- *Does the operational organization have a robust data analytics capability?*
- *Are metrics and indicators provided when needed to support timely decision-making?*
- *Are metrics and indicators clearly understood throughout the operational organization?*
- *Are indicators aligned with operational mission and business goals?*

f. Compliance

The compliance attribute includes sources of risk associated with the ability of the operational organization to ensure that mission operations comply with all organizational policies as well as appropriate laws and regulations. Areas of risk include lack of objective oversight mechanisms in place to ensure compliance, lack of accountability, and inadequate reporting and record-keeping.

Exploratory Questions

- *Does the operational organization objectively evaluate compliance with policies and applicable laws and regulations?*
- *Are non-compliance incidents reported and tracked to closure?*
- *Are operational staff held accountable for compliance with policies, laws, and regulations?*
- *Does the organization keep records of compliance checks and incidents of non-compliance?*

g. Risk Management

The risk management attribute includes sources of risk associated with the existence and effectiveness of a comprehensive operational risk management capability within the operational organization. Areas of risk include not having a defined operational risk strategy, lack of robust operational risk identification approaches, the inability to analyze and prioritize operational risks, and the failure to mitigate operational risk.

Exploratory Questions

- *Does the operational organization have a documented and communicated operational risk management strategy?*
- *Does the operational organization have comprehensive risk identification approaches to help continuously identify mission and business risks?*
- *Are mission and business risks analyzed and prioritized?*
- *Does the operational organization mitigate the most critical risks to mission and business effectiveness?*

3. Strategic Planning

The strategic planning element includes sources of risk associated with the strategic planning capabilities and effectiveness of the operational organization. It includes establishing and articulating the operational organization’s vision and mission, values, goals, and objectives and monitoring their accomplishment.

a. Vision and Mission

The vision and mission attribute includes sources of risk associated with the process of setting and communicating the vision and mission objectives of the operational organization. Areas of risk include not having well-defined vision and mission statements that reflect the reason for existence of the operational organization, not communicating the organization's vision and mission, or mismatch between the stated vision and mission and actual operations.

Exploratory Questions

- *Does the operational organization have explicit vision and mission statements that reflect the purpose of the operational unit?*
- *Has the operational organization communicated its vision and mission to all relevant stakeholders?*
- *Do actual operations align with the operational organization's stated vision and mission?*

b. Values

The values attribute includes sources of risk associated with guiding principles established to help operational staff understand acceptable behavior and action during mission execution. Areas of risk include not having an established set of core values to guide action and behavior, values that are in conflict with actions of operational leadership, or values that don’t have an active influence on operations.

Exploratory Questions

- *Has the operational organization established a set of core values designed to influence acceptable actions and behavior of operational staff?*
- *Does staff in leadership positions exhibit behavior in conflict with stated values?*
- *Do the stated values influence the actions and behavior of operational staff during mission execution?*

c. Goals

The goals attribute includes sources of risk associated with documented and communicated goals, tied to the organization’s values and mission, that explain what the operational organization intends to achieve. Areas of risk include not having documented goals, goals that aren’t aligned with the vision or mission statements of the organization, or goals that aren’t specific, measureable, achievable, and timely.

Exploratory Questions

- *Are the operational organization’s goals documented and communicated to relevant stakeholders?*
- *Do stated goals align with the vision and mission*

statements of the operational organization?

- *Are the operational organization’s goals specific, measureable, achievable, and timely?*

d. Objectives

The objectives attribute includes sources of risk associated with the specific steps that the operational organization intends to take to achieve goals. Areas of risk include objectives that aren’t tied to stated goals, objectives that lack clarity, lack of assigned responsibility for accomplishment of objectives, or objectives without specific timelines and milestones.

Exploratory Questions

- *Are strategic objectives of the operational organization tied specifically to organizational goals?*
- *Are strategic objectives clear and concise, with specific steps detailed to avoid execution confusion?*
- *Do stated objectives include timelines, responsibilities, and milestones?*

e. Monitoring

The monitoring attribute includes sources of risk associated with monitoring the implementation of the operational organization’s strategic plan. Areas of risk include failure to understand when the organization deviates from strategic plan achievement; failure to adjust strategic plans, goals, or objectives when mission or business needs shift; or failure to communicate progress toward strategic plan achievement.

Exploratory Questions

- *Does the operational organization monitor achievement of strategic plans?*
- *Are goals and objectives monitored and measured?*
- *When mission or business needs change, does the operational organization re-evaluate strategic plans, goals, and objectives for relevance?*
- *Is progress toward strategic plan achievement communicated to relevant stakeholders?*

4. Stakeholder Management

The stakeholder management element includes sources of risk associated with how the operational organization manages relevant stakeholders. It includes identifying relevant stakeholders, planning for their involvement, engaging stakeholders appropriately, and controlling stakeholder involvement during the execution of mission and business activities.

a. Identification

The identification attribute includes sources of risk associated with identifying relevant stakeholders who are affected by mission and business outcomes. Areas of risk include failure to understand the impact of mission and business outcomes on stakeholders, failure to explicitly list stakeholders and how they should be involved in mission activities, or failure to re-evaluate relevant stakeholders as mission and business changes occur.

Exploratory Questions

- *Has the operational organization evaluated the impact of mission and business outcomes on stakeholders?*
- *Has the operational organization explicitly identified both internal and external stakeholders who are effected by mission and business outcomes?*
- *As mission and business needs change, does the operational organization re-evaluate which stakeholders to involve during mission and business activities?*

b. Stakeholder Management Plan

The stakeholder management plan attribute includes sources of risk associated with the operational organization's plan for involving relevant stakeholders during mission and business activities. Areas of risk include failure to plan for the involvement of relevant stakeholders in mission and business planning and execution activities, failure to document the stakeholder management plan, or failure to maintain the plan as mission and business needs change.

Exploratory Questions

- *Has the operational organization planned for the involvement of relevant stakeholders during mission and business planning and execution activities?*
- *Is the stakeholder management plan documented?*
- *Does the operational organization update the stakeholder management plan when mission and business needs change?*

c. Engagement

The engagement attribute includes sources of risk associated with ensuring that relevant stakeholders are engaged as appropriate during mission and business activities. Areas of risk include failure to monitor stakeholder involvement, stakeholders who are unable or unwilling to participate as required, or stakeholders who engage inappropriately.

Exploratory Questions

- *Does the operational organization monitor stakeholder involvement in relation to the stakeholder management plan?*
- *Do all relevant stakeholders participate as planned?*
- *Do stakeholders engage inappropriately (try to unduly influence outcomes, disrupt mission planning or execution)?*

d. Controlling

The controlling attribute includes sources of risk associated with controlling stakeholder involvement. Areas of risk include failure to control stakeholder access to plans and mission outcomes or to take corrective action when stakeholders aren’t involved appropriately.

Exploratory Questions

- *Does the operational organization control stakeholder access to plans and mission outcomes?*
- *When stakeholders aren’t engaging as required, does the operational organization take corrective action?*

5. Continuous Improvement

The continuous improvement element includes sources of risk associated with the continuous identification and implementation of operational improvements. It includes identification of problems impacting mission and business outcomes, identifying opportunities for improvement, determining the root cause of problems, and planning improvement activities and implementing improvements.

a. Problem Identification

The problem identification attribute includes sources of risk associated with the ability of the operational organization to identify problems, issues, weaknesses, or constraints that negatively impact mission or business outcomes. Areas of risk include inability to determine negative outcomes, failure to document problems, and failure to encourage discovery of problems.

Exploratory Questions

- *Can the operational organization detect when problems, issues, weaknesses, or constraints negatively impact mission or business outcomes?*
- *Are problems documented to allow for further analysis?*
- *Does operational leadership encourage staff to identify and communicate problems?*

b. Opportunity Identification

The opportunity identification attribute includes sources of risk associated with the ability of the operational organization to identify potential opportunities that could positively impact mission or business outcomes. Areas of risk include lack of analysis of current operations, failure to identify external best practices for possible adoption, and discouraging operational staff from suggesting improvements.

Exploratory Questions

- *Does the operational organization analyze past and current operations to identify potential improvement opportunities?*
- *Does the operational organization look for best practices and improvement opportunities externally?*
- *Does the operational organization encourage staff to identify opportunities for improvement?*

c. Root Cause Analysis

The root cause analysis attribute includes sources of risk associated with the ability of the operational organization to identify root causes of problems. Areas of risk include lack of analysis to determine root cause, fixing problems before determining the true cause, and inability to prevent recurrence of problems with certainty.

Exploratory Questions

- *Does the operational organization analyze negative* *outcomes to determine their root cause?*

- *Does the operational organization attempt to solve problems without understanding the underlying cause of the problem?*
- *When proposing solutions to problems, can the operational organization provide certainty that the solutions will prevent recurrence of the problems?*

d. Improvement Planning

The improvement planning attribute includes sources of risk associated with the ability of the operational organization to plan operational improvements. Areas of risk include failure to create a program plan for the improvement, failure to assign responsibility to plan the improvement activities, and failure to communicate the plan for improvement.

Exploratory Questions

- *When planning improvement activities, does the operational organization create a documented plan of action and milestones?*
- *Does the operational organization assign responsibility for plan improvements?*
- *Are operational improvement plans communicated to all relevant stakeholders?*

e. Implementation

The implementation attribute includes sources of risk associated with the ability of the operational organization to successfully implement operational improvements. Areas of risk include failure to fully resource the improvement plan, failure to address organizational change considerations such as resistance and training, and failure to evaluate the effectiveness of the improvement.

Exploratory Questions

- *Does the operational organization provide adequate resources to implement improvement plans?*
- *When implementing operational improvements, does the organization address resistance to change, training, and other organizational change considerations?*
- *After an operational improvement is implemented, does the organization evaluate the effectiveness of the change?*

APPENDIX B – OPERATIONAL RISK SURVEY

A.1 SURVEY INSTRUMENT

Those who trust to chance must abide by the results of chance. ~ Calvin Coolidge

Service and Solution Delivery Risk

The purpose of Risk Management is to identify potential problems before they occur, so that risk-handling activities may be planned and invoked as needed to mitigate adverse impacts on achieving objectives. Identifying and mitigating risks is critical to ensuring delivery effectiveness.

The purpose of this survey is to evaluate the effectiveness of Risk Management practices and to explore the relationship between a customer’s operational or mission risk and the ability to deliver solutions and services that mitigate these risks.

Questionnaire (How strongly do you support the following statements?)

1. My program team has a documented risk management process.

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

2. My program team has an active risk register that reflects the team’s most critical current risks.

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

3. My program team has a robust, continuous risk identification process.

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

4. My program team actively mitigates the program’s top risks.

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

5. The leadership above my program actively elicits risks and helps mitigate risks to my program.

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

6. My program team actively elicited operational risks and mission threats from customers ***during the capture phase***.

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

7. My program team actively elicited quality attributes (responsiveness, adaptability, evolvability, agility, scalability, etc.) ***during the capture phase***.

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

8. The customer actively participates with the program team ***during execution*** to identify and mitigate operational risk.

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

9. The customer actively participates with the program team ***during execution*** to prioritize quality attributes

(responsiveness, adaptability, evolvability, agility, scalability, etc.) and evaluate the ability of the solution or service to satisfy critical quality attributes during development.

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

10. The customer interaction with the program team is positive.

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

11. My customer would say that the solution or service we deliver mitigates operational risk or mission threats.

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

12. My customer would say that the solution or service we deliver meets all critical quality attributes (affordability, agility, scalability, etc.).

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

13. The CACI program team consistently meets all customer cost and schedule objectives.

Not At All	A Little	Moderately	Considerably	To A Great Extent	Unknown
○	○	○	○	○	○

Demographics

Predominate Program Type (select only one)	**Approximate Program Value (annual revenue):**			
○ Solution Development	$0M - $5M	$5M - $15M	$15M - $50M	Above $50M

○ Service Delivery ○ Professional Services	○	○	○	○

Program Risk Classification ○ High ○ Medium ○ Low

Program Visibility Classification ○ High ○ Medium ○ Low

Approximate Team Size (FTEs): ________

A.2 RAW SURVEY RESPONSES

Table 1 provides the raw results of the survey to include the respondents (Resp) and their answers to questions 1 through 13 (Q1 through Q13) and program type (PT) of Solution Development (SD), Services (SVC), or Professional Services (PS).

Table 1. Raw Survey Responses

Resp	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**	**Q11**	**Q12**	**Q13**	**PT**
1	3	3	3	4	3	4	3	3	3	3	3	4	5	PS
2	1	1	3	4	3	4	3	4	5	5	3	4	4	PS
3	1	1	1	3	2	2	2	2	3	5	4	4	5	PS
4	1	1	1	1	3	1	4	1	1	3	1	2	5	SVC
5	3	2	2	4	4	1	1	3	5	5	5	5	5	SVC
6	5	5	4	5	5	3	4	5	5	4	5	4	4	PS
7	5	4	4	4	3	4	5	4	4	5	4	4	5	SVC
8	3	3	3	3	3	4	4	2	3	4	3	4	4	SVC
9	5	5	5	5	1	1	5	3	2	5	4	5	4	SVC
10	5	4	5	4	4	5	5	5	4	5	5	5	5	SVC
11	5	5	5	5	5	5	5	5	5	5	5	5	5	PS
12	2	2	2	4	2	1	1	4	4	5	5	4	5	SVC
13	1	1	2	3	4	2	2	3	3	4	5	5	4	PS
14	2	1	2	5	4	2	3	5	4	5	5	5	5	PS
15	3	5	3	3	5	5	5	5	4	5	5	5	5	PS
16	3	3	3	4	4	4	4	4	4	5	4	4	4	PS
17	3	2	3	4	1	2	2	4	3	3	2	2	2	SD
18	2	1	1	2	2	1	1	3	1	4	1	5	5	PS
19	4	4	3	3	1	2	2	5	5	4	3	4	5	SVC
20	1	1	1	2	1	2	2	1	2	5	4	3	5	SD
21	3	5	4	4	3	1	1	5	4	4	4	4	4	SVC

22	2	5	1	3	4	2	2	5	5	5	4	4	1	SVC
23	2	1	1	5	1	5	5	4	3	5	4	5	5	PS
24	3	4	2	3	1	1	1	2	2	5	4	3	5	SD
25	2	1	2	4	3	2	2	3	3	5	4	3	3	SVC
26	4	5	2	4	4	3	4	5	4	5	4	4	5	SD
27	3	3	2	2	1	1	1	1	1	3	3	3	2	SD
28	4	4	4	5	4	4	4	4	4	4	4	4	4	PS
29	3	4	3	4	3	2	2	3	3	5	4	5	5	SD
30	5	4	4	5	4	1	5	2	3	3	4	4	5	SD
31	4	3	1	5	2	1	1	5	5	5	1	4	5	SD
32	3	3	2	2	1	1	1	2	3	4	4	3	3	SD
33	3	3	2	3	3	4	2	3	2	5	4	4	5	SVC
34	2	2	1	2	5	1	1	3	1	3	4	5	5	PS
35	2	3	4	4	4	1	1	2	2	3	4	4	4	PS
36	1	1	1	4	5	1	1	2	5	5	5	5	5	SVC
37	4	3	3	5	4	5	5	5	4	5	5	5	5	PS
38	4	5	4	4	2	2	2	1	3	5	4	4	4	SVC
39	4	1	3	5	3	2	4	1	4	5	4	5	5	PS
40	3	1	3	3	1	4	4	3	3	5	4	4	5	SVC
41	4	4	3	5	2	1	1	1	1	4	2	3	5	SD
42	4	4	4	5	4	4	5	4	4	5	4	1	5	SD
43	3	4	4	4	5	3	2	2	3	3	4	5	5	SD
44	3	4	4	5	4	4	5	4	5	5	4	4	4	SD
45	3	3	3	3	1	2	3	2	3	5	4	3	4	SD
46	5	5	5	5	1	5	5	5	5	5	5	5	5	SD
47	4	4	4	5	5	3	3	3	4	5	5	5	5	SVC
48	3	3	2	4	5	2	3	4	4	5	5	5	5	PS
49	4	2	2	2	4	3	3	1	2	3	3	3	4	SD
50	2	4	5	5	4	5	5	3	1	4	4	3	4	SVC
51	5	5	5	4	4	1	1	3	2	4	4	3	4	SD
52	5	4	4	5	5	1	5	5	4	5	5	5	5	PS
53	4	4	3	3	3	3	1	3	3	4	4	4	4	PS
54	1	1	1	1	1	1	1	1	1	4	1	4	5	PS
55	3	2	3	3	4	1	3	3	4	5	4	5	5	SD
56	5	5	4	5	5	4	4	5	5	4	5	5	5	PS
57	3	1	2	5	5	1	1	5	2	2	3	2	4	SVC
58	4	5	4	5	5	4	4	3	5	4	4	3	5	SVC
59	3	2	3	4	3	4	4	2	2	4	4	4	4	PS
60	3	1	2	5	1	3	2	1	1	2	4	5	5	SVC
61	3	3	2	4	2	5	4	4	4	5	4	4	5	SD
62	4	4	3	4	5	2	5	4	5	5	5	4	5	SD
63	5	5	5	4	5	1	5	5	5	3	4	4	4	SD
64	1	1	1	2	1	2	2	3	3	4	3	4	3	SD
65	2	2	3	3	3	2	2	3	3	4	4	4	4	PS
66	2	1	2	2	3	1	1	1	1	4	4	4	5	PS
67	5	2	2	2	3	1	2	2	3	3	4	3	2	SD
68	3	3	2	3	2	4	4	5	5	5	5	5	5	SD
69	4	3	4	5	4	4	4	5	5	5	5	5	4	PS
70	4	4	3	4	1	4	4	1	1	1	1	1	1	SD

71	5	2	3	5	5	3	4	5	5	5	5	5	5	SVC
72	4	5	4	5	5	4	4	4	5	5	4	3	4	SVC
73	2	1	2	4	3	3	3	3	3	4	5	5	5	SVC
74	1	1	1	3	1	4	4	4	3	5	5	5	5	PS
75	2	3	3	4	3	1	1	1	2	5	4	4	5	PS
76	4	2	1	2	3	2	2	2	3	5	4	3	4	SD
77	4	4	4	5	4	4	5	5	5	5	5	4	5	SD
78	4	4	4	5	5	1	1	2	3	4	5	4	4	SVC
79	4	5	3	4	4	4	4	3	3	5	4	4	4	SVC
80	3	1	2	4	3	1	1	4	4	5	4	4	5	PS
81	5	3	5	3	4	3	3	2	2	5	4	4	4	PS
82	2	2	2	3	2	2	2	3	3	3	3	3	3	PS
83	3	4	3	4	1	1	1	5	5	5	4	4	5	SVC
84	5	5	3	4	3	2	2	5	5	4	4	4	4	SD
85	4	3	4	5	4	3	3	5	5	5	4	5	5	PS
86	4	4	4	5	3	3	4	4	4	5	5	5	4	SVC
87	4	5	4	4	1	1	1	4	2	5	4	1	4	SD
88	1	1	1	1	1	1	1	2	4	5	5	4	3	SD
89	3	3	1	5	5	1	1	3	3	5	5	5	5	SVC
90	1	1	2	3	4	1	1	3	4	5	5	5	5	SVC
91	2	2	1	2	1	2	2	1	1	3	4	3	4	SVC
92	5	5	4	4	4	1	1	5	5	3	4	5	4	PS
93	3	1	2	3	1	2	2	3	3	5	3	4	5	SD
94	3	3	3	4	3	4	4	2	4	5	4	4	5	SD
95	3	2	2	1	2	2	2	3	3	5	4	5	4	SD
96	4	4	3	5	4	5	4	5	3	5	4	4	3	SD
97	1	2	4	4	2	3	2	5	4	5	4	5	5	PS
98	3	1	1	4	1	5	5	4	4	5	4	5	5	PS
99	2	5	3	4	3	1	1	2	2	5	4	4	4	PS
100	2	4	2	5	4	1	1	5	3	5	4	4	5	PS
101	3	4	4	4	4	2	1	1	1	5	4	3	5	PS
102	1	1	1	3	2	2	2	2	2	5	3	5	4	PS
103	3	3	3	4	3	2	4	5	5	5	3	3	3	SVC
104	5	4	4	3	1	4	3	2	2	5	4	5	3	PS

APPENDIX C – PAPERS

C.1 2015 IEEE SOFTWARE TECHNOLOGY CONFERENCE

This paper was accepted, presented, and published as part of the conference proceedings.

C.2 2016 CONFERENCE ON SYSTEMS ENGINEERING RESEARCH

This paper was accepted, presented, and published in a special peer-reviewed issue of the INCOSE Systems Engineering journal.

C.3 2016 INCOSE INTERNATIONAL SYMPOSIUM

This paper was accepted for a poster session at the conference.

C.1 2015 IEEE SOFTWARE TECHNOLOGY CONFERENCE

USING OPERATIONAL RISK MANAGEMENT TO INCREASE SYSTEMS ENGINEERING EFFECTIVENESS

Brian P. Gallagher
Senior Vice President, Operational Excellence
CACI International, Inc.
brian.gallagher@colostate.edu, bgallagher@caci.com

Dr. Kenneth Nidiffer
Director of Strategic Plans for Government Programs
Carnegie Mellon University, Software Engineering Institute
nidiffer@sei.cmu.edu

Dr. Ronald M. Sega
Director, Systems Engineering
Colorado State University
ron.sega@colostate.edu

ABSTRACT

One measure of effectiveness of any given systems engineering practice is the ability of that practice to mitigate product or project risk. Product and project risk reduction is the focus of most risk management processes. When a project team has a robust risk management process, it continually identifies risks that may impact its ability to produce a product that meets customer requirements within cost and schedule constraints.

One missing aspect of most systems engineering risk management approaches is a focus on operational risk. That is, the evolving risk to business or mission needs of the end-user. This lack of focus on operational risk during the engineering process encourages the creation of a chasm between evolving need and delivered product capabilities. The longer the development process, the wider that gap, and the end-user becomes less receptive to deeming the capability operationally effective.

The purpose of this research is to introduce operational risk concepts into the systems engineering process, specifically through the use of operational risk scenarios, with the goal of improving program outcomes. This paper introduces ORDERED, a repeatable method used to influence systems engineering practices by continually identifying operational risks before and throughout the engineering lifecycle.

Keywords: Risk Management, Systems Engineering, Software Engineering, Operational Risk Management

INTRODUCTION

Systems engineering is *an interdisciplinary approach and means to enable the realization of successful systems*[1]. The practices, approaches, methods, and tools of systems engineering have been codified over time and evolve as technology and system complexity increases. The purpose of having a set of proven practices for engineers to follow is to reduce system development risk and increase the probability of delivering a system that meets an operational need[2].

The tools applied to a given problem are selected based on an understanding of certain quality attributes of the product under development or the management aspects of the team producing the product within cost and schedule constraints. Therefore, a given practice is only viewed as effective if it reduces product or project risk or improves product or project outcomes at the same risk level.

Product-focused or technical risk is concerned with the technical performance and quality attributes of the end product. **For example**, a product may have stringent reliability requirements. Another product may have near real-time processing requirements. The systems engineering methods and tools for mitigating reliability risks may include using design patterns such as redundant hardware and software or fault detection and remediation mechanisms. Products with real-time requirements might use design patterns with the ability to ensure schedulability and analyze process behavior.

Project-focused or management risk is concerned with the management aspects of the development lifecycle. For example, if a project has multiple customers who are prone to having conflicting requirements, rapid-prototyping and user juries may be used as approaches to mitigate these stakeholder involvement risks.

If the product is dependent on other components or products that are developed simultaneously, the project may select architectural patterns that separate concerns and allow independent evolution of components by separate teams or collaboration tools such as employing an Interface Control Working Group to mitigate the risk of the inter-operating systems having deployment issues.

One missing aspect of most systems engineering risk management processes, such as those described in the Guide to the Systems Engineering Body of Knowledge[3] or the INCOSE Systems Engineering Handbook[1], is a focus on evolving operational risk during system development.

Wrubel and Gross describe this disconnect, stating, ...*requirements for any given system are highly likely to evolve between the development of a system concept and the time at which* *the system is operationally deployed as new threats, vulnerabilities, technologies, and conditions emerge and users adapt their understanding of their needs as system development progresses*[4].

Some project teams attempt to manage this risk by selecting an evolutionary approach, which allows for an incremental commitment to design decisions and incorporates *off-ramps* and *on-ramps* for technology or addition of new requirements due to changes in mission need[5].

These threats, vulnerabilities, and technology changes could effect operational risk. When the operational risk is great, end-users bypass the traditional engineering process and create more streamlined avenues to acquire capability.

During Operation Iraqi Freedom, the United States Army faced a new and evolving threat. Enemy forces were no match for a traditional military, so it relied on asymmetric tactics. Improvised Explosive Devices became the weapon of choice because they were easy to build and deploy and were highly effective. The Army wasn't prepared either in terms of detection and defeat systems or from a psychological perspective.

Coupled with an acquisition process that was slow to react to the evolving operational threat and outcry from both service members and the general population, the Army created the Joint Improvised Explosive Device Defeat Organization (JIEDDO) with the sole purpose of defeating this new operational risk. JIEDDO, recently re-named the Joint Improvised-Threat Defeat Agency, was able to bypass the Army's acquisition process and get equipment and capabilities to the field quickly.

From a tactical perspective, the focus on defeating a specific operational risk was successful. Capabilities were fielded, and lives were saved. From a strategic perspective, these quickly-fielded systems lack certain quality attributes such as robustness, evolvability, and maintainability that would have been considered in a traditional systems engineering approach. The resulting quickly-fielded capabilities increased total cost of ownership and logistical complexity[6].

When system requirements are created to solely reduce strategic risk such as affordability or other long-term efficiencies, the resulting systems could be less relevant from a tactical or operational perspective. The driving requirements are associated with cost reduction, reducing redundant systems, or integrating capabilities rather than mitigating near-term operational risk.

The Air Force's Expeditionary Combat Support System had only a vague set of objectives when it began development in 2004[7]. According to a report by the United States Senate Permanent Subcommittee on Investigations, these objectives resulted in ...*a new, fully-integrated logistics system that* *would replace an unspecified number of older, unconnected logistics systems*. This lack of clarity and disconnect between solving critical operational threats and risks resulted in $1.1 billion in wasted funding and a system that was not deployable.

According to Senator John McCain, (R-Arizona), *The Air Force's Expeditionary Combat Support System, or E.C.S.S., is a prime example of how a system designed to save money can actually waste billions of taxpayer dollars without producing any usable capability*[8].

To increase the effectiveness of systems engineering, its practices, methods, and tools need to have a greater emphasis on eliciting and understanding operational risk and the development of enhanced methods to continually track and react to evolving operational threat and risk during the development, deployment, and sustainment phases of the system lifecycle. To that end, this paper introduces an approach that may be used to influence systems engineering activities with the objective of improving operational effectiveness and acceptance of engineered solutions.

This approach is referred to here as Operational Risk-Driven Engineering Requirements/Engineering Development (ORDERED) and is graphically shown in **Figure 1**.

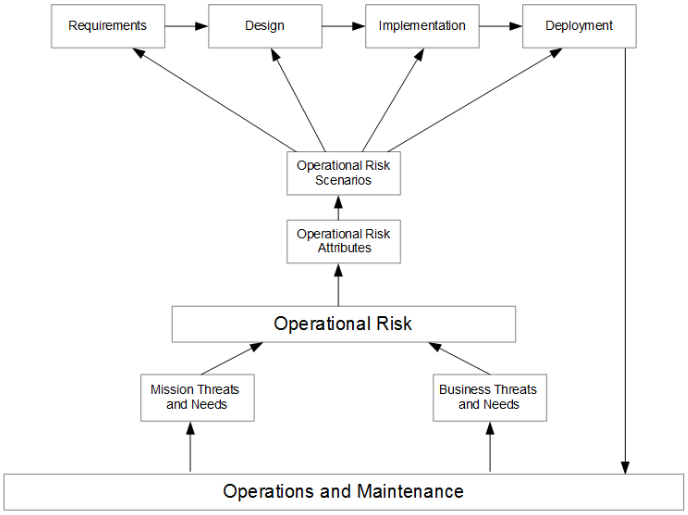

Requirements
Design
Implementation
Deployment
Operational Risk Scenarios
Operational Risk Attributes
Operational Risk
Mission Threats and Needs
Business Threats and Needs
Operations and Maintenance

Figure 1. The ORDERED Approach

OPERATIONAL RISK

For the purpose of ORDERED, operational risk is defined simply as the possibility of suffering mission or business loss. Mission loss in terms of less effective mission accomplishment or complete failure to accomplish mission objectives. Business loss in terms of economic affordability or long-term viability of performing the mission.

An operational organization is any group of individuals teamed together with a common purpose to carry out a mission. A mission is comprised of a specific task or set of tasks carried out by operational personnel[9]. Tasks may be described as either mission-essential or mission-support[10].

Mission-essential tasks directly contribute to mission execution. For example, if the operational organization was a community fire department, mission-essential tasks could include emergency response, firefighting, and rescue tasks. Mission-support tasks could include equipment maintenance, training, and fire prevention awareness.

Mission risks would be driven by any number of conditions such as events, activities, processes, and systems that could impact the operational organization's ability to perform its mission or could negatively impact the full accomplishment of the mission. The impact is tactical in that the mission is impacted directly.

Business risks are also driven by similar conditions, but the impact is more strategic. A flat-tire on a fire truck is a risk to performing the mission task of fighting fires, and therefore, may be described as a mission risk. A lower tax-base in a community may impact the fire department's ability to perform preventive maintenance or hire and train future firefighters, and therefore, could be described as a business risk. This distinction is valuable when identifying operational risk.

When a focus is solely on immediate mission risks, longer-term considerations such as affordability or long-term viability of the organization are ignored. When the focus is solely on business risks, mitigation actions or system solutions may not be operationally effective in the short-term. The balance between mission and business considerations helps ensure that solutions and mitigation actions are both operationally relevant and support the strategic needs of the organization.

THE ORDERED APPROACH

The ORDERED process steps are shown in **Figure 2.** ORDERED is a continuous process where operational risks are identified and analyzed throughout the engineering process. The risks or risk areas are characterized by identifying operational risk attributes and scenarios to further describe the concern in a manner that helps bridge the gap between operational activities and engineering activities. These scenarios are then evaluated against current and future engineering activities to ensure that requirements and development activities mitigate operational risk.

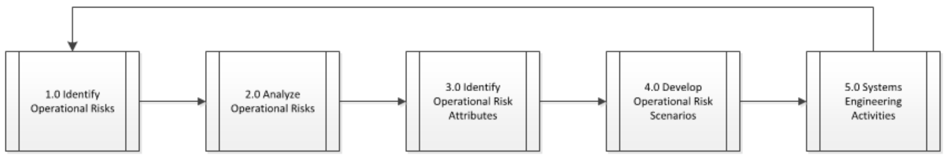

1.0 Identify Operational Risks
2.0 Analyze Operational Risks
3.0 Identify Operational Risk Attributes
4.0 Develop Operational Risk Scenarios
5.0 Systems Engineering Activities

Figure 2. ORDERED Process Steps

A. *Identify Operational Risks*

Risks are identified by having a clear understanding of the mission and business context of the operational organization to include mission-critical and mission-support tasks, objectives, and success criteria and then exploring areas of concern based on potentially failing to achieve, or fully achieve, operational mission success.

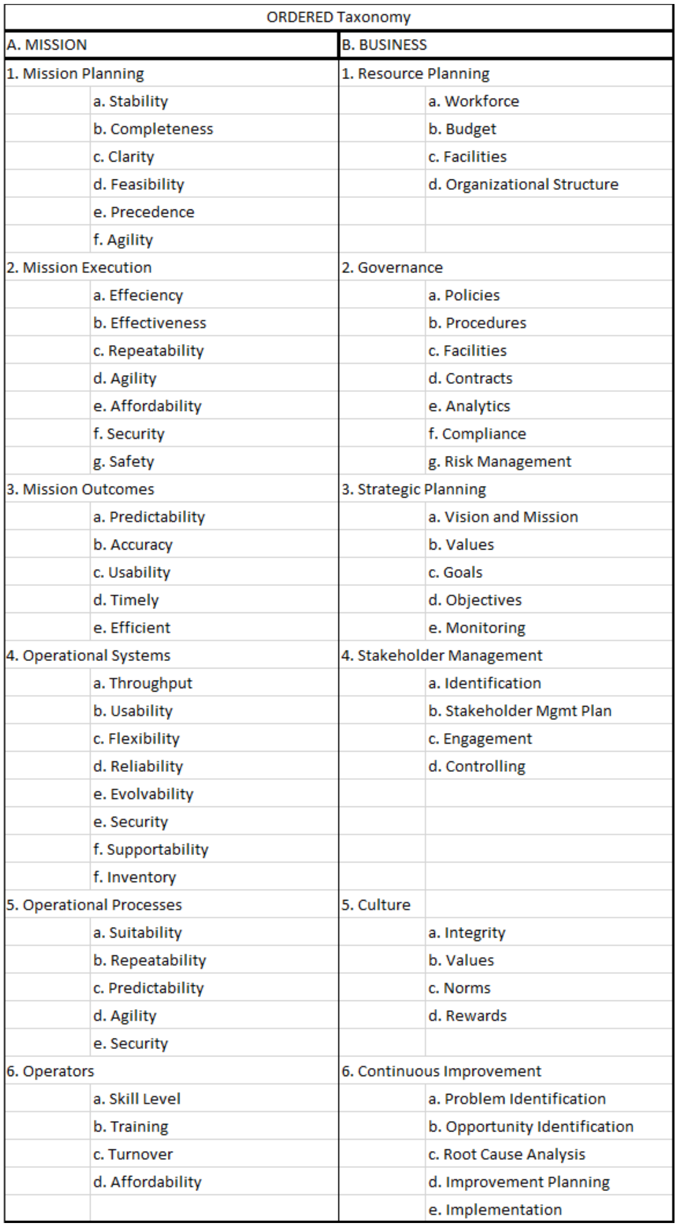
There are many methods for identification of risk that include continuous risk identification by all members of the organization, structure risk identification sessions, and milestone or event-based risk identification[3]. Structured risk identification sessions are facilitated activities with stakeholders and subject matter experts available to help brainstorm operational risks. Individual risk statements are captured in a structured manner to allow for analysis.

Regardless of identification method or methods used, sources of risk are explored by operational personnel and systems engineers. ORDERED uses a taxonomy to help with risk identification. A taxonomy is useful both when exploring sources of risk as well as when classifying risks after they are identified to help with the Analyze Operational Risks process.

The ORDERED Taxonomy is shown in **Figure 3**. The taxonomy was developed and simplified by considering several source documents[11, 12, 13, 14] as well as personal experience.

The ORDERED taxonomy consists of two *categories*: Mission and Business. The next level of the taxonomy contains *elements* such as Mission Planning, Operational Systems, and Culture. The final level of the taxonomy consists of *attributes*.

Operational organizations use the taxonomy to help identify both mission-impacting concerns as well as business-impacting



ORDERED Taxonomy			
A. MISSION		B. BUSINESS	
1. Mission Planning		1. Resource Planning	
	a. Stability		a. Workforce
	b. Completeness		b. Budget
	c. Clarity		c. Facilities
	d. Feasibility		d. Organizational Structure
	e. Precedence		
	f. Agility		
2. Mission Execution		2. Governance	
	a. Effeciency		a. Policies
	b. Effectiveness		b. Procedures
	c. Repeatability		c. Facilities
	d. Agility		d. Contracts
	e. Affordability		e. Analytics
	f. Security		f. Compliance
	g. Safety		g. Risk Management
3. Mission Outcomes		3. Strategic Planning	
	a. Predictability		a. Vision and Mission
	b. Accuracy		b. Values
	c. Usability		c. Goals
	d. Timely		d. Objectives
	e. Efficient		e. Monitoring
4. Operational Systems		4. Stakeholder Management	
	a. Throughput		a. Identification
	b. Usability		b. Stakeholder Mgmt Plan
	c. Flexibility		c. Engagement
	d. Reliability		d. Controlling
	e. Evolvability		
	e. Security		
	f. Supportability		
	f. Inventory		
5. Operational Processes		5. Culture	
	a. Suitability		a. Integrity
	b. Repeatability		b. Values
	c. Predictability		c. Norms
	d. Agility		d. Rewards
	e. Security		
6. Operators		6. Continuous Improvement	
	a. Skill Level		a. Problem Identification
	b. Training		b. Opportunity Identification
	c. Turnover		c. Root Cause Analysis
	d. Affordability		d. Improvement Planning
			e. Implementation

Figure 3. The ORDERED Risk Taxonomy

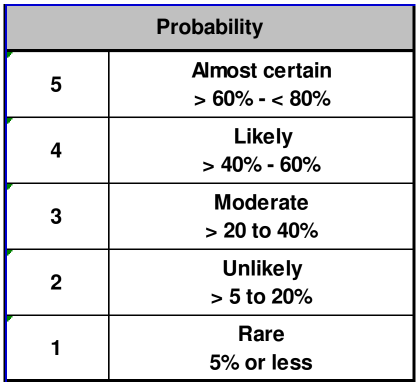
concerns. This allows a balance between short-term mission risks and longer-term business risks.

B. *Analyze Operational Risks*

Risk Exposure (RE) is the product of the probability (P) that the risk will occur and the impact (I) to the organization if the risk occurs: RE = P x I. The goal in determining risk exposure is to understand the relative criticality of a given risk in order to help decide which risks should be mitigated, in what order, and the number of resources that the organization is willing to expend on mitigation activities.

Determining risk exposure is not an exact science and relies on the best judgment of individuals. For this reason the ORDERED approach keeps this step simple.

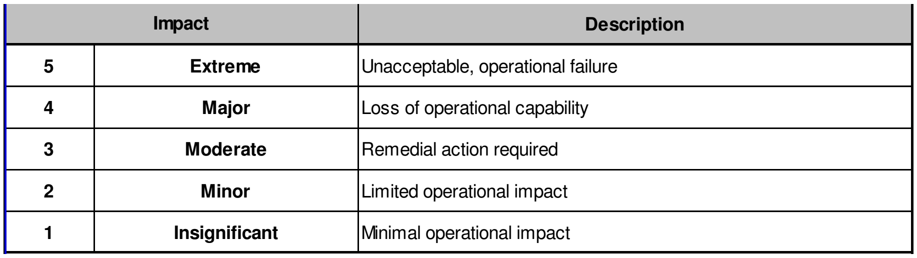
The operational organization must decide how to assign a probability and impact score to each risk. ORDERED uses a simple 1 to 5 rating for probability as shown in **Figure 4**, with 1 being the lowest probability of occurrence and 5 being the highest probability of occurrence.



Probability	
5	Almost certain > 60% - < 80%
4	Likely > 40% - 60%
3	Moderate > 20 to 40%
2	Unlikely > 5 to 20%
1	Rare 5% or less

Figure 4. Probability of Occurrence

While probability of occurrence becomes a simple determination of likelihood of the risk occurring based on best judgment, impact of occurrence must take into consideration the impact of the risk to the mission or business needs of the organization. Each operational organization will adjust the impact definitions to meet its needs. A generic impact of occurrence table is shown in **Figure 5.**



Impact		Description
5	Extreme	Unacceptable, operational failure
4	Major	Loss of operational capability
3	Moderate	Remedial action required
2	Minor	Limited operational impact
1	Insignificant	Minimal operational impact

Figure 5. Impact of Occurance

Prioritizing risks provides decision-makers with the ability to allocate scarce resources to mitigate the most important risks to mission success. A simple risk matrix as shown in **Figure 6** allows for a quick visual for decision-makers when allocating resources to mitigate operational risk.

		Insignificant	Minor	Moderate	Major	Extreme
		1	2	3	4	5
Almost Certain	5	🟨	🟨	🟥	🟥	🟥
Likely	4	🟩	🟨 RISK001 RISK005	🟨	🟥 RISK003 RISK004	🟥
Moderate	3	🟩	🟨	🟨	🟨	🟥
Unlikely	2	🟩	🟩	🟨 RISK002	🟨	🟥
Rare	1	🟩	🟩	🟩	🟨	🟨

Figure 6. Risk Matrix

In this example, both RISK003 and RISK004 have a major impact on operations and are both likely to occur. Priority would be given to ensure that these two risks are mitigated by systems engineering activities and project design decisions.

C. *Identify Operational Risk Attributes*

An operational risk attribute is a characteristic of the operational mission or business that will be judged negatively by stakeholders unless the operational risk is mitigated. The purpose of mapping operational risk attributes to risk statements is to further clarify the operational concern and to help when identifying mitigation actions.

A starting point in mapping operational risk attributes is the ORDERED risk taxonomy. The lowest level of the taxonomy contains attributes describing the aspect of risk associated with the elements and categories of the taxonomy. Additional attributes to explore include quality attributes as described in

Attribute Driven Design[15] engineering approaches and the Method Framework for Engineering System Architectures[16].

In addition to understanding the attributes associated with the operational risk, additional insight into the actual concern is useful when determining mitigation actions. While it helps to understand that a given risk is associated with an ORDERED taxonomic *element* and *attribute*, the additional understanding from eliciting the area of concern from the individual or group who identified the risk provides more definitive focus.

For example, an operator may have identified the following risk: *Current systems were designed using nominal data loads; the system may not scale.* The risk could be mapped to the Operational Systems *element* and Throughput *attribute* of the taxonomy.

Simply knowing that Throughput is an attribute may not provide enough detail. The attribute concern in this example could be described as mission stress. The operator is specifically concerned about how the system will operate when the mission becomes much more intense and the system needs to operate effectively when additional source data are processed.

D. *Develop Scenarios*

Scenarios are simply expressions of real-world interactions. They may be formal, structured and verbose, or freer form and expressed simply[17]. The purpose of scenarios as used to influence engineering activities is to describe expected results of a system during development in terms of real-world behavior[18]. Scenarios describe how the system should behave under certain conditions when presented with certain stimuli[19].

Operational risk scenarios describe the unwanted behavior of the system that would cause mission or business impact to the operational organization. Similar to the concept of anti-patterns in systems and software engineering[20], operational risk scenarios describe undesirable outcomes that need to be mitigated as they increase operational risk.

The ORDERED method uses a simplified format to describe the risk scenario based on the Architecture Tradeoff Analysis Method[21]. The operational risk scenario should describe a source that provides a stimulus to a system or operational task, the environment or artifact effected by the stimulus, and the unwanted response or outcome. Example operational risk scenarios are listed below:

1. *An operator requests fire suppression during a high intensity operation with degraded communications, and the request fails to transmit within five minutes.*
2. *A resource manager attempts to re-assign a military member while the member is relocating to a new assignment, and the system fails to locate the member.*

The key difference between engineering scenarios and operational risk scenarios is that operational risk scenarios describe negative or unwanted behavior or outcomes while engineering scenarios describe expected behavior or outcomes.

E. *Influence Systems Engineering*

Informing systems or software engineering activities with operational risk scenarios becomes part of the project's overall engineering activities. This is a continuous process of refining requirements, design and architectural decisions, implementation choices, testing approaches, and deployment strategies to mitigate operational risk so that the resulting behavior of the system, product, or capability avoids high priority operational risk scenarios.

Boehm recommends a requirements approach that includes emphasizing value-driven, shared-vision-driven, change-driven, and risk-driven activities[22]. Central to these approaches is exploration of operational scenarios describing intended behavior.

Risk-driven activities allow engineering leadership to apply resources to mitigate highest risks or to avoid performing activities that increase risk. The addition of operational risk scenarios to expected behavior scenarios allows engineers and operational users to explore behavior that they want the resulting system, product, or capability to help mitigate or avoid.

Informing architecture and design with operational risk scenarios is part of a larger architecture and design validation activity. Architecture is simply the highest level of design. It represents the first artifact that structures a system, component, or capability into its constituent physical or logical sub-parts.

It also represents the first opportunity to ensure that the resulting design and implementation enables desired attributes and avoids undesirable attributes. The addition of operational risk scenarios during architectural development and validation allows architects and engineers to select or create architectural mechanisms and constructs to avoid operational risk.

Using operational risk scenarios to influence implementation decisions allows for more robust trade decisions whereby selected implementation details are chosen to mitigate operational risk. Testing approaches and deployment strategies influenced by the end-user’s most critical operational risk scenarios are likely to improve operational acceptability of new systems, components, or capabilities.

CONCLUSION AND FURTHER RESEARCH AREAS

Operational risk should drive systems engineering activities from concept development through deployment. The reason that a new system or capability is developed is to mitigate some mission or business need or threat. These needs and threats evolve over time, yet most engineering approaches ignore operational risk, allowing the chasm between the evolving need and the system under development to grow.

This paper introduced ORDERED, a repeatable approach designed to influence systems engineering activities through a continuous focus on operational risk. The next steps are to apply the approach and evaluate the outcomes. Adding operational *opportunity* scenarios to operational *risk* scenarios may enrich the approach further by eliciting opportunities to enhance mission effectiveness during the engineering lifecycle.

Many factors influence the success or failure of a development project. A structured focus on the evolving mission and business needs and threats of end-users aimed at explicitly driving requirements and informing engineering activities should improve the operational acceptability of the system, component, or capability under development.

REFERENCES

1. Wiley, INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. 2015: Wiley.

2. Elm, J.P. and D.R. Goldenson, The Business Case for Systems Engineering Study: Results of the Systems Engineering Effectiveness Survey. 2012, DTIC Document.

3. Pyster, A., et al., Guide to the Systems Engineering Body of Knowledge (SEBoK), 2012.

4. Wrubel, E. and Jon Gross, Contracting for Agile Software Development in the Department of Defense: An Introduction (CMU/SEI-2015-TN-006). 2015, Retrieved August 22, 2015, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=442499.

5. Boehm, B. and J.A. Lane, Using the incremental commitment model to integrate system acquisition, systems engineering, and software engineering. CrossTalk, 2007. 19(10): p. 4-9.

6. Ellis, R.F., R.D. Rogers, and B.M. Cochran, Joint Improvised Explosive Device Defeat Organization (JIEDDO): Tactical Successes Mired in Organizational Chaos; Roadblock in the Counter-IED Fight. 2007, DTIC Document.

7. Aronin, B.S., et al., Expeditionary Combat Support System: Root Cause Analysis. 2011, DTIC Document.

8. McCain, J. FLOOR REMARKS BY SENATOR JOHN MCCAIN ON THE AIR FORCE'S ECSS PROGRAM. 2014, Available from: http://www.mccain.senate.gov/public/index.cfm/2014/7/floor-remarks-by-senator-john-mccain-on-the-air-force-s-ecss-program.

9. Gallagher, B.P., Interpreting Capability Maturity Model Integration (CMMI) for Operational Organizations. 2002.

10. Air Force Instruction 90-1 102, Performance Management. 2000.

11. Gallagher, B.P., et al., A Taxonomy of Operational Risks. 2005.

12. Gallagher, B., et al., CMMI for Acquisition: Guidelines for Improving the Acquisition of Products and Services. 2011: Addison-Wesley Professional.

13. ISO, I., 31000: 2009 Risk management–Principles and guidelines. International Organization for Standardization, Geneva, Switzerland, 2009.

14. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). 2013: Project Management Institute, Incorporated.

15. Wojcik, R., et al., Attribute-Driven Design (ADD), Version 2.0. 2006, DTIC Document.

16. Firesmith, D.G., et al., The method framework for engineering system architectures. 2008: CRC Press.

17. Sutcliffe, A. Scenario-based requirements engineering in Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International. 2003.

18. Mylopoulos, J., L. Chung, and E. Yu, From object-oriented to goal-oriented requirements analysis. Communications of the ACM, 1999. 42(1): p. 31-37.

19. Bass, L., Mark Klein, and Gabriel Moreno, Applicability of General Scenarios to the Architecture Tradeoff Analysis Method (CMU/SEI-2001-TR-014). 2001, Retrieved August 22, 2015, from the Software Engineering Institute, Carnegie Mellon University.

20. Brown, W.H., R.C. Malveau, and T.J. Mowbray, AntiPatterns: refactoring software, architectures, and projects in crisis. 1998.

21. Kazman, R., Mark Klein, and Paul Clements, ATAM: Method for Architecture Evaluation (CMU/SEI-2000-TR-004). 2000, Retrieved August 22, 2015, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=5177.

22. Selby, R.W., Software engineering: Barry W. Boehm's lifetime contributions to software development, management, and research. Vol. 69. 2007: John Wiley & Sons.

C.2 2016 CONFERENCE ON SYSTEMS ENGINEERING RESEARCH

2016 Conference on Systems Engineering Research

USING OPERATIONAL RISK TO INCREASE SYSTEMS ENGINEERING EFFECTIVENESS

Brian P. Gallagher[a*], Dr. Ronald M. Sega[b], Dr. Kenneth Nidiffer[c]

[a]CACI International, Inc., Arlington, VA 22201, USA
[b]Colorado State University, Fort Collins, CO 80523, USA
[c]Carnegie Mellon University Software Engineering Institute,
Arlington, VA 22201, USA

ABSTRACT

When a project team has a robust risk management process, it continually identifies risks that may impact its ability to produce a product that meets customer requirements within cost and schedule constraints. Typical risk management approaches emphasize the focus on programmatic risk and technical risk.

One missing aspect of systems engineering risk management approaches is a focus on operational risk. That is, the evolving risk to business or mission needs of the end-user. This lack of focus on operational risk during the engineering process encourages the creation of a chasm between evolving need and delivered product capabilities.

The longer the development process, the wider that gap, and the end-user becomes less receptive to deeming the capability operationally effective. This research explores the use of operational risk identification and mitigation techniques during the systems engineering process. An approach to identify operational risk and to use risk scenarios to influence systems engineering is discussed, and the results of a survey correlating operational risk management and project outcomes is presented.

© 2016 Gallagher, Sega, and Nidiffer.

Keywords: Systems Engineering, Risk Management, Operational Risk Management, Risk Scenarios

1. INTRODUCTION

Systems engineering is *an interdisciplinary approach and means to enable the realization of successful systems*[1]. The practices, approaches, methods, and tools of systems engineering have been codified over time and evolve as technology and system complexity increases. The purpose of having a set of proven practices for engineers to follow is to reduce system development risk and increase the probability of delivering a system that meets an operational need[2].

The tools applied to a given problem are selected based on an understanding of certain quality attributes of the product under development or the management aspects of the team producing the product within cost and schedule constraints. Therefore, a given practice is only viewed as effective if it reduces product or project risk or improves product or project outcomes at the same risk level.

Product-focused or technical risk is concerned with the technical performance and quality attributes of the end product. For example, a product may have stringent reliability requirements. Another product may have strict real-time processing requirements.

The systems engineering methods and tools for mitigating reliability risks may include using design patterns such as redundant hardware and software or fault detection and remediation mechanisms. Products with real-time requirements might use design patterns with the ability to ensure schedulability and analyze process behavior.

Project-focused or management risk is concerned with the management aspects of the development lifecycle. For example, if a project has multiple customers who are prone to having conflicting requirements, rapid-prototyping and user juries may be used as approaches to mitigate these stakeholder involvement risks.

If the product is dependent on other components or products that are developed simultaneously, the project team may select architectural patterns that separate concerns and allow independent evolution of components by separate teams or collaboration tools such as employing cross-project Integrated Product Teams to mitigate the risk of the inter-operating systems having deployment issues.

One missing aspect of most systems engineering risk management processes such as those described in the Guide to the Systems Engineering Body of Knowledge[3] or the INCOSE Systems Engineering Handbook[1] is a focus on evolving operational risk during system development.

Wrubel and Gross describe this disconnect, stating,

...*requirements for any given system are highly likely to evolve* *between the development of a system concept and the time at which the system is operationally deployed as new threats, vulnerabilities, technologies, and conditions emerge, and users adapt their understanding of their needs as system development progresses*[4].

Some project teams attempt to manage this risk by selecting an evolutionary approach that allows for an incremental commitment to design decisions and incorporates *off-ramps* and *on-ramps* for technology or addition of new requirements due to changes in mission need[5].

These threats, vulnerabilities, and technology changes could effect operational risk. When the operational risk is great, end-users bypass the traditional engineering process and create more streamlined avenues to acquire capability.

During Operation Iraqi Freedom, the United States Army faced a new and evolving threat. Enemy forces were no match for a traditional military, so it relied on asymmetric tactics. Improvised Explosive Devices became the weapon of choice because they were easy to build and deploy and were highly effective. The Army wasn't prepared either in terms of detection and defeat systems or from a psychological perspective.

Coupled with an acquisition process that was slow to react to the evolving operational threat and outcry from both service members and the general population, the Army created the Joint

Improvised Explosive Device Defeat Organization (JIEDDO) with the sole purpose of defeating this new operational risk. JIEDDO, recently re-named the Joint Improvised-Threat Defeat Agency, was able to bypass the Army's acquisition process and get equipment and capabilities to the field quickly.

From a tactical perspective, the focus on defeating a specific operational risk was successful. Capabilities were fielded, and lives were saved. From a strategic perspective, these quickly-fielded systems lack certain quality attributes such as robustness, evolvability, and maintainability that would have been considered in a traditional systems engineering approach. The resulting quickly-fielded capabilities increased total cost of ownership and logistical complexity[6].

When system requirements are created to solely reduce strategic risk such as affordability or other long-term efficiencies, the resulting systems could be less relevant from a tactical or operational perspective. The driving requirements are associated with cost reduction, reducing redundant systems, or integrating capabilities rather than mitigating near-term operational risk.

The Air Force's Expeditionary Combat Support System had only a vague set of objectives when it began development in 2004[7]. According to a report by the United States Senate Permanent Subcommittee on Investigations, these objectives resulted in ...*a new, fully-integrated logistics system that would replace an unspecified number of older, unconnected logistics systems*.

This lack of clarity and disconnect between solving critical operational threats and risks resulted in $1.1 billion in wasted funding and a system that was not deployable.

According to Senator John McCain, (R-Arizona), *The Air Force's Expeditionary Combat Support System, or E.C.S.S., is a prime example of how a system designed to save money can actually waste billions of taxpayer dollars without producing any usable capability*[8].

To increase the effectiveness of systems engineering, its practices, methods, and tools need to have a greater emphasis on eliciting and understanding operational risk and the development of enhanced methods to continually track and react to evolving operational threat and risk during the development, deployment, and sustainment phases of the system lifecycle.

To that end, this paper describes an approach that may be used to influence systems engineering activities with the objective of improving operational effectiveness and acceptance of engineered solutions. This approach is referred to here as Operational Risk-Driven Engineering Requirements/Engineering Development (ORDERED) and is graphically shown in **Figure 1**.

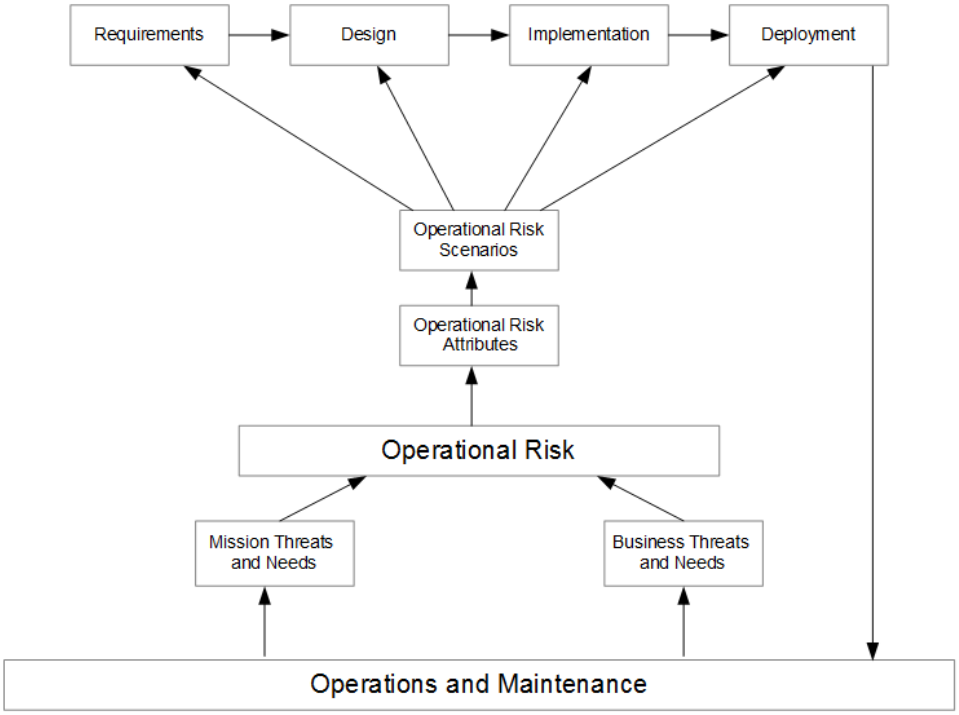

Requirements
Design
Implementation
Deployment
Operational Risk Scenarios
Operational Risk Attributes
Operational Risk
Mission Threats and Needs
Business Threats and Needs
Operations and Maintenance

Figure 1. The ORDERED Approach.

2. OPERATIONAL RISK

For the purpose of ORDERED, operational risk is defined simply as the possibility of suffering mission or business loss. Mission loss in terms of less effective mission accomplishment or complete failure to accomplish mission objectives. Business loss in terms of economic affordability or long-term viability of performing the mission.

An operational organization is any group of individuals teamed together with a common purpose to carry out a mission. A mission is comprised of a specific task or set of tasks carried out by operational personnel[9]. Tasks may be described as either mission-essential or mission-support[10].

Mission-essential tasks directly contribute to mission execution. For example, if the operational organization was a community fire department, mission-essential tasks could include emergency response, firefighting, and rescue tasks. Mission-support tasks could include equipment maintenance, training, and fire prevention awareness.

Mission risks would be driven by any number of conditions such as events, activities, processes, and systems that could impact the operational organization's ability to perform its mission or could negatively impact the full accomplishment of the mission. The impact is tactical in that the mission is impacted directly.

Business risks are also driven by similar conditions, but the impact is more strategic. A flat-tire on a fire truck is a risk to performing the mission task of fighting fires, and therefore, may be described as a mission risk. A lower tax-base in a community may impact the fire department's ability to perform preventive maintenance or hire and train future firefighters, and therefore, could be described as a business risk. This distinction is valuable when identifying operational risk.

When a focus is solely on immediate mission risks, longer-term considerations such as affordability or long-term viability of the organization are ignored. When the focus is solely on business risks, mitigation actions or system solutions may not be operationally effective in the short-term. The balance between mission and business considerations helps ensure that solutions and mitigation actions are both operationally relevant and support the strategic needs of the organization.

2.1. *The ORDERED Approach*

The ORDERED process steps are shown in **Figure 2**. ORDERED is a continuous process where operational risks are identified and analyzed throughout the engineering process. The risks or risk areas are then characterized by identifying operational risk attributes and scenarios to further describe the concern in a manner that helps bridge the gap between operational activities and engineering activities. These scenarios are then evaluated against current and future engineering activities to ensure that

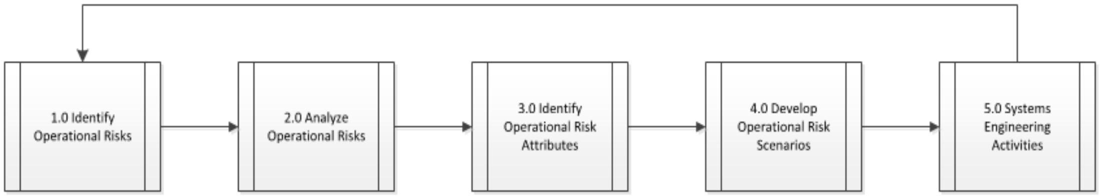

1.0 Identify Operational Risks
2.0 Analyze Operational Risks
3.0 Identify Operational Risk Attributes
4.0 Develop Operational Risk Scenarios
5.0 Systems Engineering Activities

Figure 2. ORDERED Process Steps

requirements and development activities mitigate operational risk.

2.1.1. *Identify Operational Risks*

Risks are identified by having a clear understanding of the mission and business context of the operational organization to include mission-critical and mission-support tasks, objectives, and success criteria and then exploring areas of concern based on potentially failing to achieve, or fully achieve, operational mission success.

There are many methods for identification of risk that include continuous risk identification by all members of the organization, structure risk identification sessions, and milestone or event-based risk identification[3]. Structured risk identification sessions are facilitated activities with stakeholders and subject matter experts available to help brainstorm operational risks. Individual risk statements are captured in a structured manner to allow for analysis.

Regardless of identification method or methods used, sources of risk are explored by operational personnel and systems engineers. ORDERED uses a taxonomy to help with risk identification. A taxonomy is useful both when exploring sources of risk as well as when classifying risks after they are identified to help with the Analyze Operational Risks process.

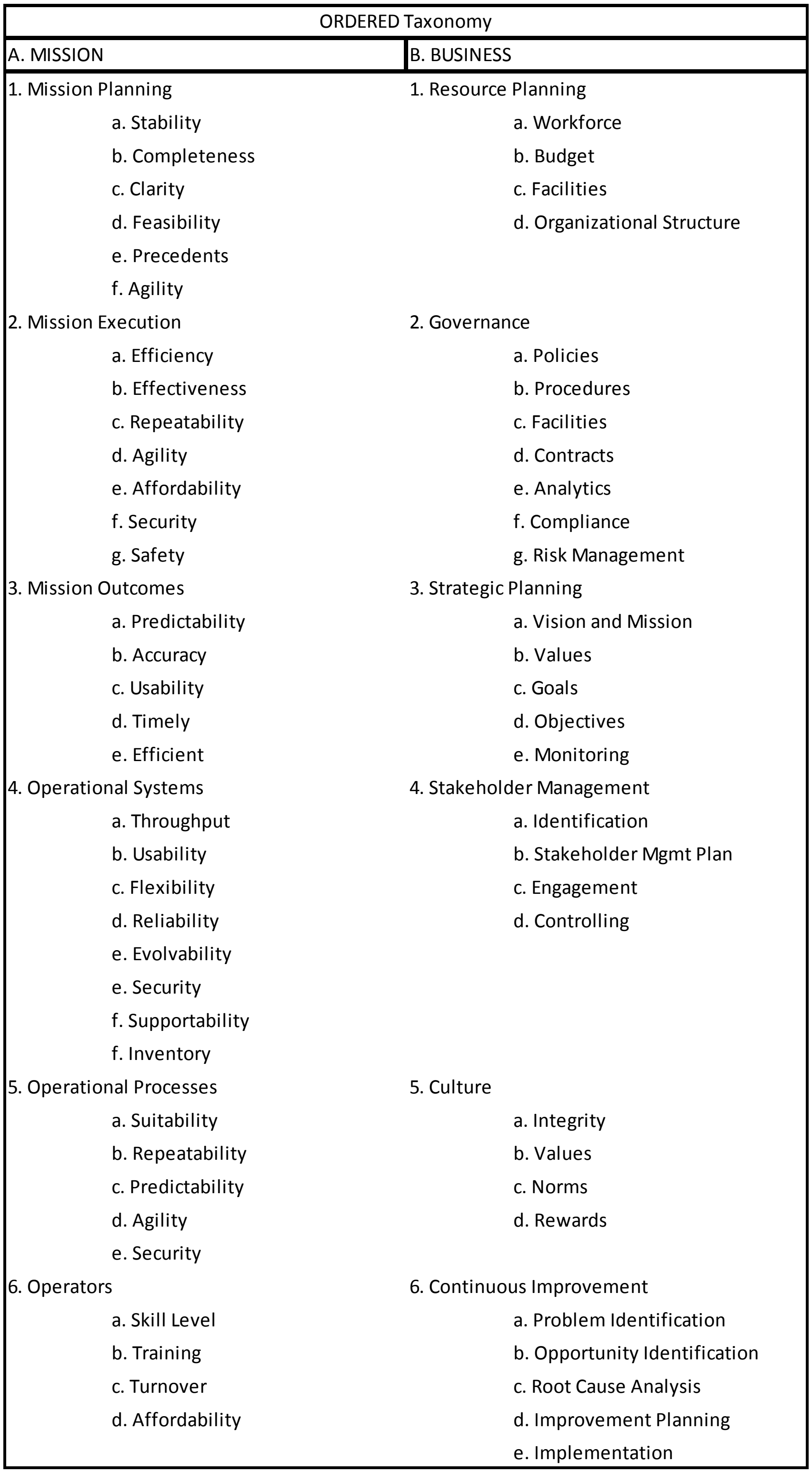
The ORDERED Taxonomy is shown in **Figure 3**. The taxonomy was developed and simplified by considering several source documents[11, 12, 13, 14] as well as personal experience.

The ORDERED taxonomy consists of two *categories*: Mission and Business. The next level of the taxonomy contains *elements* such as Mission Planning, Operational Systems, and Culture. The final level of the taxonomy consists of *attributes*.

Operational organizations use the taxonomy to help identify both mission-impacting concerns as well as business-impacting concerns. This allows a balance between short-term mission risks and longer-term business risks.

2.1.2. *Analyze Operational Risks*

Analyzing operational risk is the same as analyzing risk in a traditional process. Risk Exposure (RE) is the product of the probability (P) that the risk will occur and the impact (I) to



ORDERED Taxonomy	
A. MISSION	B. BUSINESS
1. Mission Planning	1. Resource Planning
a. Stability	a. Workforce
b. Completeness	b. Budget
c. Clarity	c. Facilities
d. Feasibility	d. Organizational Structure
e. Precedents	
f. Agility	
2. Mission Execution	2. Governance
a. Efficiency	a. Policies
b. Effectiveness	b. Procedures
c. Repeatability	c. Facilities
d. Agility	d. Contracts
e. Affordability	e. Analytics
f. Security	f. Compliance
g. Safety	g. Risk Management
3. Mission Outcomes	3. Strategic Planning
a. Predictability	a. Vision and Mission
b. Accuracy	b. Values
c. Usability	c. Goals
d. Timely	d. Objectives
e. Efficient	e. Monitoring
4. Operational Systems	4. Stakeholder Management
a. Throughput	a. Identification
b. Usability	b. Stakeholder Mgmt Plan
c. Flexibility	c. Engagement
d. Reliability	d. Controlling
e. Evolvability	
e. Security	
f. Supportability	
f. Inventory	
5. Operational Processes	5. Culture
a. Suitability	a. Integrity
b. Repeatability	b. Values
c. Predictability	c. Norms
d. Agility	d. Rewards
e. Security	
6. Operators	6. Continuous Improvement
a. Skill Level	a. Problem Identification
b. Training	b. Opportunity Identification
c. Turnover	c. Root Cause Analysis
d. Affordability	d. Improvement Planning
	e. Implementation

Figure 3. The ORDERED Risk Taxonomy

the organization if the risk occurs: RE = P x I. The goal in determining risk exposure is to understand the relative criticality of a given risk in order to help decide which risks should be mitigated, in what order, and the number of resources that the organization is willing to expend on mitigation activities.

Determining risk exposure is not an exact science and relies on the best judgment of individuals. For this reason the ORDERED approach keeps this step simple.

The operational organization must decide how to assign a probability and impact score to each risk. ORDERED uses a simple 1 to 5 rating for probability, with 1 being the lowest probability of occurrence and 5 being the highest probability of occurrence.

While probability of occurrence becomes a simple determination of likelihood of the risk occurring based on best judgment, impact of occurrence must take into consideration the impact of the risk to the mission or business needs of the organization. Each operational organization will adjust the impact definitions to meet its needs.

Prioritizing risks provides decision-makers with the ability to allocate scarce resources to mitigate the most important risks to mission success. A simple risk matrix as shown in **Figure 4** allows for a quick visual for decision-makers when allocating resources to mitigate operational risk.

		Insignificant	Minor	Moderate	Major	Extreme
		1	2	3	4	5
Almost Certain	5	🟨	🟨	🟥	🟥	🟥
Likely	4	🟩	🟨 RISK001 RISK005	🟨	🟥 RISK003 RISK004	🟥
Moderate	3	🟩	🟨	🟨	🟨	🟥
Unlikely	2	🟩	🟩	🟨 RISK002	🟨	🟥
Rare	1	🟩	🟩	🟩	🟨	🟨

Figure 4. Risk Matrix

In this example, both RISK003 and RISK004 have a major impact on operations and are both likely to occur. Priority would be given to ensure that these two risks are mitigated by systems engineering activities and project design decisions.

2.1.3. *Identifying Operational Risk Attributes*

An operational risk attribute is a characteristic of the operational mission or business that will be judged negatively by stakeholders unless the operational risk is mitigated. The purpose of mapping operational risk attributes to risk statements is to further clarify operational concerns and to help when identifying mitigation actions.

A starting point in mapping operational risk attributes is the ORDERED risk taxonomy. The lowest level of the taxonomy contains attributes describing the aspect of risk associated with the elements and categories of the taxonomy. Additional attributes to explore include quality attributes as described in Attribute Driven Design[15] engineering approaches and the Method Framework for Engineering System Architectures[16].

In addition to understanding the attributes associated with the operational risk, additional insight into the actual concern is useful when determining mitigation actions. While it helps to understand that a given risk is associated with an ORDERED taxonomic element and attribute, the additional understanding from eliciting the area of concern from the individual or group who identified the risk provides more definitive focus.

For example, an operator may have identified the following risk: *Current systems were designed using nominal data loads; the system may not scale*. The risk could be mapped to the Operational Systems element and Throughput attribute of the taxonomy.

Simply knowing that Throughput is an attribute may not provide enough detail. The attribute concern in this example could be described as mission stress. The operator is specifically concerned about how the system will operate when the mission becomes much more intense and the system needs to operate effectively when additional source data are processed.

2.1.4. *Develop Scenarios*

Scenarios are simply expressions of real-world interactions. They may be formal, structured and verbose, or freer form and expressed simply[17]. The purpose of scenarios as used to influence engineering activities is to describe expected results of a system during development in terms of real-world behavior[18].

Scenarios describe how the system should behave under certain conditions when presented with certain stimuli[19]. Operational risk scenarios describe the unwanted behavior of the system that would cause mission or business impact to the operational organization. Similar to the concept of anti-patterns in systems and software engineering[20], operational risk scenarios describe undesirable outcomes that need to be mitigated as they increase operational risk.

The ORDERED method uses a simplified format to describe the risk scenario based on the Architecture Tradeoff Analysis Method[21]. The operational risk scenario should describe a source that provides a stimulus to a system or operational task, the environment or artifact effected by the stimulus, and the unwanted response or outcome.

Example operational risk scenarios are listed below:

1. *An operator requests fire suppression during a high intensity operation with degraded communications; and the request fails to transmit within five minutes.*
2. *A resource manager attempts to re-assign a military member while the member is relocating to a*

new assignment; and the system fails to locate the member.

The key difference between engineering scenarios and operational risk scenarios is that operational risk scenarios describe negative or unwanted behavior or outcomes while engineering scenarios describe expected behavior or outcomes.

2.1.5. *Influence Systems Engineering*

Informing systems engineering activities with operational risk scenarios becomes part of the project’s overall engineering activities. This is a continuous process of refining requirements, design and architectural decisions, implementation choices, testing approaches, and deployment strategies to mitigate operational risk so that the resulting behavior of the system, product, or capability avoids high priority operational risk scenarios.

Boehm recommends a requirements approach that includes emphasizing value-driven, shared-vision-driven, change-driven, and risk-driven activities[22]. Central to these approaches is exploration of operational scenarios describing intended behavior.

Risk-driven activities allow engineering leadership to apply resources to mitigate highest risks or to avoid performing activities that increase risk. The addition of operational risk scenarios to expected behavior scenarios allows engineers and operational users to explore behavior that they want the resulting system, product, or capability to help mitigate or avoid.

Informing architecture and design with operational risk scenarios is part of a larger architecture and design validation activity. Architecture is simply the highest level of design. It represents the first artifact that structures a system, component, or capability into its constituent physical or logical sub-parts. It also represents the first opportunity to ensure that the resulting design and implementation enables desired attributes and avoids undesirable attributes. The addition of operational risk scenarios during architectural development and validation allows architects and engineers to select or create architectural mechanisms and constructs to avoid operational risk.

Using operational risk scenarios to influence implementation decisions allows for more robust trade decisions whereby selected implementation details are chosen to mitigate operational risk. Testing approaches and deployment strategies influenced by the end-user's most critical operational risk scenarios are likely to improve operational acceptability of new systems, components, or capabilities.

2.2. *Operational Risk Survey*

The purpose of using operational risk scenarios to influence systems engineering activities is to improve project outcomes. That is, systems and services delivered to end-users that meet cost and schedule expectations, meet all desired quality attributes, and fulfill operational needs thus lowering operational risk.

The authors developed a survey instrument in an attempt to understand the relationship between operational risk considerations and project outcomes. Using a Likert scale consisting of *Not At All*, *A Little*, *Moderately*, *Considerably*, *To A Great Extent*, and *Unknown*, participants were asked to indicate how strongly they supported the statements shown in **Table 1.**

Operational risk considerations were defined as actively eliciting operational risk from end-users during the early solution development stages of a program as well as actively and continuously involving end-user perspectives during development to identify and mitigate evolving operational risk throughout the program lifecycle (Questions 6 and 8). Program performance was defined as meeting cost and schedule expectations,

Table 1. Risk Survey Questions

Question Number	**Question**
1	My project team has a documented risk management process.
2	My project team has an active risk register that reflects the team’s most critical current risks.
3	My project team has a robust, continuous risk

	identification process.
4	My project team actively mitigates the project's top risks.
5	The leadership above my project actively elicits risks and helps mitigate risks to my project.
6	My project team actively elicited operational risks and mission threats from customers and end-users during the capture phase.
7	My project team actively elicited quality attributes (responsiveness, adaptability, evolvability, agility, scalability, etc.) during the capture phase.
8	The customer actively participates with the project team during execution to identify and mitigate operational risk.
9	The customer actively participates with the project team during execution to prioritize quality attributes (responsiveness, adaptability, evolvability, agility, scalability, etc.) and evaluate the ability of the solution or service to satisfy critical quality attributes during development.
10	The customer interaction with the project team is positive.
11	My customer would say that the solution or service we deliver mitigates operational risk or mission threats.
12	My customer would say that the solution or service we deliver meets all critical quality attributes (affordability, agility, scalability, etc.).
13	The project team consistently meets all customer cost and schedule objectives.

delivering a system that satisfies the end-user's most critical quality attribute requirements, and delivering a system or service that mitigates operational risk (Questions 11, 12, and 13).

In addition, the survey attempted was designed to allow the conduct of analysis to understand the relationship between the existence of an effective risk management process on the program and program outcomes (Questions 1, 2, 3, and 4). Additional questions in the list were asked for purposes other than stated above.

The survey was administered to 104 project managers on October 14, 2015. The projects were classified as solution development, service delivery, and professional services as shown in **Figure 5**.

A solution development project is defined as a project where the team is responsible for developing and delivering a solution (typically a tangible product such as a software/hardware system) to a customer. A service delivery project is defined as a project where the team is responsible for developing and delivering a service to the customer and is expected to meet customer outcomes such as service level agreements. A professional services project is defined as a project where the project team is responsible for delivering

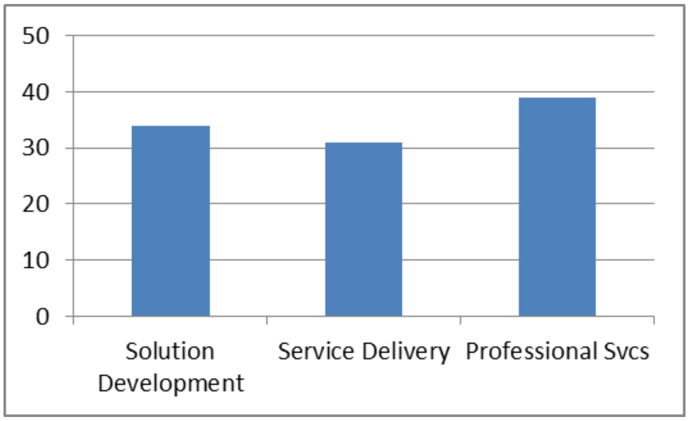


Figure 5. Project Type

qualified staff that provides expertise and works at the direction of the customer to support the customer's mission.

The projects ranged in size from small (under $5 million in annual revenue) to large (over $50 million in annual revenue) as shown in **Figure 6.**

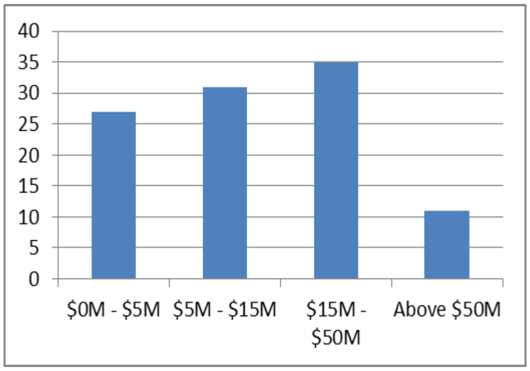


Figure 6. Project Revenue

The results were analyzed by first examining the variation in responses of the thirteen questions to determine if enough variation existed to allow further analysis. The analysis of the distribution of results shown in **Figure 7** indicates enough variation within and between questions to allow further analysis.

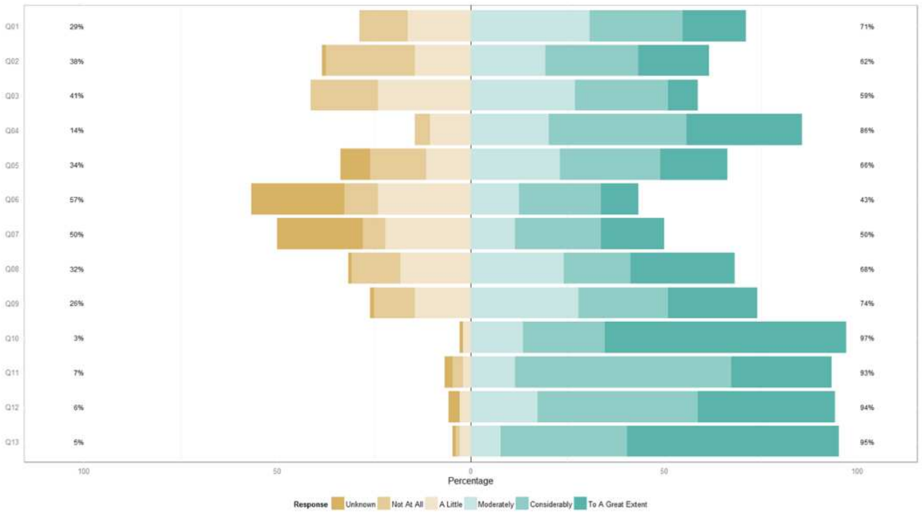


Figure 7. Likert Analysis

The two areas explored here are the relationship between the existence of an effective risk management process and project performance and the relationship between an operational risk focus and project performance. Questions 1, 2, 3, and 4 were combined to provide an aggregate score of risk process effectiveness. They measure the existence of a documented risk process, the use of a risk register, an active and continuous risk identification and mitigation process, and the project mitigating its most critical risks.

Questions 6 and 8 were combined to provide an aggregate score of operational risk effectiveness. They measure active elicitation of the customer's operational risks during the project's capture phase (where early lifecycle solution activities occur) and elicitation and mitigation of operational risk during project execution.

Questions 11, 12, and 13 were combined to provide an aggregate score of project performance. They measure the customer’s perspective of the project meeting cost and schedule objectives, mitigating their most critical operational risks, and delivering a service or solution that meets all expected quality attributes.

Each project’s aggregate measure for the three areas, risk process effectiveness, operational risk effectiveness, and project performance, were then divided into three categories indicating the lower third of effectiveness or performance, the middle third of effectiveness or performance, and the top third of effectiveness or performance. **Figure 8** shows the result of risk process capability compared to project performance.

Simply looking at the chart, one might conclude that projects with a more effective or capable risk process perform better than projects with an ineffective risk process. Fifty

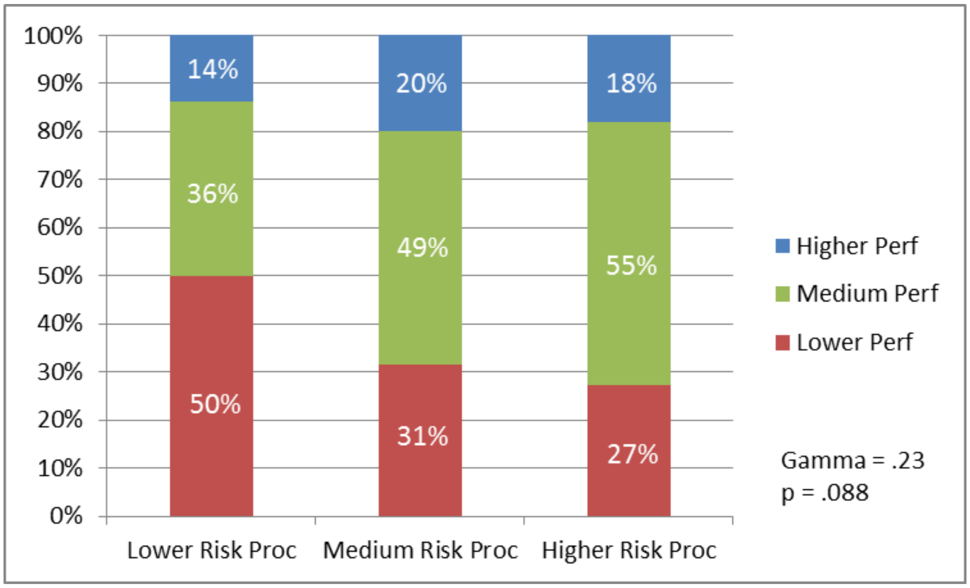


Figure 8. Risk Process Capability and Project Performance

percent of the projects with lower risk process capability exhibited lower project performance. That number decreased to 31 percent for projects with medium risk process capability and down to 27 percent for projects with higher risk process capability.

The number of projects exhibiting higher project performance across the low, medium, and high risk process capability stayed roughly the same, while the projects exhibiting medium project performance increased from 36 percent to 49 percent to 55 percent across the three groups. Performing ordinal logistic regression analysis of the data reveals a Gamma score of .23 and p-value of .088.

Gamma is a measure of association that expresses the strength of relationship between two ordinal variables[23]. Gamma values of less than 0.2 may be considered as weak, values around 0.3 may be thought of as moderately strong, values near 0.5 are considered strong, and values over 0.6 are very strong.

P-values measure the probability that the observed relationship in the sampled data occurs by chance alone. Values of $p < 0.05$ are used as a basis for rejecting the null hypothesis, that is having confidence that the relationship is not specious[24].

The Gamma score of .23 indicates a weak relationship between the two variables, and a high p-value of .088 decreases our confidence that the relationship observed is valid. In other words, it would be difficult to conclude with certainty using this data that projects with an effective risk process outperform projects with a less effective risk process.

Figure 9 shows the results of comparing the existence of an operational risk process capability and project outcomes.

Once again, simply looking at the chart, one might conclude that projects that focus on identifying and mitigating operational risk throughout their lifecycle perform better than projects that don’t focus on operational risk. The number of projects exhibiting lower project performance decreased from 50 percent for projects with low risk process capability to 36

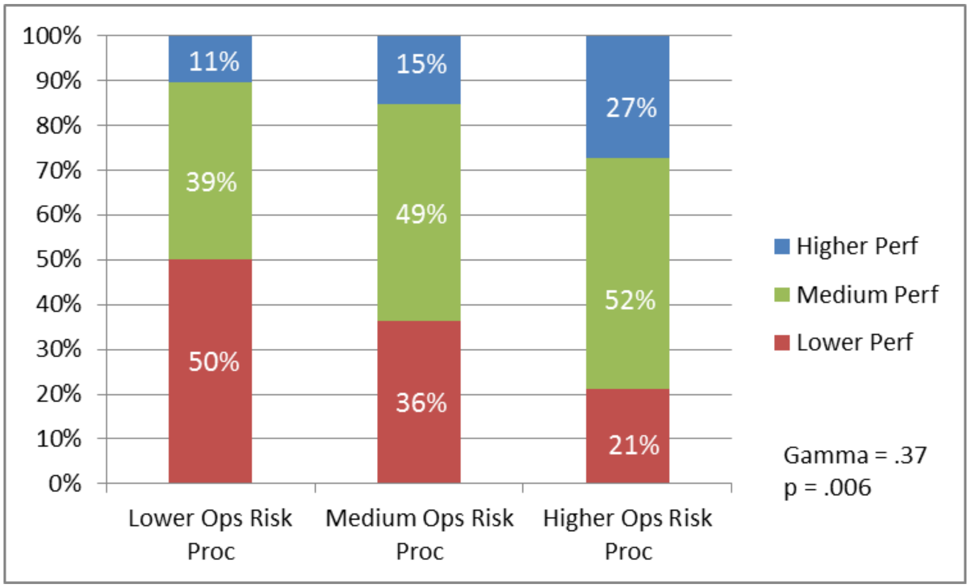


Figure 9. Operational Risk Process Capability and Project Performance

percent for projects with medium operational risk process capability down to 21 percent for projects with higher operational risk process capability.

Projects exhibiting medium project performance increased from 39 percent for projects with low operational process performance to 49 percent for projects with medium operational process performance and increasing to 52 percent for projects with higher operational risk process performance.

Projects exhibiting high project performance increased from 11 percent for projects with lower operational risk process performance to 15 percent for projects with medium operational risk process capability to 27 percent for projects with higher operational risk process capability. The Gamma score shows a moderately strong to strong positive relationship between the two variables, and the p-value of .006 provides confidence that the relationship is valid.

The caution here is that the ordinal logistic regression analysis performed provides only confidence that there is a correlation between an operational risk focus and project performance and an indication of the strength of that relationship. It does not provide a causal relationship. In other words, from the data alone, one cannot conclude that an operational risk focus causes project performance or that higher project performance causes higher operational risk process capability. One may only conclude that there is a positive correlation between the variables: they move in the same direction.

2.3. *Survey Conclusions*

Given the strength of the relationship and the low p-value, the authors are confident that projects within the sample that focus on operational risk during the project lifecycle also have better project performance than projects that focus less on operational risk during the project lifecycle.

Further analysis may provide additional insights. Project type or revenue (size) may influence the outcomes of the analysis. Larger projects may have a more formal risk process in place or may have lower project performance due to the inherently higher risk of larger projects. Solution development projects may have stronger risk practices in place versus professional services projects.

3. CONCLUSIONS AND FURTHER RESEARCH AREAS

Operational risk should drive systems engineering activities from concept development through deployment. The reason that a new system or capability is developed is to mitigate mission or business needs or threats. These needs and threats evolve over time, yet most engineering approaches ignore operational risk, allowing the chasm between the evolving need and the system under development to grow.

This paper described ORDERED, a repeatable approach designed to influence systems engineering activities through a continuous focus on operational risk. Using operational risk scenarios, developed through operational risk identification and analysis activities, ORDERED intends to increase the probability of project success. Adding operational opportunity scenarios to operational risk scenarios may enrich the approach further by eliciting opportunities to enhance mission effectiveness during the engineering lifecycle.

Many factors influence the success or failure of a development project. A structured focus on the evolving mission and business needs and threats of end-users aimed at explicitly driving requirements and informing engineering activities should improve the operational acceptability of the system, component, or capability under development. The results of this survey of 104 project managers indicate that an increased focus on operational risk during the project lifecycle correlates to better project performance outcomes.

Additional research on methods and tools to elicit and analyze operational risk as part of the systems engineering process is needed.

REFERENCES

1. Wiley, INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. 2015: Wiley.

2. Elm, J.P. and D.R. Goldenson, The Business Case for Systems Engineering Study: Results of the Systems Engineering Effectiveness Survey. 2012, DTIC Document.

3. Pyster, A., et al., Guide to the Systems Engineering Body of Knowledge (SEBoK), 2012.

4. Wrubel, E. and Jon Gross, Contracting for Agile Software Development in the Department of Defense: An Introduction (CMU/SEI-2015-TN-006). 2015, Retrieved August 22, 2015, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=442499.

5. Boehm, B. and J.A. Lane, Using the incremental commitment model to integrate system acquisition, systems engineering, and software engineering. CrossTalk, 2007. 19. (10): p. 4-9.

6. Ellis, R.F., R.D. Rogers, and B.M. Cochran, Joint Improvised Explosive Device Defeat Organization (JIEDDO): Tactical Successes Mired in Organizational Chaos; Roadblock in the Counter-IED Fight. 2007, DTIC Document.

7. Aronin, B.S., et al., Expeditionary Combat Support System: Root Cause Analysis. 2011, DTIC Document.

8. McCain, J. FLOOR REMARKS BY SENATOR JOHN MCCAIN ON THE AIR FORCE’S ECSS PROGRAM. 2014, Available from: http://www.mccain.senate.gov/public/index.cfm/2014/7/floor-remarks-by-senator-john-mccain-on-the-air-force-s-ecss-program.

9. Gallagher, B.P., Interpreting Capability Maturity Model Integration (CMMI) for Operational Organizations. 2002.

10. Air Force Instruction 90-1 102, Performance Management. 2000.

11. Gallagher, B.P., et al., A Taxonomy of Operational Risks. 2005.

12. Gallagher, B., et al., CMMI for Acquisition: Guidelines for Improving the Acquisition of Products and Services. 2011: Addison-Wesley Professional.

13. ISO, 31000: 2009 Risk management–Principles and guidelines, in International Organization for Standardization, Geneva, Switzerland. 2009.

14. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). 2013, Project Management Institute, Incorporated.

15. Wojcik, R., et al., Attribute-Driven Design (ADD), Version 2.0. 2006, DTIC Document.

16. Firesmith, D.G., et al., The method framework for engineering system architectures. 2008: CRC Press.

17. Sutcliffe, A. Scenario-based requirements engineering in Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International. 2003.

18. Mylopoulos, J., L. Chung, and E. Yu, From object-oriented to goal-oriented requirements analysis. Communications of the ACM, 1999. 42(1): p. 31-37.

19. Bass, L., Mark Klein, and Gabriel Moreno, Applicability of General Scenarios to the Architecture Tradeoff Analysis Method (CMU/SEI-2001-TR-014). 2001, Retrieved August 22, 2015, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=5637.

20. Brown, W.H., R.C. Malveau, and T.J. Mowbray, AntiPatterns: refactoring software, architectures, and projects in crisis. 1998.

21. Kazman, R., Mark Klein, and Paul Clements, ATAM: Method for Architecture Evaluation (CMU/SEI-2000-TR-004). 2000, Retrieved August 22, 2015, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=5177.

22. Selby, R.W., Software engineering: Barry W. Boehm's lifetime contributions to software development, management, and research. Vol. 69. 2007: John Wiley & Sons.

23. Freeman, L.C., Elementary applied statistics: for students in behavioral science. 1965: John Wiley & Sons.

24. Elm, J.P., et al., A Survey of Systems Engineering Effectiveness-Initial Results (with detailed survey response data). 2008, DTIC Document.

C.3 2016 INCOSE INTERNATIONAL SYMPOSIUM

INCREASING SYSTEMS ENGINEERING EFFECTIVENESS THROUGH OPERATIONAL RISK CONSIDERATIONS

Brian P. Gallagher
SVP, Operational Excellence
CACI International, Inc.
Colorado State University
703-841-4016
brian.gallagher@colostate.edu, bgallagher@caci.com

Dr. Ronald M. Sega
Director, Systems Engineering
Colorado State University
970-491-7067
ron.sega@colostate.edu

Dr. Kenneth Nidiffer
Director of Strategic Plans for Government Programs
Carnegie Mellon University, Software Engineering Institute
703-247-1387
nidiffer@sei.cmu.edu

Copyright © 2016 by Brian P. Gallagher.
Published and used by INCOSE with permission.

ABSTRACT

One measure of effectiveness of any given systems engineering practice is the ability of that practice to mitigate product or project risk. Product and project risk reduction is the focus of most risk management processes. When a project team has a robust risk management process, it continually identifies risks that may impact its ability to produce a product that meets requirements within cost and schedule constraints.

One missing aspect of most systems engineering risk management approaches is a focus on operational risk. That is, the evolving risk to business or mission needs of the end-user. This lack of focus on operational risk during the engineering process encourages the creation of a chasm between evolving need and delivered product capabilities. The longer the development process, the wider that gap, and the end-user becomes less receptive to deeming the capability operationally effective.

This research explores the use of operational risk identification and mitigation techniques during the systems engineering process and attempts to determine whether this increased focus would have a positive effect on systems engineering outcomes.

INTRODUCTION

Systems engineering is *an interdisciplinary approach and means to enable the realization of successful systems* (Wiley, 2015). The practices, approaches, methods, and tools of systems engineering have been codified over time and evolve as technology and system complexity increases. The purpose of having a set of proven practices for engineers to follow is to reduce system development risk and increase the probability of delivering a system that meets an operational need (Elm & Goldenson, 2012).

The tools applied to a given problem are selected based on an understanding of certain quality attributes of the product under development or the management aspects of the team producing the product within cost and schedule constraints. Therefore, a given practice is only viewed as effective if it reduces product or project risk or improves product or project outcomes at the same risk level.

Product-focused or technical risk is concerned with the technical performance and quality attributes of the end product. For example, a product may have stringent reliability requirements. Another product may have near real-time processing requirements. The systems engineering methods and tools for mitigating reliability risks may include using design patterns such as redundant hardware and software or fault detection and remediation mechanisms. Products with real-time requirements might use design patterns with the ability to ensure schedulability and analyze process behavior.

Project-focused or management risk is concerned with the management aspects of the development lifecycle. For example, if a project has multiple customers who are prone to having conflicting requirements, rapid-prototyping and user juries may be used as approaches to mitigate these stakeholder involvement risks. If the product is dependent on other components or products that are developed simultaneously, the project may select architectural patterns that separate concerns and allow independent evolution of components by separate teams or collaboration tools such as employing interface working groups or integrated product teams to mitigate the risk of the inter-operating systems having deployment issues.

One missing aspect of most systems engineering risk management processes such as those described in the Guide to the Systems Engineering Body of Knowledge (Pyster et al., 2012) or the INCOSE Systems Engineering Handbook (Wiley, 2015) is a focus on evolving operational risk during system development. Wrubel and Gross describe this disconnect, stating, ...*requirements for any given system are highly likely to evolve between the development of a system concept and the time at which the system* *is operationally deployed as new threats, vulnerabilities, technologies, and conditions emerge, and users adapt their understanding of their needs as system development progresses* (Wrubel, 2015).

Some projects attempt to manage this risk by selecting an evolutionary approach that allows for an incremental commitment to design decisions and incorporates *off-ramps* and *on-ramps* for technology or addition of new requirements due to changes in mission need (Boehm and Lane, 2007).

These threats, vulnerabilities, and technology changes could effect operational risk. When the operational risk is great, end-users bypass the traditional engineering process and create more streamlined avenues to acquire capability.

During Operation Iraqi Freedom, the United States Army faced a new and evolving threat. Enemy forces were no match for a traditional military, so they relied on asymmetric tactics. Improvised Explosive Devices became the weapon of choice because they were easy to build and deploy and were highly effective. The Army wasn’t prepared either in terms of detection and defeat systems or from a psychological perspective.

Coupled with an acquisition process that was slow to react to the evolving operational threat and outcry from both service members and the general population, the Army created the Joint Improvised Explosive Device Defeat Organization (JIEDDO) with the sole purpose of defeating this new operational risk. JIEDDO, recently renamed the Joint Improvised-Threat Defeat Agency, was able to bypass the Army's acquisition process and get equipment and capabilities to field quickly.

From a tactical perspective, the focus on defeating a specific operational risk was successful. Capabilities were fielded, and lives were saved. From a strategic perspective, these quickly-fielded systems lack certain quality attributes such as robustness, evolvability, and maintainability that would have been considered in a traditional systems engineering approach. The resulting quickly-fielded capabilities increased total cost of ownership and logistical complexity (Ellis, Rogers, & Cochran, 2007).

When system requirements are created to solely reduce strategic risk such as affordability or other long-term efficiencies, the resulting systems could be less relevant from a tactical or operational perspective. The driving requirements are associated with cost reduction, reducing redundant systems, or integrating capabilities rather than mitigating near-term operational risk.

The Air Force's Expeditionary Combat Support System had only a vague set of objectives when it began development in 2004 (Aronin et al., 2011). According to a report by the United States Senate Permanent Subcommittee on Investigations, these objectives resulted in ...*a new, fully-integrated logistics system that would replace an unspecified number of older, unconnected logistics systems*.

This lack of clarity and disconnect between solving critical operational threats and risks resulted in $1.1 billion in wasted funding and a system that was not deployable. According to Senator John McCain, (R-Arizona), *The Air Force's Expeditionary Combat Support System, or E.C.S.S., is a prime example of how a system designed to save money can actually waste billions of taxpayer dollars without producing any usable capability* (McCain, 2014). This research explores the use of operational risk identification and mitigation techniques during the systems engineering process and attempts to determine whether this increased focus would have a positive effect on systems engineering outcomes.

OPERATIONAL RISK

Operational risk is defined simply as the possibility of suffering mission or business loss. Mission loss in terms of less effective mission accomplishment or complete failure to accomplish mission objectives. Business loss in terms of economic affordability or long-term viability of performing the mission.

An operational organization is any group of individuals teamed together with a common purpose to carry out a mission. A mission is comprised of a specific task or set of tasks carried out by operational personnel (Gallagher, 2002).

Tasks may be described as either mission-essential or mission-support (*Air Force Instruction 90-1 102, Performance Management*, 2000). Mission-essential tasks directly contribute to mission execution. For example, if the operational organization was a community fire department, mission-essential tasks could include emergency response, firefighting, and rescue tasks. Mission-support tasks could include equipment maintenance, training, and fire prevention awareness.

Mission risks would be driven by any number of conditions such as events, activities, processes, and systems that could impact the operational organization’s ability to perform its mission or could negatively impact the full accomplishment of the mission. The impact is tactical in that the mission is impacted directly.

Business risks are also driven by similar conditions, but the impact is more strategic. A flat-tire on a fire truck is a risk to performing the mission task of fighting fires, and therefore, may be described as a mission risk. A lower tax-base in a community may impact the fire department’s ability to perform preventive maintenance or hire and train future firefighters, and therefore, could be described as a business risk. This distinction is valuable when identifying operational risk.

When a focus is solely on immediate mission risks, longer-term considerations such as affordability or long-term viability of the organization are ignored. When the focus is solely on business risks, mitigation actions or system solutions may not be operationally effective in the short-term. The balance between mission and business considerations helps ensure that solutions and mitigation actions are both operationally relevant and support the strategic needs of the organization.

OPERATIONAL RISK SURVEY

The authors developed a survey instrument in an attempt to understand the relationship between operational risk considerations and project outcomes. Using a Likert scale consisting of *Not At All*, *A Little*, *Moderately*, *Considerably*, *To A Great Extent*, and *Unknown*, participants were asked to indicate how strongly they supported the statements shown in **Table 1**.

Operational risk considerations were defined as actively eliciting operational risk from end-user during the early solution development stages of a program as well as actively and continuously involving end-user perspectives during development to identify and mitigate evolving operational risk throughout the program lifecycle (Questions 6 and 8).

Program performance was defined as meeting cost and schedule expectations, delivering a system that satisfies the end-user's most critical quality attribute requirements, and delivering a system or service that mitigates operational risk (Questions 11, 12, and 13). In addition, the survey attempted to understand the relationship between the existence of an effective risk management process on the program and program outcomes (Questions 1, 2, 3, and 4). Additional questions in the list were asked for purposes other than stated above.

Table 1. Risk Survey Questions

Question Number	Question
1	My project team has a documented risk management process.
2	My project team has an active risk register that reflects the team's most critical current risks.
3	My project team has a robust, continuous risk identification process.
4	My project team actively mitigates the project's top risks.
5	The leadership above my project actively elicits risks and helps mitigate risks to my project.
6	My project team actively elicited operational risks and mission threats from customers and end-users during the capture phase.
7	My project team actively elicited quality attributes (responsiveness, adaptability, evolvability, agility,

	scalability, etc.) during the capture phase.
8	The customer actively participates with the project team during execution to identify and mitigate operational risk.
9	The customer actively participates with the project team during execution to prioritize quality attributes (responsiveness, adaptability, evolvability, agility, scalability, etc.) and evaluate the ability of the solution or service to satisfy critical quality attributes during development.
10	The customer interaction with the project team is positive.
11	My customer would say that the solution or service we deliver mitigates operational risk or mission threats.
12	My customer would say that the solution or service we deliver meets all critical quality attributes (affordability, agility, scalability, etc.).
13	The project team consistently meets all customer cost and schedule objectives.

PRELIMINARY FINDINGS

The survey was administered to 104 project managers on October 14, 2015. The projects were classified as solution development, service delivery, and professional services as shown in **Figure 1.**

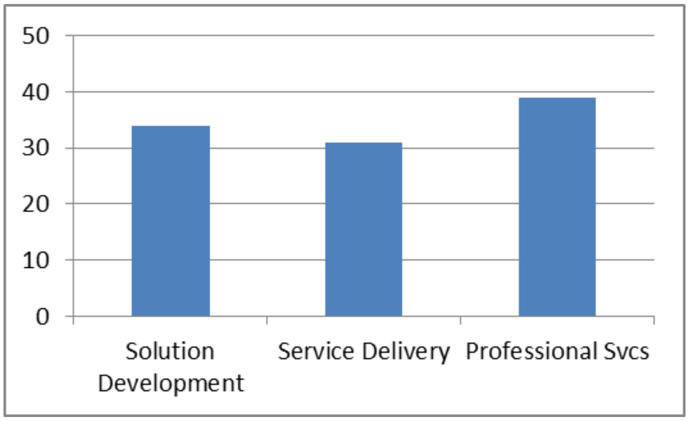


Figure 1. Project Type

A solution development project is defined as a project where the team is responsible for developing and delivering a solution (typically a tangible product such as a software/hardware system) to a customer. A service delivery project is defined as a project where the team is responsible for developing and delivering a service to the customer and is expected to meet customer outcomes such as service level agreements. A professional services project is defined as a project where the project team is responsible for delivering

qualified staff that provides expertise and works at the direction of the customer to support the customer's mission.

The projects ranged in size from small (under $5 million in annual revenue) to large (over $50 million in annual revenue) as shown in **Figure 2.**

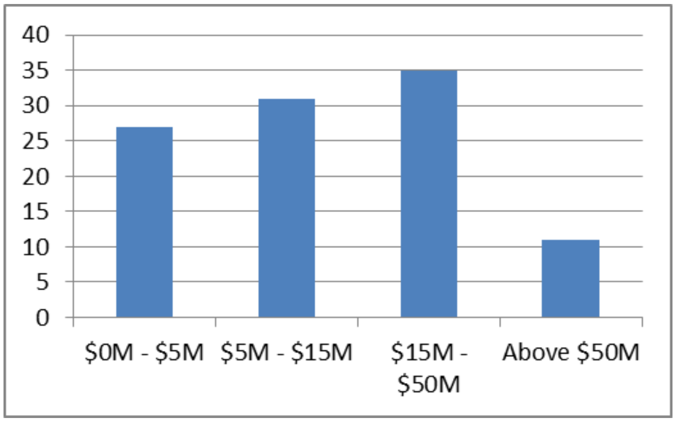


Figure 2. Project Revenue

The results were analyzed by first examining the variation in responses of the thirteen questions to determine if enough variation existed to allow further analysis. The analysis of the distribution of results shown in **Figure 3** indicates enough variation within and between questions to allow further analysis.

The two areas explored here are the relationship between the existence of an effective risk management process and project performance and the relationship between an operational risk focus and project performance. Questions 1, 2, 3, and 4

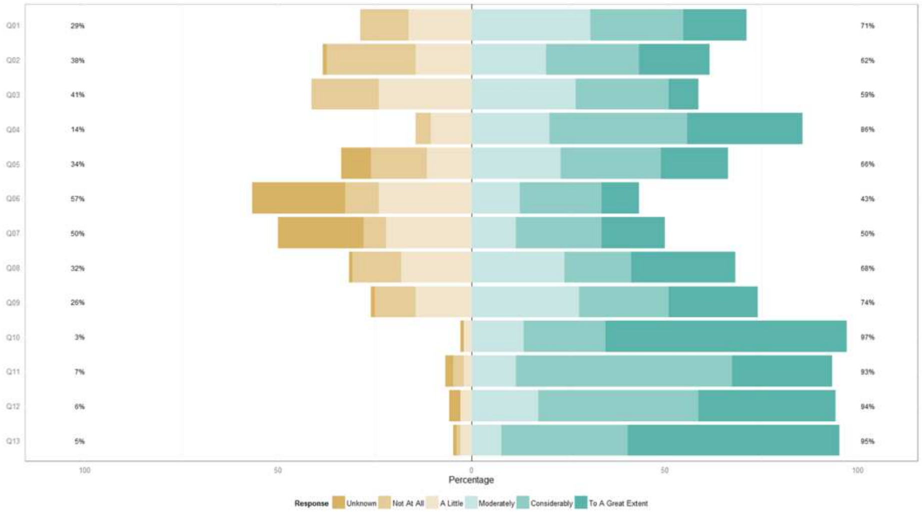


Figure 3. Likert Analysis

were combined to provide an aggregate score of risk process effectiveness. They measure the existence of a documented risk process, the use of a risk register, an active and continuous risk identification and mitigation process, and the project mitigating its most critical risks.

Questions 6 and 8 were combined to provide an aggregate score of operational risk effectiveness. They measure active elicitation of the customer's operational risks during the project's capture phase (where early lifecycle solution activities occur) and elicitation and mitigation of operational risk during project execution.

Questions 11, 12, and 13 were combined to provide an aggregate score of project performance. They measure the customer's perspective of the project meeting cost and schedule objectives, mitigating their most critical operational risks, and delivering a service or solution that meets all expected quality attributes.

Each project's aggregate measure for the three areas, risk process effectiveness, operational risk effectiveness, and project performance, were then divided into three categories indicating the lower third of effectiveness or performance, the middle third of effectiveness or performance, and the top third of effectiveness or performance. **Figure 4** shows the result of risk process capability compared to project performance.

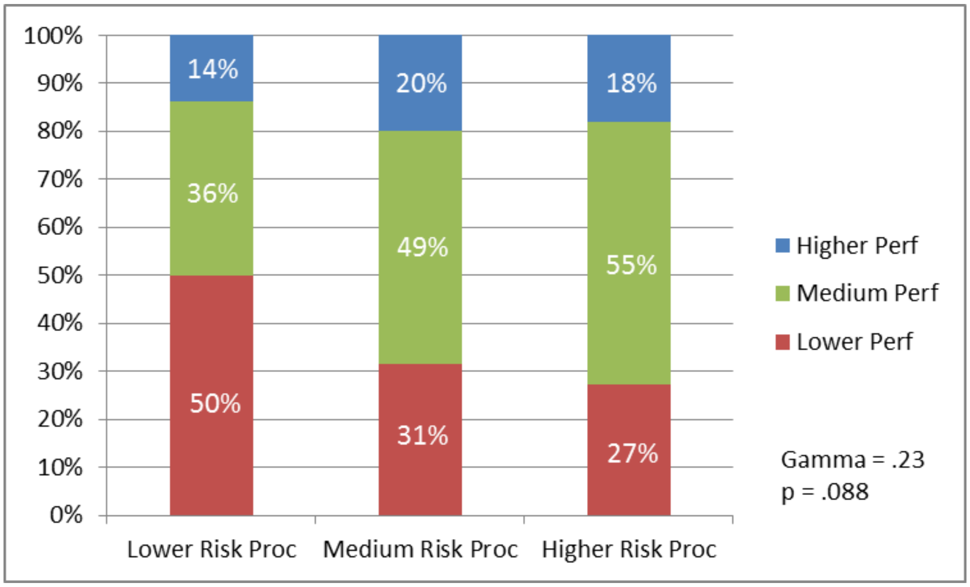


Figure 4. Risk Process Capability and Project Performance

Simply looking at the chart, one might conclude that projects with a more effective or capable risk process perform better than projects with an ineffective risk process. Fifty percent of the projects with lower risk process capability exhibited lower project performance. That number decreased to 31 percent for projects with medium risk process capability and down to 27 percent for projects with higher risk process capability.

The number of projects exhibiting higher project performance across the low, medium, and high risk process capability stayed roughly the same, while the projects exhibiting medium project performance increased from 36 percent to 49 percent to 55 percent across the three groups.

Performing ordinal logistic regression analysis of the data reveals a Gamma score of .23 and p-value of .088. Gamma is a measure of association that expresses the strength of relationship between two ordinal variables (Freeman, 1965). Gamma values of less than 0.2 may be considered as weak, values around 0.3 may be thought of as moderately strong, values near 0.5 are considered strong, and values over 0.6 are very strong.

P-values measure the probability that the observed relationship in the sampled data occurs by chance alone. Values of $p < 0.05$ are used as a basis for rejecting the null hypothesis, that is having confidence that the relationship is not specious (Elm, Goldenson, Emam, Donatelli, & Neisa, 2008). The Gamma score of .23 indicates a weak relationship between the two variables, and a high p-value of .088 decreases our confidence that the relationship observed is valid. In other words, it would be difficult to conclude with certainty using this data that projects with an effective risk process outperform projects with a less effective risk process.

Figure 5 shows the results of comparing the existence of an operational risk process capability and project outcomes.

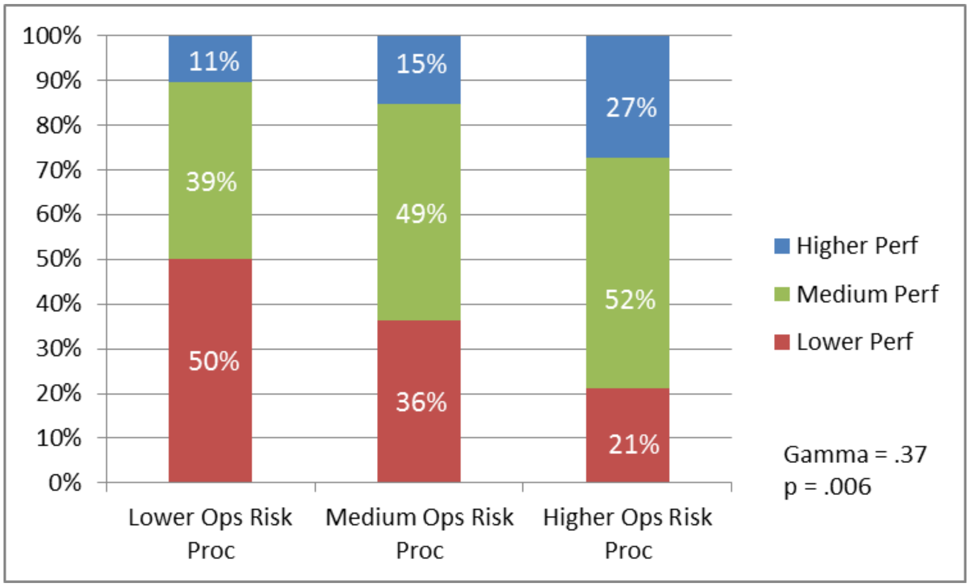


Figure 5. Operational Risk Process Capability and Project Performance

Once again, simply looking at the chart, one might conclude that projects that focus on identifying and mitigating operational risk throughout their lifecycle perform better than projects that don't focus on operational risk. The number of projects exhibiting lower project performance decreased from 50 percent for projects with low risk process capability to 36 percent for projects with medium operational risk process capability down to 21 percent for projects with higher operational risk process capability.

Projects exhibiting medium project performance increased from 39 percent for projects with low operational process performance to 49 percent for projects with medium operational process performance and increasing to 52 percent for projects with higher operational risk process performance. Projects exhibiting high project performance increased from 11 percent for projects with lower operational risk process performance to 15 percent for projects with medium operational risk process capability to 27 percent for projects with higher operational risk process capability.

The Gamma score shows a moderately strong to strong positive relationship between the two variables, and the p-value of .006 provides confidence that the relationship is valid.

The caution here is that the ordinal logistic regression analysis performed provides only confidence that there is a correlation between an operational risk focus and project performance and an indication of the strength of that relationship. It does not provide a causal relationship. In other words, from the data alone, one cannot conclude that an operational risk focus causes project performance or that higher project performance causes higher operational risk process capability. One may only conclude that there is a positive correlation between the variables: they move in the same direction.

SURVEY CONCLUSIONS

Given the strength of the relationship and the low p-value, the authors are confident that projects within the sample that focus on operational risk during the project lifecycle also have better project performance than projects that focus less on operational risk during the project lifecycle.

Further analysis may provide additional insights. Project type or revenue (size) may influence the outcomes of the analysis. Larger projects may have a more formal risk process in place or may have lower project performance due to the inherently higher risk of larger projects. Solution development projects may have stronger risk practices in place versus professional services projects.

CONCLUSIONS AND FURTHER RESEARCH AREAS

Operational risk should drive systems engineering activities from concept development through deployment. The reason that a new system or capability is developed is to mitigate some mission or business need or threat. These needs and threats evolve over time, yet most engineering approaches ignore operational risk, allowing the chasm between the evolving need and the system under development to grow.

Many factors influence the success or failure of a development project. A structured focus on the evolving mission and business needs and threats of end-users aimed at explicitly driving requirements and informing engineering activities should improve the operational acceptability of the system, component, or capability under development. The results of this survey of 104 project managers indicate that an increased focus on operational risk during the project lifecycle correlates to better project performance outcomes.

Additional research on methods and tools to elicit and analyze operational risk as part of the systems engineering process is needed.

REFERENCES

Air Force Instruction 90-1 102, Performance Management (Air Force Instruction 90-1 102). (2000).

Aronin, B. S., Bailey, J. W., Byun, J. S., Davis, G. A., Wolfe, C. L., Frazier, T. P., & Bronson, P. F. (2011). *Expeditionary Combat Support System: Root Cause Analysis*.

Boehm, B. & Lane, J. A. (2007). Using the incremental commitment model to integrate system acquisition, systems engineering, and software engineering. *CrossTalk, 19* (10), 4-9.

Ellis, R. F., Rogers, R. D., & Cochran, B. M. (2007). *Joint Improvised Explosive Device Defeat Organization (JIEDDO): Tactical Successes Mired in Organizational Chaos; Roadblock in the Counter-IED Fight*.

Elm, J. P. & Goldenson, D. R. (2012). *The Business Case for Systems Engineering Study: Results of the Systems Engineering Effectiveness Survey*.

Elm, J. P., Goldenson, D. R., Emam, K. E., Donatelli, N., & Neisa, A. (2008). *A Survey of Systems Engineering Effectiveness-Initial Results (with detailed survey response data)*.

Freeman, L. C. (1965). *Elementary applied statistics: for students in behavioral science*: John Wiley & Sons.

Gallagher, B. P. (2002). Interpreting Capability Maturity Model Integration (CMMI) for Operational Organizations.

McCain, J. (2014). FLOOR REMARKS BY SENATOR JOHN MCCAIN ON THE AIR FORCE'S ECSS PROGRAM. Retrieved from http://www.mccain.senate.gov/public/index.cfm/2014/7/floor-remarks-by-senator-john-mccain-on-the-air-force-s-ecss-program.

Pyster, A., Olwell, D. H., Hutchison, N., Enck, S., Anthony Jr, J. F., & Henry, D. (2012). Guide to the Systems Engineering Body of Knowledge (SEBoK) v. 1.0. 1. *Guide to the Systems Engineering Body of Knowledge (SEBoK)*.

Wiley. (2015). *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*: Wiley.

Wrubel, E., & Gross, Jon. (2015). *Contracting for Agile Software Development in the Department of Defense: An Introduction (CMU/SEI-2015-TN-006)*.