Risk Management

Consider a broad range of conditions and events that can affect the potential for success, and it becomes easier to strategically allocate limited resources where and when they are needed the most

Software Engineering Institute | Carnegie Mellon University

Overview

The SEI has been conducting research and development in various aspects of risk management for more than 20 years. Over that time span, many solutions have been developed, tested, and released into the community. In the early years, we developed and conducted Software Risk Evaluations (SREs), using the Risk Taxonomy. The tactical Continuous Risk Management (CRM) approach to managing project risk followed, which is still in use today—more than 15 years after it was released. Other applications of risk management principles have been developed, including CURE (focused on COTS usage), ATAM® (with a focus on architecture), and the cyber-security-focused OCTAVE.® In 2006, the SEI Mission Success in Complex Environments (MSCE) project was chartered to develop practical and innovative methods, tools, and techniques for measuring, assessing, and managing mission risks. At the heart of this work is the Mission Risk Diagnostic (MRD), which employs a top-down analysis of mission risk.

Mission risk analysis provides a holistic view of the risk to an interactively complex, socio-technical system. The first step in this type of risk analysis is to establish the objectives that must be achieved. The objectives define the desired outcome, or "picture of success," for a system. Next, systemic factors that have a strong influence on the outcome (i.e., whether or not the objectives will be achieved) are identified. These systemic factors, called drivers, are important because they define a small set of factors that can be used to assess a system's performance and gauge whether it is on track to achieve its key objectives. The drivers are then analyzed, which enables decision makers to gauge the overall risk to the system's mission.

The MRD has proven to be effective for establishing confidence in the characteristics of software-reliant systems across the life cycle and supply chain. The SEI has the MRD in a variety of domains, including software acquisition and development; secure software development; cybersecurity incident management; and technology portfolio management. The MRD has also been blended with other SEI products to provide unique solutions to customer needs.

Although most programs and organizations use risk management when developing and operating software-reliant systems, preventable failures continue to occur at an alarming rate. In many instances, the root causes of these preventable failures can be traced to weaknesses in the risk management practices employed by those programs and organizations. For this reason, risk management research at the SEI continues. The SEI provides a wide range of risk management solutions. Many of the older SEI methodologies are still successfully used today and can provide benefits to your programs.

The MSCE work on mission risk analysis—top-down, systemic analyses of risk in relation to a system's mission and objectives—is better suited to managing mission risk in complex, distributed environments. These newer solutions can be used to manage mission risk across the lifecycle and supply chain, enabling decision makers to more efficiently engage in the risk management process, navigate through a broad tradeoff space (including performance, reliability, safety, and security considerations, among others), and strategically allocate their limited resources when and where they are needed the most.

Finally, the SEI’s CERT Division is using the MRD to assess software security risk across the lifecycle and supply chain. As part of this work, CERT is conducting research into risk-based measurement and analysis, where the MRD is being used to direct an organization’s measurement and analysis efforts.

Getting Started

Every program or organization conducts risk management on some level, no matter how large or small they are. Whether you are acquiring, developing and operating software-intensive systems or systems of systems, the risk management approach you use is integral to success. Even though most programs and organizations implement some type of risk management approach preventable failures continue to occur because of:

- Uneven and inconsistent application of risk-management practice
- Significant gaps in risk-management practice
- Ineffective integration of risk-management practice
- Increasingly complex management environment

Our tools and methods can help you make a paradigm shift to a systemic approach to risk management. Or we can help you improve your current risk management approach.

Consulting

The SEI recognizes that although most programs and organizations implement some type of risk management approach, preventable failures continue to occur. In addition, many programs use risk management approaches that are bureaucratic, time-intensive, and consume valuable program resources. The SEI can work with you to

- conduct an expert-led independent risk assessment of your critical systems using the MRD
- teach you how to perform risk self-assessments using the MRD
- develop a customized risk assessment that meets your unique requirements
- develop risk models and simulations
- develop custom risk management solutions to help meet your software security needs

Our Practical Risk Management course is based on the Mission Risk Diagnostic and the Risk Management Framework, a requirements-based look at what a sound risk management practice should include.

Courses

- Practical Risk Management (PRM): Framework and Methods

Workshops

- Risk Management Improvement Workshops (using part or all of the PRM course)

Evaluation Services

- Mission Risk Diagnostic Evaluation: gain a comprehensive, high-level view of your project
- Risk Management Framework Evaluation: to help you identify gaps in your risk management practice

Blended Solutions

- MRD integrated with other SEI solutions for unique or complex issues

Tools and Methods: Current Solutions

Whether you are working in a systems-of-systems, multi-program, or single-program environment, our tools and methods can help you make a paradigm shift to a systemic approach to risk management. The foundation of this is mission risk analysis which is based on system theory. The underlying principle of system theory is to analyze a system as a whole rather than decomposing it into individual components and then analyzing each component separately. The goal of mission risk analysis is to identify a set of systemic factors that have a strong influence on the outcome (i.e., whether or not the objectives will be achieved). These systemic factors, or drivers, are important because they define a small set of factors that can be used to assess a system and determine whether it is on track to achieve its mission and objectives.

The Mission Risk Diagnostic (MRD) is a versatile method for assessing risk in interactively complex software-reliant systems that can be applied across the lifecycle (i.e., acquisition, development, operations) and supply chain. It analyzes a set of systemic risk factors to aggregate decision-making data and provides decision makers with a benchmark of a system's current state. The resulting gap between a system's current and desired states points to specific areas where additional investment is warranted. The MRD can be self-applied by the person or group that is responsible for managing a system or conducted by external parties on behalf of the responsible person or group.

The MRD defines the basic platform for performing mission risk assessment. Optional analyses can be added to the basic MRD platform as needed to assess mission risk in unique or specialized environments. For example, you can add analysis modules to the MRD platform to assess risk in system-of-system environments. Likewise, you can add a causal analysis to determine the root causes of mission risk.

The MRD is featured in a public course, Practical Risk Management, (which can also be taught onsite) as well as workshops that combine part or all of the course along with hands-on development and refinement of the methodology to suit a particular organization's needs. You can learn to do your own evaluations using MRD or have us perform an independent, third-party evaluation of your program.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

DM-0004429

About the SEI

For more than three decades, the Software Engineering Institute (SEI) has been helping government and industry organizations acquire, develop, operate, and sustain software systems that are innovative, affordable, enduring, and trustworthy. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and based at Carnegie University, a global research university annually rated among the best for its programs in computer science and engineering.

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412.268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu