Software Engineering Institute

Mission Risk Diagnostic (MRD) Method Description

Christopher Alberts
Audrey Dorofee

Carnegie Mellon

Table of Contents

List of Figures

List of Tables

Acknowledgments

Abstract

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. In particular, Carnegie Mellon® Software Engineering Institute (SEI) field experience indicates that programs and organizations throughout government and industry are unable to assess their risks effectively. For example, SEI independent assessments routinely uncover significant risks that have not been brought to the attention of key decision makers. When decision makers are unaware of significant risks, they are unable to take action to mitigate those risks. As a result, SEI researchers undertook a project to examine and improve the practice of risk assessment. The SEI has developed the Mission Risk Diagnostic (MRD) to assess risk in interactively complex, socio-technical systems across the life cycle and supply chain. To date, the SEI has employed the MRD in a variety of domains, including software acquisition and development, cybersecurity, software security, and business portfolio management. This technical note provides an overview of the MRD method.

1 Introduction

OCCURRENCE OF PREVENTABLE FAILURES

Although most programs and organizations use risk management when developing and operating software-reliant systems, preventable failures continue to occur at an alarming rate. Several reasons contribute to the occurrence of these failures, including

- significant gaps in the risk management practices employed by programs and organizations

- uneven and inconsistent application of risk management practices within and across organizations

- ineffective integration of risk management with program and organizational management

- increasingly complex management environment

INABILITY TO ASSESS RISK EFFECTIVELY

Over the past several years, Carnegie Mellon® Software Engineering Institute (SEI) field experience has yielded anecdotal evidence that programs and organizations throughout government and industry are unable to assess their risks effectively. For example, SEI independent assessments typically uncover significant risks that have not been brought to the attention of key decision makers within the programs and organizations that are being assessed. When decision makers are unaware of significant risks, they are unable to take action to mitigate those risks. As a result, SEI researchers undertook a project to examine and improve the practice of risk assessment. This technical note provides the results of that project by describing a systematic approach for assessing risk in interactively complex, socio-technical systems.

®   Carnegie Mellon is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

SEI BACKGROUND IN RISK MANAGEMENT

Since the early 1990s, the SEI has conducted research and development in the area of risk management and has applied risk management methods, tools, and techniques across the life cycle (including acquisition, development, and operations) and supply chain. In addition, past SEI research examined various types of risk, including software development risk [Dorofee 1996, Williams 1999, Alberts 2009], system acquisition risk [Gallagher 1999], operational risk [Gallagher 2005], mission risk [Alberts 2009] and information security risk [Alberts 2002], among others. In this technical note, SEI researchers have codified this experience in the form of a mission-based risk assessment.

MISSION RISK DIAGNOSTIC (MRD)

The SEI is developing the Mission Risk Diagnostic (MRD) to assess risk in interactively complex, socio-technical systems, such as projects, programs, and processes, across the life cycle and supply chain. The overarching goal of the MRD is to determine the extent to which a system is in position to achieve its mission and objective(s).

SEI field experience over the past several years has shown the MRD to be an efficient and effective means of analyzing risk in interactively complex systems. To date, the SEI has employed the MRD in a variety of domains, including software acquisition and development, cybersecurity, software security, and business portfolio management.

PURPOSE OF THIS DOCUMENT

The purpose of this technical note is to present an overview of the MRD method. However, this document does not provide step-by-step procedures for conducting the MRD. A guidebook that is focused on how to conduct the MRD is a candidate for future publication. In addition, domain-specific methods consistent with the MRD might also be considered for future publication.

INTENDED AUDIENCE

The primary audience for this technical note is people who are responsible for assessing and managing risk in development and operational settings. People who are interested in the following topics might also find this document useful:

- time- and resource-efficient methods for assessing and managing risk
- general project or program management

STRUCTURE OF THIS DOCUMENT

This technical note is divided into the following sections:

- *Section 1: Introduction*—provides a brief overview of the MRD and defines the audience for this document

- *Section 2: Risk Management Concepts*—presents background information about risk management

- *Section 3: Two Approaches for Analyzing Risk*—presents an overview of concepts underlying tactical risk analysis and mission risk analysis

- *Section 4: Mission Risk Diagnostic (MRD) Concepts*—describes the foundational concepts of the MRD method

- *Section 5: Mission Risk Diagnostic (MRD) Method*—provides an overview of the activities and tasks that must be completed when conducting the MRD method

- *Section 6: Summary*—presents a summary of key concepts introduced in the technical note

2   Risk Management Concepts

MULTIPLE CONTEXTS OF RISK MANAGEMENT

The term *risk* is used universally, but different audiences often attach different meanings to it [Kloman 1990]. In fact, the details about risk and how it supports decision making depend upon the context in which it is applied [Charette 1990]. For example, safety professionals view risk management in terms of reducing the number of accidents and injuries. A hospital administrator views risk as part of the organization's quality assurance program, while the insurance industry relies on risk management techniques when setting insurance rates. Each industry thus uses a definition that is uniquely tailored to its context. No universally accepted definition of risk exists.

THREE CONDITIONS OF RISK

Whereas specific definitions of risk might vary, a few characteristics are common to all definitions. For risk to exist in any circumstance, the following three conditions must be satisfied [Charette 1990]:

1.   The potential for loss must exist.
2.   Uncertainty with respect to the eventual outcome must be present.[1]
3.   Some choice or decision is required to deal with the uncertainty and potential for loss.

BASIC DEFINITION OF RISK

The three characteristics can be used to forge a very basic definition of the word *risk*. Most definitions focus on the first two conditions—loss and uncertainty—because they are the two measurable aspects of risk. Thus, the essence of risk, no matter what the domain, can be succinctly captured by the following definition: *Risk is the probability of suffering harm or loss.*[2]

---

[1]   Some researchers separate the concepts of certainty (the absence of doubt), risk (where the probabilities of alternative outcomes are known), and uncertainty (where the probabilities of possible outcomes are unknown). However, because uncertainty is a fundamental attribute of risk, this technical note does not differentiate between decision making under risk and decision making under uncertainty.

[2]   This definition is derived from the definition used in Dorofee [1996].

COMPONENTS OF RISK   Figure 1 illustrates the three components of risk:

- *potential event* – an act, occurrence, or happening that alters current conditions and leads to a loss
- *condition* – the current set of circumstances that leads to or enables risk
- *consequence* – the loss that results when a potential event occurs; the loss is measured in relation to the status quo (i.e., current state)

From the risk perspective, a condition is a passive element. It exposes an entity[3] (e.g., project, system) to the loss triggered by the occurrence of an event. However, by itself, a risk condition will *not* cause an entity to suffer a loss or experience an adverse consequence; it makes the entity *vulnerable* to the effects of an event [Alberts 2006].
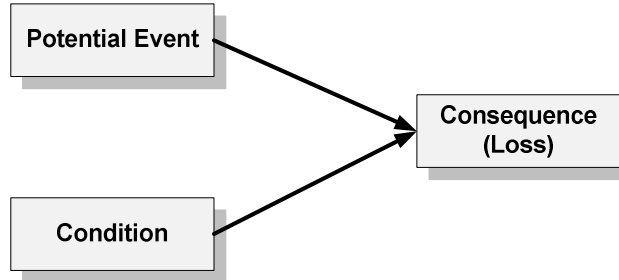
Figure 1:   Components of Risk

EXAMPLE: RISK   A project team is developing a software-reliant system for a customer. The team has enough people with the right skills to perform its tasks and complete its next milestone on time and within budget (status quo). However, the team does not have redundancy among team members' skills and abilities (condition). If the team loses people with certain key skills (potential event), then it will not be able to complete its assigned tasks (consequence/loss). This puts the next milestone in jeopardy, which is a loss when measured in relation to the status quo (on track to achieve the next milestone).

However, if none of the team members leaves or is reassigned (i.e., the event does not occur), then the project should suffer no adverse consequences. Here, the condition enables the event to produce an adverse consequence or loss.

---

[3]   An entity is the object that is affected by risk. The entities of interest in this technical note are interactively complex, software-reliant systems. Examples include projects, programs, business processes, and networked technologies.

REALIZED RISK: CHANGING THE CURRENT CONDITIONS

When a risk occurs, an adverse consequence (i.e., a loss) is realized. The ultimate effect of this consequence is to change the current set of conditions confronting the entity (i.e., project, system). In the previous example, a realized risk means that the project team has lost people and no longer has enough people to complete its assigned tasks. The project now faces a problem that must be resolved. Put another way, the risk has become a problem. (The concept of an issue/problem is addressed in more detail below.)

RISK MEASURES

Three measures are associated with a risk: (1) probability, (2) impact, and (3) risk exposure.[4] The basic relationships between probability and impact and the components of risk are shown in Figure 2.[5] In this context, *probability* is defined as a measure of the likelihood that an event will occur, while *impact* is defined as a measure of the loss that occurs when a risk is realized. *Risk exposure* provides a measure of the magnitude of a risk based on current values of probability and impact.

Probability

```
┌──────────────────┐
│ Potential Event  │────┐
└──────────────────┘    │          Impact
                        ▼    ┌──────────────────┐
                             │   Consequence    │
                        ▲    │     (Loss)       │
┌──────────────────┐    │    └──────────────────┘
│    Condition     │────┘
└──────────────────┘
```
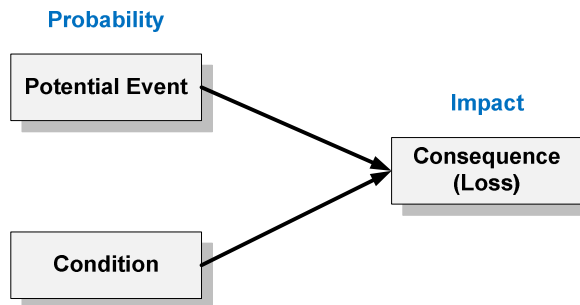
Figure 2:   *Risk Measures and the Components of Risk (Simplified View)*

---

4   A fourth measure, time frame, is sometimes used to measure the length of time before a risk is realized or the length of time in which action can be taken to prevent a risk.

5   The relationships between probability and impact and the components of risk depicted in Figure 2 are based on the simplifying assumption that the loss resulting from the occurrence of an event is known with certainty. In many cases, a range of adverse outcomes might be possible. For example, consider a project team that is worried about the consequence of losing team members. The magnitude of the loss will depend on a number of factors, such as which team member leaves the project, whether anyone is available to take the team member's place, the skills and experience of potential replacements, and so forth. The consequence could be minor if an experienced person is available to step in and contribute right away. On the other hand, the consequence could be severe if no one is available to step in and contribute. A range of probable outcomes is thus possible. When multiple outcomes are possible, probabilities are associated with the potential outcomes. As a result, risk analysts must consider two probabilities—one associated with the potential event and another associated with the consequence. However, basic risk assessments assume that the loss is known with relative certainty (or they only focus on the most likely consequence), and only the probability associated with the event is considered.

RISK MANAGEMENT

Risk management is a systematic approach for minimizing exposure to potential losses. It provides a disciplined environment for

- continuously assessing what could go wrong (i.e., assessing risks)
- determining which risks to address (i.e., setting mitigation priorities)
- implementing actions to address high-priority risks and bring those risks within tolerance

RISK MANAGEMENT ACTIVITIES

Figure 3 illustrates the three core risk management activities:

- **assess risk**—transform the concerns people have into distinct, tangible risks that are explicitly documented and analyzed
- **plan for controlling risk**—determine an approach for addressing each risk; produce a plan for implementing the approach
- **control risk**—deal with each risk by implementing its defined control plan and tracking the plan to completion
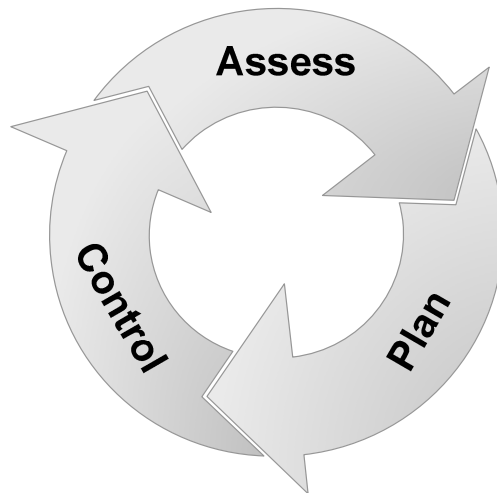
Figure 3:   Risk Management Activities

ISSUE/PROBLEM

One of the fundamental conditions of risk is uncertainty regarding its occurrence. A risk, by definition, might or might not occur. In contrast, an *issue*[6] (also referred to as a *problem*) is a condition that directly produces a loss or adverse consequence. With an issue, no uncertainty exists—the condition exists and is having a negative effect on performance.[7] Issues can also lead to (or contribute to) other risks by

- creating a circumstance that enables an event to trigger additional loss
- making an existing event more likely to occur
- aggravating the consequences of existing risks

COMPONENTS OF ISSUE/PROBLEM

Figure 4 illustrates the two components of an issue or problem:

- *condition* – the current set of circumstances that produces a loss or adverse consequence
- *consequence* – the loss that is triggered by an underlying condition that is present

From the issue perspective, a condition directly causes an entity (e.g., project, system) to suffer a loss or experience an adverse consequence. Unlike a risk, an issue does *not* need an event to occur to produce a loss or adverse consequence.
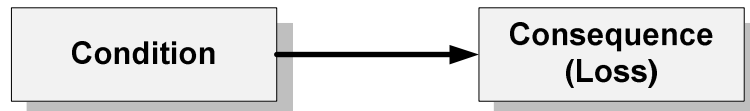
Figure 4:   Components of Issue/Problem

EXAMPLE: ISSUE/PROBLEM

A project team is developing a software-reliant system for a customer. The team does not have enough people with the right skills to perform the team's assigned tasks (condition). As a result, the team will not be able to complete all of its assigned tasks before the next milestone (consequence/loss). No event is required for the loss to occur, which distinguishes and issue/problem from a risk.

---

6   People do not always find it easy to distinguish between an issue and the future risk posed by that issue (if left uncorrected). This confusion can result in issues being documented in a risk database and being treated like risks (and vice versa). Management must take great care to ensure that their approaches for managing issues and risks are integrated appropriately and understood by both management and staff.

7   Many of the same tools and techniques can be applied to both issue and risk management.

OPPORTUNITY

Risk is focused on the potential for loss; it does not address the potential for gain. The concept of opportunity is focused on the potential for a positive outcome. An *opportunity* is the probability of realizing a gain. It thus enables an entity to improve its current situation relative to the status quo.

Very often, an opportunity is focused on the gain that could be realized from an allocation or reallocation of resources. It defines a set of circumstances that provides the potential for a desired gain and often requires an investment or action to realize that gain (i.e., to take advantage of the opportunity). Pursuit of an opportunity can produce new risks or issues, and it can also change existing risks or issues.

COMPONENTS OF OPPORTUNITY

Figure 5 illustrates the three components of opportunity:

- *potential event* – an act, occurrence, or happening that alters current conditions and leads to a gain
- *condition* – the current set of circumstances that produces opportunity
- *consequence* – the gain that will occur when a potential event occurs; the gain is measured in relation to the status quo (i.e., current state)

From the opportunity perspective, a condition is a passive element that creates the circumstances in which an event can lead to a positive outcome. By itself, a condition will *not* cause an entity to realize a gain or experience a positive consequence. However, the condition creates circumstances in which a gain is possible.
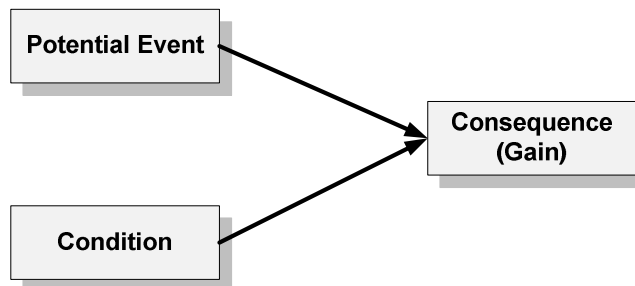
Figure 5: *Components of Opportunity*

EXAMPLE: OPPORTUNITY

A project team is developing a software-reliant system for a customer. Current status and quality reports indicate that the team is not on track to achieve its next milestone (status quo). Another project in the company has just delivered its product to its customer, and its team members will be made available to projects throughout the company (condition). If the project manager brings additional personnel who have the right knowledge, skills, and abilities onto the project (event), then the team might be able to increase its productivity and be in position to meet its next milestone (consequence/gain). Here, the gain is improved performance in relation to the status quo.

OPPORTUNITY: POTENTIAL TO TRIGGER ISSUES AND RISKS

It should be noted that adding people to the project could pose some downside issues and risks. People already working on the project will have to mentor the new people and bring them up to speed, which could lower productivity for a time. Also, the people who are available might not have the right mix of skills and experience needed by the project, which would not increase the team's productivity (or might actually lower productivity and make matters worse). The downside issues and risks associated with pursuing an opportunity must be considered when analyzing that opportunity.

STRENGTH

A *strength* is a condition that is driving an entity (e.g., project, system) toward a desired outcome. With a strength, no uncertainty exists—the condition exists and is having a positive effect on performance (i.e., driving an entity toward a desired outcome).

COMPONENTS OF STRENGTH

Figure 6 illustrates the two components of a strength:

- *condition* – the current set of circumstances that guide an entity toward a desired outcome (i.e., consequence)
- *consequence* – the desired outcome that is being pursued

Here, the condition directly helps an entity (e.g., project, system) move toward the desired outcome or result.
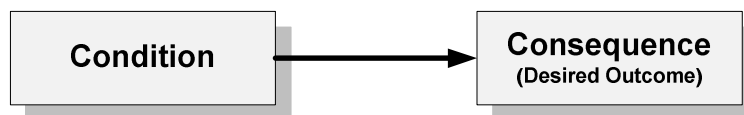
Figure 6:   Components of Strength

EXAMPLE: STRENGTH

A project team is developing a software-reliant system for a customer. The team has enough people with the right skills to perform the team's assigned tasks and has enough redundancy in skills needed to meet the next milestone (condition). Its people are its strength. As a result, the team is positioned to execute its tasks and activities effectively and efficiently, putting the project in position to achieve its next milestone.

CAUSAL CHAIN

The success or failure of an activity or endeavor is influenced by the range of circumstances that are present. Figure 7 depicts a causal chain of conditions and events[8] that affect whether an activity will achieve a desired set of objectives. This causal chain includes

- strengths that are driving the activity toward a successful outcome
- issues or problems that are driving the activity toward a failed outcome
- risks that could degrade performance and make a failed outcome more likely
- opportunities that could improve performance and make a successful outcome more likely

Figure 7:   *Causal Chain of Conditions, Events, and Consequences*

---

[8]   In the causal chain diagram, consequences are the effects that are triggered by conditions and events. A consequence represents a change to the current set of conditions. In other words, a consequence is viewed as a condition that is the product of other conditions and events. This is why the causal chain is referred to as "a causal chain of conditions and events" rather than a "causal chain of conditions, events, and consequences."

NAVIGATING THROUGH THE CAUSAL CHAIN

Effective risk management requires navigating through this causal chain, assessing the current potential for loss, and implementing strategies for minimizing the potential for loss. The next section builds on the concepts in this section by examining two fundamental approaches for analyzing risk.

3 Two Approaches for Analyzing Risk

GOAL OF THE MRD

The goal of the Mission Risk Diagnostic (MRD) is to analyze risk in interactively complex, software-reliant systems across the life cycle and supply chain. To fully appreciate what this statement means, one needs to understand the phrase, "interactively complex, software-reliant systems."

SOCIO-TECHNICAL SYSTEM

A *socio-technical system* is defined as interrelated technical and social elements that are engaged in goal-oriented behavior. Elements of a socio-technical system include the people who are organized in teams or departments to do their work tasks and the technologies on which people rely when performing work tasks. Projects, programs, and operational processes are all examples of socio-technical systems.

SOFTWARE-RELIANT SYSTEM

A *software-reliant system* is a socio-technical system whose behavior (e.g., functionality, performance, safety, security, interoperability, and so forth) is dependent on software in some significant way [Bergey 2009]. In the remainder of this document, when the word *system* is used, it refers to a software-reliant system.

INTERACTIVE COMPLEXITY

Interactive complexity refers to the presence of unplanned and unexpected sequences of events in a system that are either not visible or not immediately understood [Perrow 1999]. The components in an interactively complex system interact in relatively unconstrained ways. When a system is interactively complex, independent failures can interact with the system in ways that cannot be anticipated by the people who design and operate the system.

TWO TYPES OF RISK ANALYSIS

Two distinct risk analysis approaches can be used when evaluating systems [Leveson 2004]: [9]

1. tactical risk analysis
2. mission risk analysis

Both types of risk analysis are addressed in this section.

---

[9]   The discussion of tactical and mission risk analysis is adapted from Leveson [2004].

3.1 Tactical Risk Analysis

TACTICAL RISK

From the tactical perspective, risk is defined as the probability that an event will lead to a negative consequence or loss. Figure 7 shows the causal chain of conditions and events that was introduced in the previous section. As depicted in the figure below, tactical risk is focused on the risk that is triggered by an individual event.
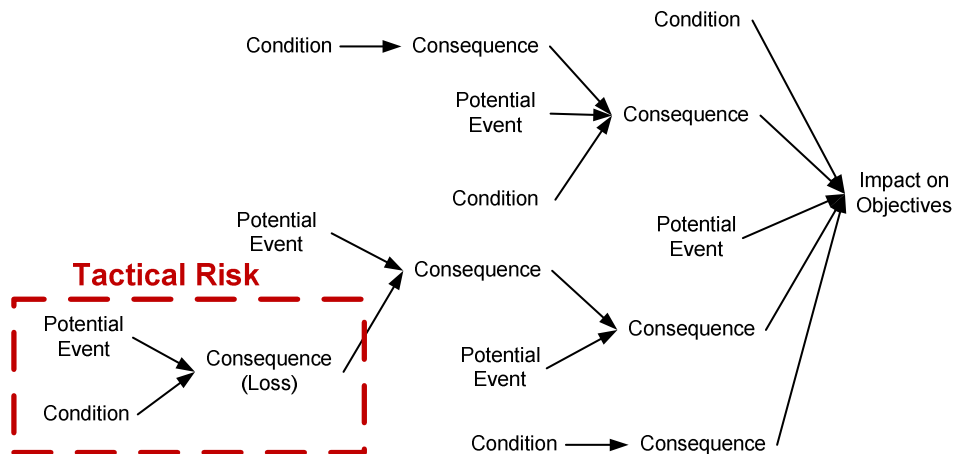
Figure 8: Tactical Risk

TACTICAL RISK ANALYSIS

The basic goal of tactical risk analysis is to evaluate a system's components for potential failures. Tactical risk analysis is based on the principle of system decomposition and component analysis. The first step of this approach is to decompose a system into its constituent components. The individual components are then prioritized, and a subset of components is designated as being critical. Next, the risks to each critical component are analyzed.

Tactical risk analysis enables stakeholders to (1) determine which components are most critical to a system and (2) analyze ways in which those critical components might fail (i.e., analyze the risk to critical components). Stakeholders can then implement effective controls designed to mitigate those potential failures. Because of its focus on preventing potential failures, tactical risk analysis has been applied extensively within the discipline of systems engineering.

LIMITATIONS OF TACTICAL RISK ANALYSIS

Analysts need to understand the limitations of using tactical risk analysis to evaluate interactively complex systems, which include the following:

- Only critical components are analyzed. Noncritical components are not examined, and interdependencies among components are not addressed.

- The selection of which conditions and events (i.e., sources or causes of risk) to consider is subjective.

- Nonlinear relationships among conditions and events (e.g., feedback) are not considered. Risk causal relationships are presumed to be simple, direct, and linear.

- Events that produce extreme or catastrophic consequences are difficult to predict because they can be triggered by the contemporaneous occurrences of multiple events, cascading consequences, and emergent system behaviors.

- Confidence in the performance of individual components does not establish confidence in the performance of the parent system.

A PARTIAL PICTURE OF RISK

When analysts attempt to decompose interactively complex systems, some system-wide behaviors become lost. It is very difficult to establish the relationship between the macro-level behavior of the system and the micro-level behavior of individual components. As a result, tactical risk analysis provides a partial picture of the risks to an interactively complex system. To get a more holistic view of risk in an interactively complex system, analysts need to employ an alternative analysis approach.

3.2 Mission Risk Analysis

MISSION RISK

From the mission perspective, risk is defined as the probability of mission failure (i.e., not achieving key objectives). *Mission risk* aggregates the effects of multiple conditions and events on a system's ability to achieve its mission.

AGGREGATING TACTICAL DATA

Because mission risk *aggregates* the effects of multiple conditions and events on system performance, it can be used to consolidate the following types of tactical data:

- strengths (i.e., positive conditions) that are driving the activity toward a successful outcome
- issues or problems that are driving the activity toward a failed outcome
- tactical risks (i.e., the risk triggered by a *single* event) that could degrade performance and make a failed outcome more likely
- tactical opportunities (i.e., the opportunity triggered by a *single* event) that could improve performance and make a successful outcome more likely

MISSION RISK ANALYSIS

Mission risk analysis is based on system theory.[10] The underlying principle of system theory is to analyze a system as a whole rather than decompose it into individual components and then analyze each component separately [Leveson 2004]. In fact, some properties of a system are best analyzed by considering the entire system, including

- influences of environmental factors
- feedback and nonlinearity among causal factors
- systemic causes of failure (as opposed to proximate causes)
- emergent properties

CONDUCTING MISSION RISK ANALYSIS

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* in this technical note, 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.

---

10   Because mission risk analysis is based on system theory, the term *systemic risk* can be used synonymously with *mission risk*. The term *mission risk* is used throughout this document.

MISSION RISK WITHIN THE CAUSAL CHAIN

Figure 9 illustrates how mission risk is viewed in the context of the causal chain of conditions and events. A driver is a construct that is used to aggregate the effects of multiple conditions and events in order to determine their combined influence on the mission's key objectives. Each driver *directly* influences whether or not objectives will be achieved. The conditions and events within the causal chain are considered to be the root causes of mission risk. Section 4 provides a detailed overview of drivers and how to use them when analyzing mission risk.
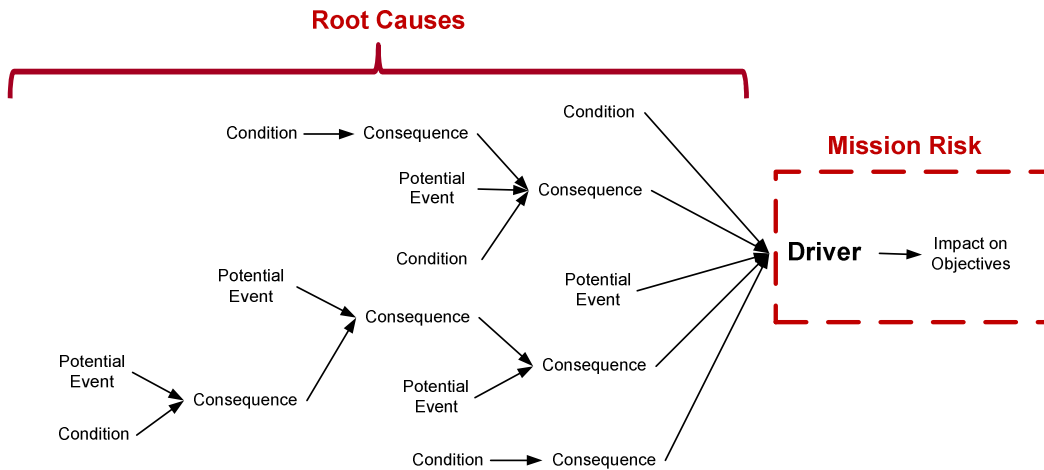
Figure 9: Mission Risk

HOLISTIC ANALYSIS

Applying mission risk analysis to interactively complex systems provides decision makers with a means of confidently assessing the behavior of the system as a whole, which is necessary when assessing assurance. The next section of this technical note builds on the concepts outlined in this section by describing a method for employing a driver-based approach to analyze mission risk in interactively complex systems.

4 Mission Risk Diagnostic (MRD) Concepts[11]

PURPOSE OF THE MRD The SEI is developing the Mission Risk Diagnostic (MRD) to assess risk in interactively complex, socio-technical systems, such as projects,[12] programs,[13] and processes.[14] The goal is to gauge the extent to which a system is in position to achieve its mission and objective(s). During its research and development activities over the past few years, the SEI has found the mission-based approach employed by the MRD to be an efficient and effective means of analyzing risk in interactively complex systems [Alberts 2009, Dorofee 2008].[15]

CORE MRD TASKS Table 1 presents a summary of the three core tasks that form the basis of the MRD. In all, the MRD comprises a total of 13 tasks that must be completed. (A description of all MRD tasks is provided in Section 5 of this document.) This section provides a conceptual overview of the three core MRD tasks. The concepts and examples in this section are presented in the context of a large-scale software acquisition and development program, which is one specific type of interactively complex system.

Table 1: Core Tasks of the MRD

Task	Description
1. Identify the mission and objective(s)	This task establishes the focus of the analysis and the specific aspects of the system that are important to decision makers. One or more objectives are identified during this activity.
2. Identify drivers	Here, a small set of critical factors (typically 10-25) that have a strong influence on whether or not the objective(s) will be achieved are established. These factors are called drivers.
3. Analyze drivers	During driver analysis, the value of each driver is evaluated to determine how it is currently influencing performance. Next, the reasons underlying the evaluation of each driver (called the rationale) and any tangible evidence that supports the rationale are documented. Finally, a visual summary of the current values of all drivers relevant to the mission and objectives being assessed is documented.

---

[11] Much of the material in this section is adapted from *A Framework for Categorizing Key Drivers of Risk* [Alberts 2009].

[12] In this document, the term *project* is defined as a planned set of interrelated tasks to be executed over a fixed period of time and within certain cost and other limitations.

[13] In this document, the term *program* is defined as a group of related projects managed in a coordinated way to obtain benefits and control not available from managing them individually. Programs usually include an element of ongoing activity.

[14] In this document, the term *process* is defined as a collection of interrelated work tasks that achieves a specific result [Sharp 2001].

[15] The MRD builds off of and expands on the work of the SEI Mission Success in Complex Environments (MSCE) Special Project. For more information on MSCE, see http://www.sei.cmu.edu/risk/.

4.1   Identify Mission and Objective(s)

GOALS OF IDENTIFYING THE MISSION AND OBJECTIVE(S)

The overarching goals when identifying the mission and objective(s) are to (1) define the fundamental purpose, or mission, of the system that is being examined and (2) establish the specific aspects of the mission that are important to decision makers. Once they have been established, the mission and objective(s) provide the foundation for conducting the assessment.

DEFINITION OF MISSION

The MRD defines the term *mission* as the fundamental purpose of the system that is being examined. In the context of an acquisition program, the mission can be expressed in terms of the software product that is being acquired, developed, and deployed.

EXAMPLE: MISSION

The following is an example of a mission statement as required by the MRD: *The XYZ Program is providing a new, web-based payroll system for our organization.*

IMPORTANCE OF MISSION

The mission statement is important because it defines the target, or focus, of the analysis effort. After the basic target has been established, the next step is to identify which specific aspects of the mission need to be analyzed in detail.

DEFINITION OF OBJECTIVE

In the MRD, an *objective* is defined as a tangible outcome or result that must be achieved when pursuing a mission. Each mission typically comprises multiple objectives. When assessing a system, analysts must select which specific objective(s) will be evaluated during the assessment. Selecting objectives refines the scope of the assessment to address the specific aspects of the mission that are important to decision makers.

SMART OBJECTIVES

In general, objectives identified during the MRD should meet the following criteria:

- *specific*—The objective is concrete, detailed, focused, and well defined. It emphasizes action and states a specific outcome to be accomplished.

- *measurable*—The objective can be measured, and the measurement source is identified.

- *achievable*—The expectation of what will be accomplished is attainable given the time period, resources available, and so on.

- *relevant*—The outcome or result embodied in the objective supports the broader mission being pursued.

- *time-bound*—The time frame in which the objective will be achieved is specified.

EXAMPLE: OBJECTIVE

During driver identification, analysts must select one or more objectives that will be analyzed. The number of objectives depends on the breadth and nature of the issues being investigated. The following is an example of a typical objective for a software acquisition and development program:

By the end of the development and deployment phase (18 months),

- *the web-based payroll system will provide payroll services at all sites across the enterprise*

- *development and deployment costs cannot exceed 20 percent of original estimates*

IMPRECISE EXPRESSION OF OBJECTIVES

The SEI's field experience shows that many decision makers (e.g., acquisition program managers) have difficulty constructing objectives that meet the above criteria for objectives. While decision makers have a tacit understanding of their objectives, they often cannot precisely articulate or express the objectives in a way that addresses the criteria. If the program's objectives are not clearly articulated, decision makers can have trouble assessing whether the program is on track for success. To address this issue, qualitative implementations of the MRD allow for imprecise expressions of objectives. Specific information about objectives that is tacitly understood by program managers and staff becomes more explicit during execution of the MRD.

4.2   Identify Drivers

GOAL OF DRIVER IDENTIFICATION

The main goal of driver identification is to establish a set of systemic factors, called drivers, that can be used to measure performance in relation to a program's mission and objectives. Once the set of drivers is established, analysts can then evaluate each driver in the set to gain insight into the likelihood of achieving the mission and objectives. To measure performance effectively, analysts must ensure that the set of drivers conveys sufficient information about the mission and objective(s) being assessed.

DEFINITION OF DRIVER

The MRD defines a *driver* as a systemic factor that has a strong influence on the eventual outcome or result (i.e., whether or not objectives will be achieved). Table 2 highlights three key attributes of a driver: *name*, *success state*, and *failure state*. The example driver in the table is named *Process*, and it examines how the program's processes are affecting achievement of the software security objective.

Table 2 also indicates that each driver has two possible states: a success state and a failure state. The success state means that the program's processes are helping to guide the program toward a successful outcome (i.e., achieving the objective(s) being evaluated). In contrast, the failure state signifies that the program's processes are driving the program toward a failed outcome (i.e., not achieving the objective(s) being evaluated).

Table 2:   Driver States

Attribute	Description	Example
Name	A concise label that describes the basic nature of the driver.	Process
Success state	A driver exerts a positive influence on the outcome.	The process being used to develop and deploy the system is sufficient.
Failure state	A driver exerts a negative influence on the outcome.	The process being used to develop and deploy the system is insufficient.

ANALYZING A DRIVER'S STATE

Analysis of a driver requires determining how it is currently acting (i.e., its current state) by examining the effects of conditions and potential events on that driver. The goal is to determine if the driver is

- almost certainly in its success state
- most likely in its success state
- equally likely to be in its success or failure states
- most likely in its failure state
- almost certainly in its failure state

The above list can be used to define a qualitative scale for driver analysis. Analyzing each driver in relation to the qualitative scale establishes a benchmark of performance in relation to a system's documented mission and objectives.

4.2.1 Deriving a Set of Drivers

MISSION, OBJECTIVE, AND DRIVER RELATIONSHIPS

The starting point for identifying a set of drivers is to articulate the mission and objectives that are being assessed. (See Section 4.1 for more information about identifying mission and objective.) Analysts can then derive a set of drivers from them. The relationships among mission, objectives, and drivers are depicted in Figure 10. When dealing with multiple objectives, analysts must be sure to record these relationships to enable effective decision making.
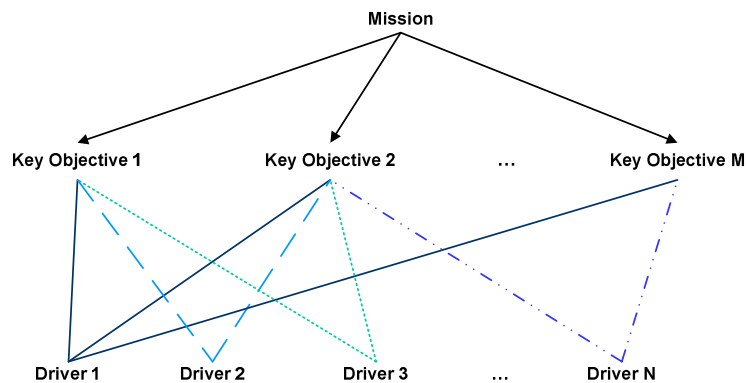
Figure 10: Relationships Among Objectives and Drivers

IMPORTANCE OF EXPERIENCE AND EXPERTISE

Deriving a unique set of drivers based on the program's mission and objectives requires gathering information from people with experience and expertise relevant to the specified mission and objectives. For example, identifying a set of drivers for software development objectives requires input from acquisition programs managers and software-reliant systems developers. Similarly, analysts seeking to identify a set of drivers for software security would consult with security experts.

QUESTIONS FOR IDENTIFYING DRIVER DATA

The experts from whom information is elicited should be familiar with the objectives that have been defined. Analysts can use the objectives to focus interviews or discussions with experts. During interviews or discussions, experts answer the following questions:

- What circumstances, conditions, and events will drive your program toward a *successful* outcome?
- What circumstances, conditions, and events will drive your program toward a *failed* outcome?

ANALYZING DRIVER DATA

After they obtain information from the experts, analysts organize the information into approximately 10–25 groups that share the driver as the central idea or theme of each group. The SEI has employed this approach for identifying drivers in a variety of areas, including software acquisition and development programs, cybersecurity processes, and business portfolio management [Alberts 2009]. The next section presents a standard set of drivers for software acquisition and development programs.

4.2.2 A Standard Set of Drivers for Software Acquisition and Development

STANDARD SET OF PROGRAM DRIVERS

The SEI has applied driver identification to software acquisition and development programs. As a result, a standard set of 20 drivers for these programs has been identified and documented. (More details about the 20 drivers can be found in the Appendix of this technical note.) Table 3 lists the name of each driver along with a question that is used when analyzing that driver's state. These standard drivers were derived from the software development program objective highlighted in Section 4.1[16] The standard set of drivers for software acquisition and development programs serves as an archetype that analysts can quickly tailor and apply to specific programs.

Table 3:   Prototype Set of Driver Questions for Software Acquisition and Development Programs

	Driver Name	Driver Question
1.	Program Objectives	Are program objectives (product, cost, schedule) realistic and achievable?
2.	Plan	Is the plan for developing and deploying the system sufficient?
3.	Process	Is the process being used to develop and deploy the system sufficient?
4.	Task Execution	Are tasks and activities performed effectively and efficiently?
5.	Coordination	Are activities within each team and across teams coordinated appropriately?
6.	External Interfaces	Will work products from suppliers, partners, or collaborators meet the program's quality and timeliness requirements?
7.	Information Management	Is the program's information managed appropriately?
8.	Technology	Does the program team have the tools and technologies it needs to develop the system and transition it to operations?
9.	Facilities and Equipment	Are facilities and equipment sufficient to support the program?
10.	Organizational Conditions	Are enterprise, organizational, and political conditions facilitating completion of program activities?
11.	Compliance	Does the program comply with all relevant policies, laws, and regulations?
12.	Event Management	Does the program have sufficient capacity and capability to identify and manage potential events and changing circumstances?
13.	Requirements	Are system requirements well understood?
14.	Architecture and Design	Are the architecture and design sufficient to meet system requirements and provide the desired operational capability?
15.	System Capability	Will the system satisfactorily meet its requirements?
16.	System Integration	Will the system sufficiently integrate and interoperate with other systems when deployed?

---

[16] The standard set of drivers for software acquisition and development programs was derived from the following generic objective: *By the end of the development and deployment phase (N months), the system will provide agreed-upon services to users, and development and deployment costs cannot exceed X percent of original estimates.*

Driver Name		Driver Question
17.	Operational Support	Will the system effectively support operations?
18.	Adoption Barriers	Have barriers to customer/user adoption of the system been managed appropriately?
19.	Operational Preparedness	Will people be prepared to operate, use, and maintain the system?
20.	Certification and Accreditation	Will the system be appropriately certified and accredited for operational use?

PROGRAMMATIC AND PRODUCT DRIVERS

The drivers in Table 3 can be divided into two fundamental types: programmatic drivers and product drivers. Drivers 1–12 are referred to as *programmatic* drivers because they provide insight into how well a system (e.g., a software acquisition and development program) is being managed. Drivers 13–20 are referred to as *product* drivers because they provide insight into the software product that is being acquired, developed, and deployed.

4.2.3 Tailoring an Existing Set of Drivers

TAILORING CONSIDERATIONS

The standard drivers (Table 3) describe factors that analysts should consider when assessing software acquisition and development programs. However, the standard set must be tailored to the requirements of a specific program to ensure that the

- set of drivers accurately reflects the objectives of the program being assessed
- set of drivers is adjusted appropriately based on the program's context and characteristics
- phrasing of each driver is consistent with the program's terminology

STARTING POINT: IDENTIFYING OBJECTIVES

The starting point when tailoring an existing set of drivers is to clearly articulate the program's mission and objectives. (See Section 4.1 for more information about identifying mission and objective.) In addition, background information about the program is required to understand what the program is trying to accomplish and to gain an appreciation for its unique context and characteristics.

After analysts gain a basic understanding of the program's context, they can then begin to tailor the drivers. Based on the objectives being assessed and the data that has been gathered, analysts must complete the following steps:

1. Determine which drivers do not apply to the program. Eliminate extraneous drivers from the set.

2. Establish whether any drivers are missing from the list. Add those drivers to the set.

3. Decide if multiple drivers from the set should be combined into a single, high-level driver. Replace those drivers with a single driver that combines them.

4. Decide if any drivers should be decomposed into multiple, more detailed drivers. Decompose each of those drivers into multiple drivers.

5. Adjust the wording of each driver to be consistent with the terminology and language of the program that is being assessed.

At this point, the tailored set of drivers can be used to assess the program's current state by conducting driver analysis.

4.3 Analyze Drivers

GOAL OF DRIVER ANALYSIS

The goal of driver analysis is to determine how each driver is influencing the objectives. More specifically, the probability of a driver being in its success state or failure state must be established.

Each driver question in Table 3 is expressed as a yes/no question that is phrased from the *success perspective*. Figure 11 depicts a driver question for the Process driver. This example will be used throughout this section when discussing driver analysis.

```
┌─────────────────────────────────────────────────────────────────────────────┐
│  Driver 3: Process                                                            │
│                                                                               │
│  Driver Question                                      Response                │
│                                                                               │
│   Is the process being used to develop and deploy the system sufficient?   ❑ Yes │
│                                                       ❑ Likely Yes            │
│      Considerations:                                  ❑ Equally Likely        │
│      ▪  Process design                                ❑ Likely No             │
│      ▪  Measurements and controls                     ❑ No                    │
│      ▪  Process efficiency and effectiveness          ❑ Don't Know            │
│      ▪  Acquisition and development life cycles                               │
│      ▪  Training                                                              │
└─────────────────────────────────────────────────────────────────────────────┘
```

Figure 11: Driver Question and Range of Responses

STRUCTURE OF DRIVER QUESTIONS

Because the question in Figure 11 is phrased from the success perspective, an answer of *yes* indicates the driver is in its success state and an answer of *no* indicates it is in its failure state. A range of answers is used to determine probabilities (likely yes, equally likely yes or no, likely no) when the answer is not a definitive yes or no. In addition, key items to consider when answering each question, called *considerations*, are provided for each driver question. The prototype set of standard driver questions for software security along with the considerations for each question are listed in the Appendix section of this technical note.

DRIVER VALUE CRITERIA

A set of *driver value criteria*, such as those shown in Figure 12, are normally used to support driver analysis. Driver value criteria serve two main purposes:

- They provide a definition of applicable responses to a driver question.
- They translate each response into the probability that the driver is in its success state, as well as the probability that it is in its failure state.

TAILORING DRIVER VALUE CRITERIA

The criteria for analyzing a driver must be tailored for each application of driver analysis. For example, the criteria in Figure 12 are based on a five-point scale, which allows decision makers to incorporate different levels of probability in their answers. A different number of answers (i.e., more or less than five) can be incorporated into the analysis when appropriate. In addition, some people prefer to include a response of *don't know* to highlight those instances where more information or investigation is needed before a driver can be analyzed appropriately.

Response	Definition	Values	
		Probability of Success State	Probability of Failure State
Yes	The answer is almost certainly "yes." Almost no uncertainty exists. There is little or no probability that the answer could be "no." (~ > 95% probability of yes)	Maximum	Minimum
Likely yes	The answer is most likely "yes." There is some chance that the answer could be "no." (~ 75% probability of yes)	High	Low
Equally likely	The answer is just as likely to be "yes" or "no." (~ 50% probability of yes)	Medium	Medium
Likely no	The answer is most likely "no." There is some chance that the answer could be "yes." (~ 25% probability of yes)	Low	High
No	The answer is almost certainly "no." Almost no uncertainty exists. There is little or no probability that the answer could be "yes." (~ < 5% probability of yes)	Minimum	Maximum

Figure 12: Driver Value Criteria

EFFECT OF CONDITIONS AND EVENTS ON DRIVERS

When they analyze a driver, analysts need to consider how conditions and potential events[17] affect that driver. In general, the following items should be considered for each driver that is analyzed:[18]

- positive conditions that support a response of *yes*

- negative conditions that support a response of *no*

- potential events with positive consequences that support a response of *yes*

- potential events with negative consequences that support a response of *no*

- unknown factors that contribute to uncertainty regarding the response

- assumptions that might bias the response

---

[17] A *condition* is defined as the current state of being or existence. Conditions define the current set of circumstances that have an impact on system performance. A *potential event* is defined as an occurrence or happening that alters current conditions and, as a result, changes a system's performance characteristics [Alberts 2009].

[18] The first four items in the list are from the causal chain of conditions and events. See Section 2 for more information about the causal chain of conditions and events. The last two items in the list, unknown factors and assumptions, relate to what is known or assumed about the causal chain of conditions and events. People will not have perfect information about conditions and events that are influencing system performance; some unknowns will exist. Analysts need to identify these unknowns and factor then into the analysis. Additional data-gathering activities can be conducted to reduce the number of unknowns. People will also make assumptions about how things are working. These assumptions can be tested to determine whether they are valid or not.

EXAMPLE: ANALYZED DRIVER

Figure 13 shows an example of an analyzed driver. The answer to the driver question is *likely no*, which means that the driver is most likely in its failure state. As a result, the program's processes are most likely insufficient for achieving the objective.

Driver 3: Process

Driver Question

Is the process being used to develop and deploy the system sufficient?

Considerations:
- Process design
- Measurements and controls
- Process efficiency and effectiveness
- Acquisition and development life cycles
- Training

Response

- ☐ Yes
- ☐ Likely Yes
- ☐ Equally Likely
- ☒ Likely No
- ☐ No
- ☐ Don't Know

Rationale

+ Previous programs have a 90% history of delivering on-time.
– The process for integration testing is likely inadequate. Historically, integration testing has used "verbal" agreements between a few managers who already know each other. With this system, there are managers and team leads who have never worked together and there are other barriers in place that make "verbal" agreements tenuous.
– There are a lot of brand new programmers (45%).
– This program required a significant change in our standard processes. There was no new training created for the new processes.
– QA did not have a chance to review the new and revised processes before they were put into practice.

Figure 13: Analyzed Driver

RATIONALE AND EVIDENCE

The rationale for the response to each driver question must also be documented because it captures the reasons why analysts selected the response. Any evidence supporting the rationale, such as the results of interviews with system stakeholders and information cited from system documentation must also be cited as well. (Figure 13 only shows the rationale.) Recording the rationale and evidence is important for validating the data and associated information products, for historical purposes, and for developing lessons learned.

DRIVER PROFILE

A *driver profile* provides a visual summary of the current values of all drivers relevant to the mission and objectives being assessed. A driver profile can be viewed as a dashboard that provides decision makers with a graphical summary of current conditions and expected performance in relation to the mission and objectives being pursued by a program. It depicts the probability that each driver is in its success state. A high probability for a driver indicates that the driver has a high probability of being in its success state.

EXAMPLE: DRIVER PROFILE

Figure 14 provides an example of a driver profile for software acquisition and development. In Figure 14, a bar graph is used to show 20 drivers that correspond to the standard set of drivers for software acquisition and development programs. Programmatic drivers are separated from the product drivers in the figure. The profile in Figure 14 indicates that the following four drivers have a high probability of being in their failure states: Program Objectives, Process, Organizational Conditions, and System Integration. The states of these four drivers should concern the program's decision makers.
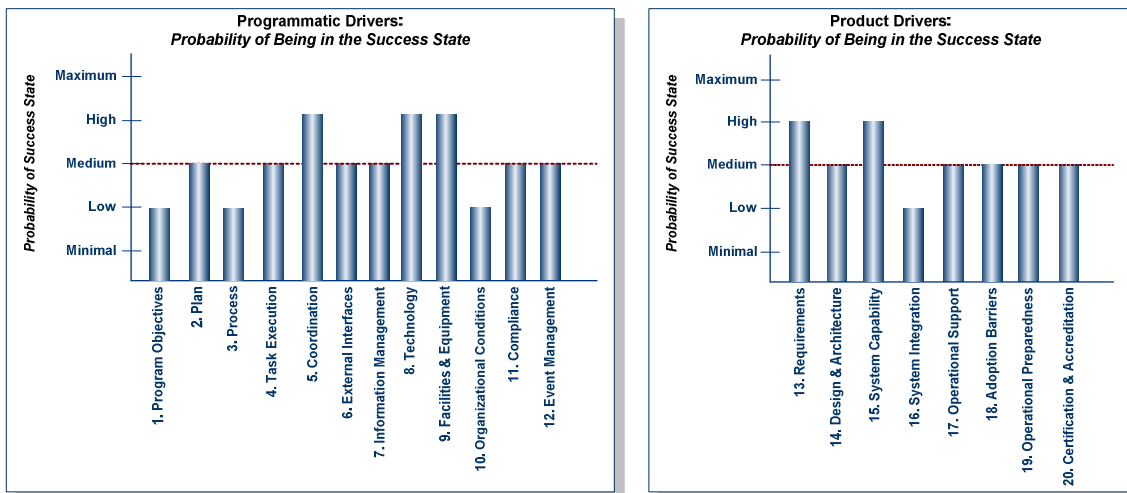
Figure 14: Driver Profile

MISSION RISK

Mission risk is defined as the probability of mission failure (i.e., not achieving key objectives). From the MRD perspective, *mission risk* is defined as the probability that a driver is in its failure state.

RELATIONSHIP BETWEEN DRIVER VALUE AND MISSION RISK

As illustrated in Figure 15, a relationship exists between a driver's success state (as depicted in a driver profile) and mission risk. A driver profile shows the probability that drivers are in their success states. Thus, a driver with a high probability of being in its success state (i.e., a high degree of momentum toward the mission) translates to a low degree of mission risk. Likewise, a driver with a low probability of being in its success state (i.e., a high probability of being in its failure state) translates to a high degree of mission risk.

The driver profile thus helps decision makers understand how much mission risk is currently affecting a system (e.g., project, program, process). Decision makers can then identify actions intended to increase the probabilities of selected drivers being in their success states and, as a result, mitigate mission risk.

Figure 15: The Relationship Between Driver Value and Mission Risk

5 Mission Risk Diagnostic (MRD) Method

PURPOSE OF THE MRD METHOD DESCRIPTION

This section describes the Mission Risk Diagnostic (MRD) method. It begins with an overview of MRD activities and tasks. Then, details for each MRD activity are provided, along with selected examples. The examples are not meant to be all-inclusive; rather they are provided to assist the reader in understanding what an activity accomplishes. The MRD method description illustrates the core activities and tasks that must be performed when conducting the method. However, it does not provide specific step-by-step directions needed to conduct the method.

CONDUCTING THE MRD METHOD

The MRD is designed to assess risk in interactively complex, socio-technical systems. It 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.

ASSESSMENT TEAM

This section is written from the perspective of using an external party to conduct the MRD.[19] A small team of people, called the *assessment team*, is responsible for conducting the assessment and reporting its findings to stakeholders.

MRD OBJECTIVES

The main objectives of the MRD are to

- assess a system's mission risk by evaluating a small set of drivers in relation to current conditions
- determine whether mission risk is within an acceptable tolerance
- identify actions to control mission risk

---

[19] The MRD can also be self-applied by the person or group that is responsible for managing a system. Self-application of the MRD is not addressed in this technical note.

MRD BENEFITS   The following are the key benefits of applying the MRD:

- The MRD provides a time-efficient means of assessing mission risk in interactively complex systems.

- People do not need to be experts in risk management to obtain actionable results.

- Results can be used to communicate status information to senior managers.

MRD LIMITATIONS   The following list summarizes the limitations of the MRD:

- The MRD must be tailored for a specific domain or problem space, which requires experience and expertise in the MRD method.

- Some issues can elude detection if people use a generic set of drivers rather than a set that uniquely reflects the specific domain and program being assessed.

- The results are only as good as the data that are gathered.

SKILLS REQUIRED   The MRD is normally performed by an assessment team that has the following skills:[20]

- detailed knowledge of the specific domain in which risk is being assessed

- knowledge of risk management

- knowledge of process improvement and management

- knowledge and skills appropriate to applying the MRD, such as

  – analytical skills

  – interviewing skills

  – facilitation skills

  – note-taking skills (i.e., ability to quickly record data that are identified by participants)

  – communication skills

---

[20]   These skills can be distributed across a number of people on the assessment team. Some people may have multiple skills, and others may be specialists. It is important is for the team performing the MRD, as a whole, to have this set of skills.

5.1 MRD Structure

MRD ACTIVITIES AND TASKS

Figure 16 illustrates the activities and tasks that must be completed when conducting the MRD. An *activity* is defined as a collection of measurable work tasks that must be completed in order to achieve a specified outcome during an assessment. The MRD method consists of three activities:

1. Prepare for the assessment

2. Conduct the assessment

3. Complete post-assessment tasks

In the MRD, each activity requires analysts to complete multiple tasks. Here, a *task* is defined as a piece of work that must be completed when performing an assessment activity. In total, the MRD comprises 13 tasks.

| Activity 1
Prepare for the assessment | Activity 2
Conduct the assessment | Activity 3
Complete post-assessment tasks |

Tasks
1.1 Form the assessment team
1.2 Develop stakeholder sponsorship
1.3 Set the scope of the assessment
1.4 Develop the assessment plan
1.5 Coordinate logistics
1.6 Tailor method and tools

Tasks
2.1 Identify mission and objective(s)
2.2 Identify drivers
2.3 Analyze drivers
2.4 Determine next steps

Tasks
3.1 Communicate results
3.2 Conduct assessment postmortem
3.3 Improve assessment process

Figure 16: MRD Activities and Tasks

MRD METHOD DESCRIPTION

The MRD method description provides an overview of each activity that must be completed when conducting the MRD. In addition, the method description also provides an overview for each task performed during Activity 2, *Conduct the assessment*.

Activity 2 is described in more detail than the other two activities because it specifies the distinct sequence of activities that uniquely defines the MRD.

STRUCTURE OF ACTIVITY DESCRIPTIONS

Each MRD activity is described in Section 5. The description of an MRD activity includes the following items:

- an introduction to the activity
- a list of key questions that the activity must answer
- a data flow diagram for the activity
- inputs to the activity
- any constraints that affect execution of the activity
- any resources that are required to conduct the activity
- the outputs produced by the activity
- key roles needed to conduct the activity
- the specific tasks that must be performed when conducting the activity

STRUCTURE OF TASK DESCRIPTIONS

Each task from Activity 2 is described in Section 5.3. The description of an MRD task includes the following items:

- an introduction to the task
- a list of key questions that the task must answer
- a data flow diagram for the task
- inputs to the task
- the final outputs produced by the task
- the specific steps that must be completed when performing the task

5.2   Prepare for the Assessment (Activity 1)

INTRODUCTION

Activity 1 of the MRD, *Prepare for the assessment*, is focused on getting ready to conduct the assessment. This includes all of the planning and logistics management needed to make the assessment execution flow smoothly as well as assuring that key stakeholders provide visible support for the assessment. This preparation lays the foundation for conducting the assessment during Activity 2.

KEY QUESTIONS

Activity 1 answers the following questions:

- Who will conduct the assessment? How will the person or group responsible for conducting the assessment acquire the necessary knowledge and abilities?

- How can stakeholder sponsorship be attained?

- What is the scope of the assessment?

- What is the plan for conducting the assessment?

- What logistics need to be addressed in order to conduct the assessment?

- How will the assessment method and support tools be tailored or modified?

DATA FLOW

The following diagram highlights the data flow for Activity 1.
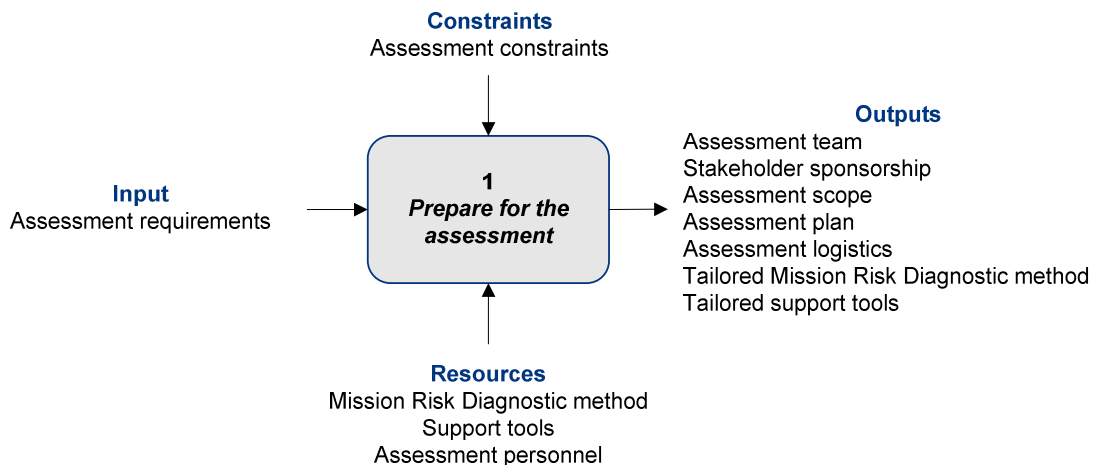
Figure 17: Data Flow for MRD Activity 1

The following input is required by Activity 1.

Input	Description
Assessment requirements	The goals of the assessment, needs of the stakeholders, and a basic description of the system being analyzed

CONSTRAINT   The following constraint affects execution of Activity 1.

Constraint	Description
Assessment constraints	Any circumstances, including logistics, personnel, schedule, and cost issues, that could affect assessment activities

RESOURCES   The following resources support execution of Activity 1.

Resource	Description
Mission Risk Diagnostic method	An approach for assessing mission risk in interactively complex, socio-technical systems, such as projects, programs, and processes
Support tools	The standard set of tools used when conducting the MRD, including worksheets, automated tools, and databases
Assessment personnel	People who are candidates to be part of an MRD assessment team

OUTPUTS   The following outputs are produced by Activity 1.

Output	Description
Assessment team	A small team of people responsible for conducting the assessment and reporting findings to the assessment sponsor(s) and selected system stakeholders
Stakeholder sponsorship	Active and visible support of the assessment by system stakeholders. Sponsorship can exist in a variety of forms, including • active participation in the assessment by management and staff • directives or policies from management facilitating implementation of the assessment • amount of funding and resources allocated to risk management activities

Output	Description
Assessment scope[21]	The boundaries of the assessment, including • the system being assessed • which system components will (and will not) be included in the assessment • stakeholders who have responsibility for the system and its components
Assessment plan	The approach for conducting the assessment, including key activities and tasks, resources required, roles and responsibilities, schedule, and funding, as well as the requirements for communicating results to key stakeholders after the assessment is complete
Assessment logistics	The facilities and equipment needed to conduct the assessment as well as communications about meeting times and locations
Tailored Mission Risk Diagnostic method	A version of the MRD that is adapted for a specific application of the method. Procedures for conducting activities and tasks are modified as needed for the specific application of the MRD.
Tailored support tools	MRD support tools that have been adapted for a specific application of the method. Support tools include worksheets, automated tools, and databases.

KEY ROLES

The following roles are needed to perform Activity 1.

Role	Description
MRD stakeholders	Decision makers from the organization that will conduct the MRD. These stakeholders are typically managers who contract with the assessment sponsor(s) and selected system stakeholders to perform a risk assessment. MRD stakeholders then select the assessment team lead and team members.
Assessment team leader	The person who is assigned responsibility for leading the assessment team. The assessment team leader leads the planning and execution of the assessment.
Assessment team	A small team of people responsible for conducting the assessment and reporting findings to the assessment sponsor(s) and selected system stakeholders
Assessment team members	People selected to be on the assessment team. The team leader assigns team members specific tasks to perform during the assessment.
Assessment sponsor(s)	The person or group that is sponsoring the assessment
System stakeholders	People who have a vested interest in the system that is being assessed. System stakeholders can include people who • manage or oversee system execution • perform activities that enable system execution • provide inputs to the system • use products or services provided by the system

---

[21] The scope defines which activities to include in the assessment and becomes a constraint in Activity 2. Some aspects of a system might be excluded from an assessment due to contract limitations or on the basis of cost.

Role	Description
Site coordinator	One person at each participating site who is responsible for (1) setting up data collection activities at the site and (2) managing logistics with the team coordinator. During the assessment, each site coordinator • helps identify who needs to participate in interviews/workshops • schedules interviews/workshops with site staff and the assessment team • coordinates meeting rooms and equipment • provides requested program documentation to the assessment team • handles unexpected events (e.g., substituting personnel in interviews/workshops)
Team coordinator	A member of the assessment team who is responsible for managing logistics with the site coordinator(s). The team coordinator works closely with each site coordinator to ensure that • site staff who will participate in interviews/workshops are identified • interviews/workshops are scheduled in a timely manner • meeting rooms and equipment are available when needed • program documentation is provided to the assessment team • any unexpected events (e.g., substituting personnel in interviews/workshops) are handled appropriately

TASKS The following table highlights the tasks performed during Activity 1.[22]

Task		Description	Output(s)
1.1	Form the assessment team	Stakeholders from the organization that will conduct the MRD (called MRD stakeholders) both select people to participate on the assessment team and select the person who will be the assessment team leader. Assessment team members acquire the knowledge and abilities they need to conduct their assigned activities.	Assessment team
1.2	Develop stakeholder sponsorship	The assessment team leader meets with the assessment sponsor(s) and selected system stakeholders to build active and visible support for the assessment. Several meetings might be needed to build the necessary sponsorship of the assessment.	Stakeholder sponsorship
1.3	Set the scope of the assessment	The assessment team determines the boundaries of the assessment based on requirements and constraints (e.g., schedule, funding, logistics, contractual restrictions).	Assessment scope
1.4	Develop the assessment plan	The assessment team creates a plan for conducting the assessment based on the assessment's scope, requirements, and constraints (schedule, funding, etc.).	Assessment plan

---

[22] Detailed descriptions of the tasks performed during Activity 1 are not provided in this document.

Task		Description	Output(s)
1.5	Coordinate logistics	The team coordinator and site coordinator(s) address logistics for data-gathering activities, including reserving rooms for meetings, making sure that any required equipment (e.g., overhead projectors, flip charts) is available, and informing people when meetings will be held.	Assessment logistics
1.6	Tailor method and tools	The assessment team adapts the MRD method and support tools (e.g., worksheets, templates, tools) for the circumstances and contexts in which they will be used.	Tailored Mission Risk Diagnostic method Tailored support tools

ORDER OF ACTIVITY 1 TASKS

The order in which the tasks of Activity 1 are performed is not necessarily fixed, although there is a logical progression.

- Some activities require more than one iteration to complete.
- Overlaps between some activities can occur.

5.3   Conduct the Assessment (Activity 2)

INTRODUCTION

During Activity 2, *Conduct the assessment*, the core assessment activities are performed. During this activity, data are gathered from people and generated from relevant documentation. These data are then used to identify and analyze a set of drivers for the system being assessed, determine whether the current state of each driver is acceptable, and identify actions for maintaining or improving the current state of each driver.

KEY QUESTIONS

Activity 2 answers the following questions:

- What is the system's mission?
- What specific aspect(s) of the mission is being assessed?
- Which systemic factors, or drivers, will be evaluated during the assessment?
- What is the probability that each driver is in its success state (i.e., driver value)?
- What are the rationale and evidence supporting the evaluation of each driver?
- What is the current snapshot or profile of all drivers?
- What strategies will be implemented after the assessment to maintain or improve current driver values?

DATA FLOW

The following diagram highlights the data flow for Activity 2.

Constraints
Stakeholder sponsorship
Assessment scope
Assessment plan
Assessment logistics

Key Outputs
Mission
Objective(s)
Drivers
Current driver values
Rationales and evidence
Driver profile
Next steps

Inputs
People's knowledge
System documentation

2
Conduct the assessment

Resources
Tailored Mission Risk Diagnostic method
Tailored support tools
Assessment team
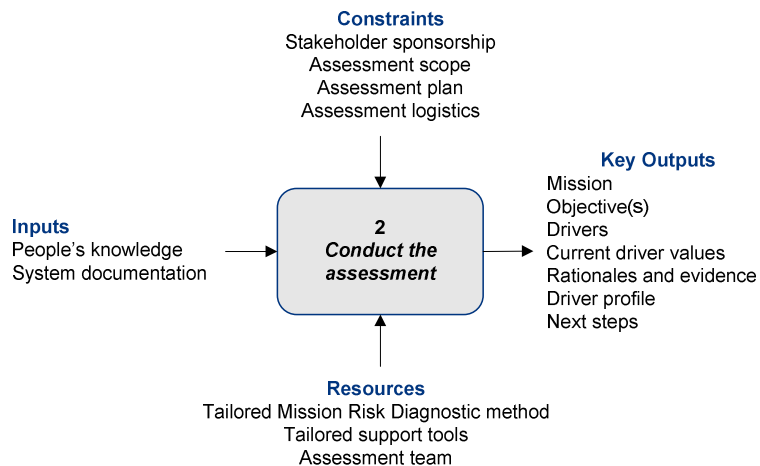
Figure 18: Data Flow for MRD Activity 2

The following inputs are required by Activity 2.

Input	Description
People's knowledge	People's individual and collective perspectives, information, and opinions about the system, factors that can affect system performance, and risks that are currently affecting the system
System documentation	Recorded information that is relevant to the system that is being assessed. Examples include mission statement, policies, procedures, process workflow, work products, and quality assurance data.

CONSTRAINTS   The following constraints affect execution of Activity 2.[23]

Constraint	Description
Stakeholder sponsorship	Active and visible support of the assessment by system stakeholders. Sponsorship can exist in a variety of forms, including • active participation in the assessment by management and staff • directives or policies from management facilitating implementation of the assessment • amount of funding and resources allocated to risk management activities
Assessment scope	The boundaries of the assessment, including • the system being assessed • which system components will (and will not) be included in the assessment • stakeholders who have responsibility for the system and its components
Assessment plan	The approach for conducting the assessment, including key activities and tasks, resources required, roles and responsibilities, schedule, and funding, as well as the requirements for communicating results to key stakeholders after the assessment is complete
Assessment logistics	The facilities and equipment needed to conduct the assessment as well as communications about meeting times and locations

---

[23]   Each constraint is an output of Activity 1.

The following resources support execution of Activity 2.[24]

Resource	Description
Assessment team	A small team of people responsible for conducting the assessment and reporting findings to the assessment sponsor(s) and selected system stakeholders
Tailored Mission Risk Diagnostic method	A version of the MRD that is adapted for a specific application of the method. Procedures for conducting activities and tasks are modified as needed for the specific application of the MRD.
Tailored support tools	MRD support tools that have been adapted for a specific application of the method. Support tools include worksheets, automated tools, and databases.

KEY OUTPUTS

The following key outputs are produced by Activity 2.[25]

Output	Description
Mission	The fundamental purpose of the system that is being examined
Objective(s)	A tangible outcome or result that must be achieved when pursuing a mission; defines specific aspects of the mission that are important to decision makers
Drivers	A systemic factor that has a strong influence on the eventual outcome or result (i.e., whether or not objectives will be achieved). Each driver is phrased as a yes-no question from the success perspective; an answer of *yes* indicates the driver is in its success state, and an answer of *no* indicates it is in its failure state.
Current drivers values	The response to a driver question (yes, likely yes, equally likely, likely no, no)
Rationales and evidence	The reasoning underlying the response to a driver question (i.e., current driver value) and any proof that supports the rationale (e.g., the results of interviews with system stakeholders, references to excerpts of system documentation)
Driver profile	A visual summary of the current values of all drivers relevant to the mission and objectives being assessed
Next steps	Actions that will be taken after the assessment is complete, who is responsible for completing each action, and the completion date for each action

---

[24]   Each resource is an output of Activity 1.

[25]   Activity 2 produces several additional outputs beyond those shown in the table. These additional outputs represent interim work products. Definitions for all relevant interim work products are provided in the task descriptions. (See Sections 5.3.1–-5.3.4 for descriptions of interim work products.)

KEY ROLES

The following roles are needed to perform Activity 2.

Role	Description
Assessment team	A small team of people responsible for conducting the assessment and reporting findings to the assessment sponsor(s) and selected system stakeholders
Assessment sponsor(s)	The person or group that is sponsoring the assessment
System stakeholders	People who have a vested interest in the system that is being assessed. System stakeholders can include people who • manage or oversee system execution • perform activities that enable system execution • provide inputs to the system • use products or services provided by the system
Domain experts	People who have considerable knowledge, experience, and expertise related to the domain of interest (e.g., software acquisition and development, information security). For example, identifying a set of drivers for software development objectives requires input from acquisition programs managers and software developers. Similarly, identifying a set of drivers for information security would require input from information security experts.

TASKS

The following table highlights the tasks performed during Activity 2.

Task	Description	Output(s)
2.1 Identify mission and objective(s)	The assessment team collects and documents usable data about the system's mission and objective(s) from the assessment sponsor(s) and selected system stakeholders. The team also collects and documents usable data about the system's mission and objective(s) by reviewing system documentation (e.g., policies, procedures, reports). The assessment team then identifies and documents the system's mission and objective(s), which form the basis for the assessment.	Mission Objective(s)
2.2 Identify drivers	The assessment team collects and documents usable data about conditions and events that can affect system performance from selected system stakeholders and domain experts. The team also collects and documents usable data about conditions and events that can affect system performance by reviewing system documentation (e.g., policies, procedures, reports). The assessment team then identifies and documents a set of factors (called drivers) that it will evaluate during the assessment.	Drivers

Task		Description	Output(s)
2.3	Analyze drivers	The assessment team collects and documents usable data about the system's current state from selected system stakeholders. The team also collects and documents usable data about the system's current state by reviewing system documentation (e.g., policies, procedures, reports). The assessment team then answers each driver question, documents the rationale and evidence for each answer, and creates a visual summary of the current values of all drivers (called the driver profile).	Current drivers values Rationales and evidence Driver profile
2.4	Determine next steps	The assessment team reviews relevant driver data from Task 2.3. The team then brainstorms candidate strategies that could be implemented after the assessment to maintain or improve current driver values. Finally, the team selects and documents the strategies that it will recommend to system stakeholders. The team can consult with system stakeholders, if appropriate, when brainstorming and selecting next steps.	Next steps

DETAILED DATA FLOW FOR ACTIVITY 2 TASKS

The figure on the next page provides a detailed data flow for the tasks that must be completed during Activity 2.
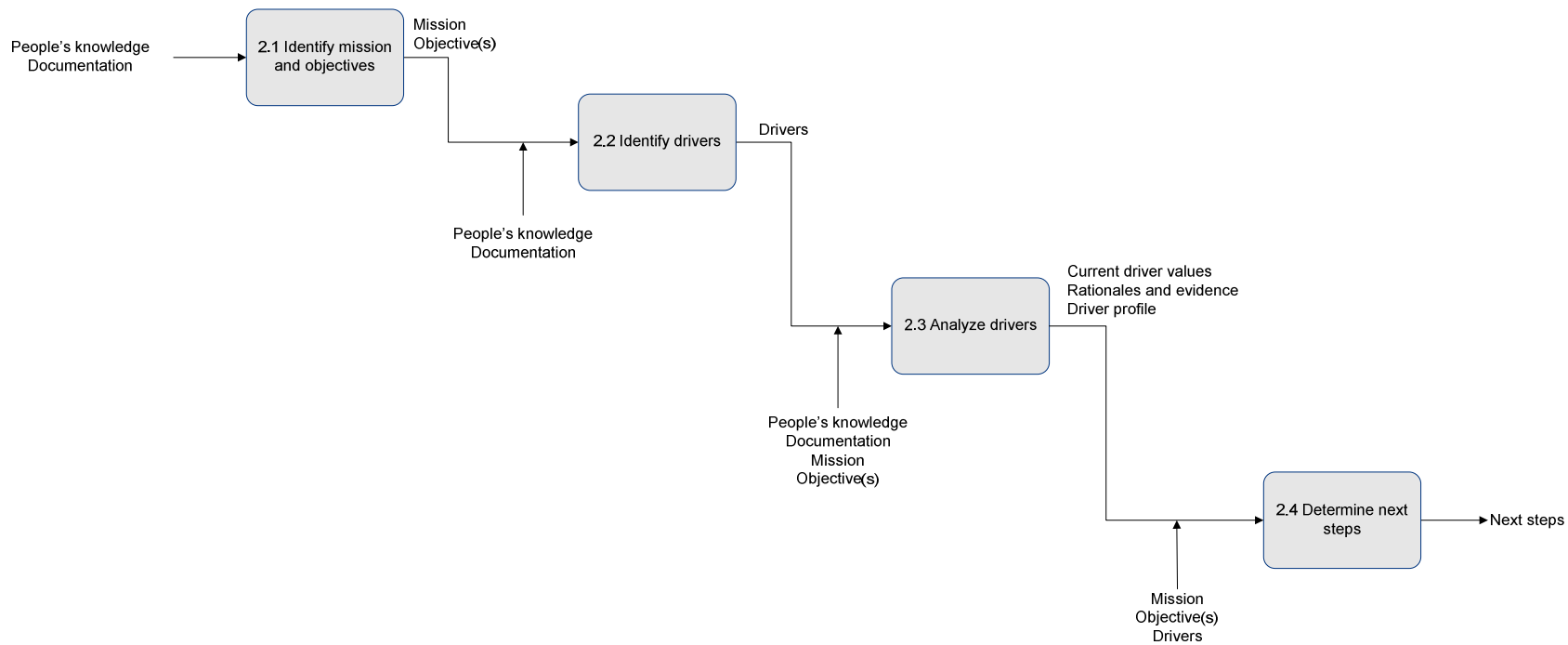
Figure 19: Detailed Data Flow for MRD Activity 2 Tasks

5.3.1   Identify Mission and Objective(s) (Task 2.1)

INTRODUCTION

Task 2.1, *Identify mission and objective(s)*, kicks off Activity 2 of the MRD. During this task, the assessment team identifies and documents the system's mission and objective(s), which define the fundamental purpose of the system that is being examined and establish the specific aspects of the mission that are important to decision makers. The mission and objective(s) provide the foundation for all subsequent assessment tasks.

KEY QUESTIONS

Task 2.1 answers the following questions:

- What is the system's mission?
- What specific aspect(s) of the mission is being assessed?

DATA FLOW

The following diagram highlights the data flow for Task 2.1.

Inputs
People's knowledge
System documentation

2.1
Identify mission and objective(s)

Outputs
Mission data from people
Mission data from documentation
Mission
Objective(s)
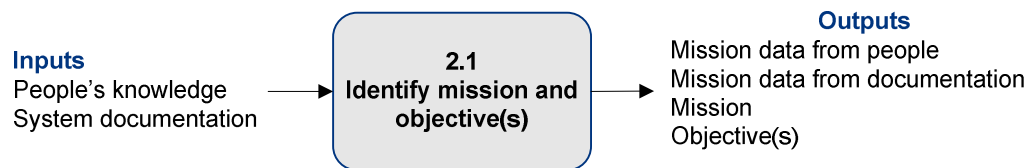
Figure 20: Data Flow for MRD Task 2.1

INPUTS

The following inputs are required by Task 2.1.

Input	Description
People's knowledge	People's individual and collective perspectives, information, and opinions about the system, factors that can affect system performance, and risks that are currently affecting the system
System documentation	Recorded information that is relevant to the system that is being assessed. Examples include mission statement, policies, procedures, process workflow, work products, and quality assurance data.

The following outputs are produced by Task 2.1.

Output	Description
Mission data from people	Usable data about the system's mission and objective(s) obtained from the assessment sponsor(s) and selected system stakeholders
Mission data from documentation	Usable data about the system's mission and objective(s) obtained from reviewing system documentation
Mission	The fundamental purpose of the system that is being examined
Objective(s)	A tangible outcome or result that must be achieved when pursuing a mission; defines specific aspects of the mission that are important to decision makers

KEY ROLES

The following roles are needed to perform Task 2.1.

Role	Description
Assessment team	A small team of people responsible for conducting the assessment and reporting findings to the assessment sponsor(s) and selected system stakeholders
Assessment sponsor(s)	The person or group that is sponsoring the assessment
System stakeholders	People who have a vested interest in the system that is being assessed. System stakeholders can include people who • manage or oversee system execution • perform activities that enable system execution • provide inputs to the system • use products or services provided by the system

STEPS

The following table highlights the steps performed during Task 2.1.

Step		Description	Output(s)
2.1.1	Gather mission data from people	The assessment team collects and documents usable data about the system's mission and objective(s) from the assessment sponsor(s) and from selected system stakeholders who have a broad view of the system and its mission.	Mission data from people
2.1.2	Generate mission data from documentation	The assessment team reviews system documentation (e.g., policies, procedures, reports). The team generates and documents usable data about the system's mission and objective(s).	Mission data from documentation

Step		Description	Output(s)
2.1.3	Establish system mission	The assessment team reviews the mission data that it has collected (from people and documentation). The team then identifies and documents the system's mission. The assessment team can review the mission with the assessment sponsor(s) and selected system stakeholders, if appropriate.	Mission
2.1.4	Establish system objective(s)	The assessment team reviews the mission data that it has collected (from people and documentation). The team then identifies and documents one or more system objectives. Each objective describes a specific aspect of the system's mission that will be evaluated during the assessment. The assessment team can review the objective(s) with the assessment sponsor(s) and selected system stakeholders, if appropriate.	Objective(s)

5.3.2   Identify Drivers (Task 2.2)

INTRODUCTION

During Task 2.2, *Identify drivers*, the assessment team identifies a sets of systemic factors, called drivers, that have a strong influence on the eventual outcome or result (i.e., whether or not objectives will be achieved). Each driver has two possible states: a success state and a failure state. The success state means that the driver is guiding the system toward its mission and objective(s). The failure state signifies that the driver is guiding the system away from its mission and objective(s).

KEY QUESTIONS

Task 2.2 answers the following questions:

- What conditions and events are driving the project or process toward a successful outcome?
- What conditions and events are driving the project or process toward an unsuccessful, or failed, outcome?
- Which systemic factors, or drivers, will be evaluated during the assessment?

DATA FLOW

The following diagram highlights the data flow for Task 2.2.

Inputs
People's knowledge
System documentation
Mission
Objective(s)

**2.2
Identify drivers**

Outputs
Driver identification data from people
Driver identification data from documentation
Drivers
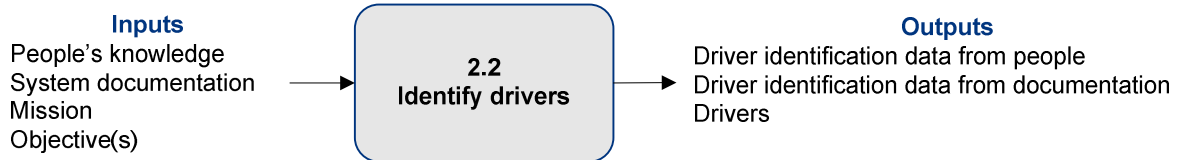
Figure 21: Data Flow for MRD Task 2.2

INPUTS

The following inputs are required by Task 2.2.

Input	Description
People's knowledge	People's individual and collective perspectives, information, and opinions about the system, factors that can affect system performance, and risks that are currently affecting the system
System documentation	Recorded information that is relevant to the system that is being assessed. Examples include mission statement, policies, procedures, process workflow, work products, and quality assurance data.
Mission	The fundamental purpose of the system that is being examined

Input	Description
Objective(s)	A tangible outcome or result that must be achieved when pursuing a mission; defines specific aspects of the mission that are important to decision makers

OUTPUTS

The following outputs are produced by Task 2.2.

Output	Description
Driver identification data from people	Usable data about conditions and events that can affect system performance obtained from selected system stakeholders
Driver identification data from documentation	Usable data about conditions and events that can affect system performance obtained from reviewing system documentation
Drivers	A systemic factor that has a strong influence on the eventual outcome or result (i.e., whether or not objectives will be achieved). Each driver is phrased as a yes-no question from the success perspective; an answer of *yes* indicates the driver is in its success state, and an answer of *no* indicates it is in its failure state.

KEY ROLES

The following roles are needed to perform Task 2.2.

Role	Description
Assessment team	A small team of people responsible for conducting the assessment and reporting findings to the assessment sponsor(s) and selected system stakeholders
System stakeholders	People who have a vested interest in the system that is being assessed. System stakeholders can include people who • manage or oversee system execution • perform activities that enable system execution • provide inputs to the system • use products or services provided by the system
Domain experts	People who have considerable knowledge, experience, and expertise related to the domain of interest (e.g., software acquisition and development, information security). For example, identifying a set of drivers for software development objectives requires input from acquisition programs managers and software developers. Similarly, identifying a set of drivers for information security would require input from information security experts.

The following table highlights the steps performed during Task 2.2.

Step		Description	Output(s)
2.2.1	Gather driver identification data from people	The assessment team collects and documents usable data from selected system stakeholders and domain experts about conditions and events that can affect system performance.	Driver identification data from people
2.2.2	Generate driver identification data from documentation	The assessment team reviews system documentation (e.g., policies, procedures, reports). The team generates and documents usable data about conditions and events that can affect system performance.	Driver identification data from documentation
2.2.3	Determine system drivers	The assessment team reviews the driver identification data that it has collected (from people and documentation). The team then identifies and documents the drivers that it will use during the assessment, either by deriving a new set of drivers or by tailoring an existing set. The assessment team can review the drivers with selected system stakeholders and domain experts, if appropriate.	Drivers

5.3.3 Analyze Drivers (Task 2.3)

INTRODUCTION

During Task 2.3, *Analyze drivers*, the assessment team evaluates the current state of the system. The team determines how each driver is currently influencing the systems' mission and objective(s) by establishing the probability that the driver is in its success state. The end product of Task 2.3 is the driver profile, which provides a visual summary of the current values of all drivers.

KEY QUESTIONS

Task 2.3 answers the following questions:

- What is the probability that each driver is in its success state (i.e., driver value)?

- What are the rationale and evidence supporting the evaluation of each driver?

- What is the current snapshot or profile of all drivers?

DATA FLOW

The following diagram highlights the data flow for Task 2.3.

Inputs
People's knowledge
System documentation
Mission
Objective(s)
Drivers

**2.3
Analyze drivers**

Outputs
Driver analysis data from people
Driver analysis data from documentation
Current driver values
Rationales and evidence
Driver profile
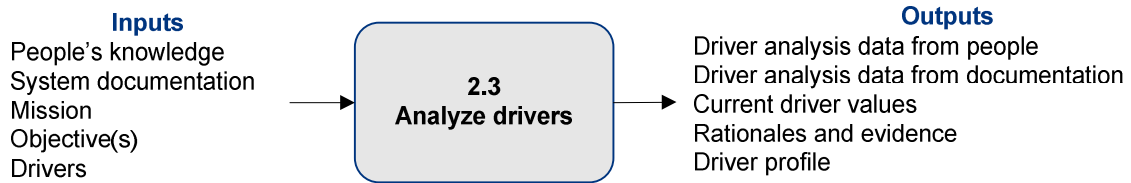
Figure 22: Data Flow for MRD Task 2.3

INPUTS

The following inputs are required by Task 2.3.

Input	Description
People's knowledge	People's individual and collective perspectives, information, and opinions about the system, factors that can affect system performance, and risks that are currently affecting the system
System documentation	Recorded information that is relevant to the system that is being assessed. Examples include mission statement, policies, procedures, process workflow, work products, and quality assurance data.
Mission	The fundamental purpose of the system that is being examined
Objective(s)	A tangible outcome or result that must be achieved when pursuing a mission; defines specific aspects of the mission that are important to decision makers

Input	Description
Drivers	A systemic factor that has a strong influence on the eventual outcome or result (i.e., whether or not objectives will be achieved). Each driver is phrased as a yes-no question from the success perspective; an answer of *yes* indicates the driver is in its success state, and an answer of *no* indicates it is in its failure state.

OUTPUTS

The following outputs are produced by Task 2.3.

Output	Description
Driver analysis data from people	Usable data about the system's current state obtained from selected system stakeholders
Driver analysis data from documentation	Usable data about the system's current state obtained from reviewing system documentation
Current drivers values	The response to a driver question (yes, likely yes, equally likely, likely no, no)
Rationales and evidence	The reasoning underlying the response to a driver question (i.e., current driver value) and any proof that supports the rationale (e.g., the results of interviews with system stakeholders, references to excerpts of system documentation)
Driver profile	A visual summary of the current values of all drivers relevant to the mission and objectives being assessed

KEY ROLES

The following roles are needed to perform Task 2.3.

Role	Description
Assessment team	A small team of people responsible for conducting the assessment and reporting findings to the assessment sponsor(s) and selected system stakeholders
System stakeholders	People who have a vested interest in the system that is being assessed. System stakeholders can include people who • manage or oversee system execution • perform activities that enable system execution • provide inputs to the system • use products or services provided by the system

The following table highlights the steps performed during Task 2.3.

Step		Description	Output(s)
2.3.1	Gather driver analysis data from people	The assessment team collects and documents usable data from selected system stakeholders about the system's current state. System stakeholders who participate in this step answer all driver questions and provide their rationale for each answer.	Driver analysis data from people
2.3.2	Generate driver analysis data from documentation	The assessment team reviews system documentation (e.g., policies, procedures, reports). The team generates and documents usable data about the system's current state. When reviewing documentation, the assessment team looks for data that provides insight into how drivers are currently acting (i.e., the probability that each driver is in its success state).	Driver analysis data from documentation
2.3.3	Evaluate drivers	The assessment team reviews the driver analysis data that it has collected (from people and documentation). The team answers all driver questions to establish the probability that each driver is in its success state. The team also documents (1) the rationale for each answer and (2) any evidence that supports each answer (e.g., results of interviews with system stakeholders, information from system documentation).	Current drivers values Rationales and evidence
2.3.4	Establish driver profile	The assessment team develops and documents a visual summary of the current values of all drivers that were evaluated.	Driver profile

5.3.4 Determine Next Steps (Task 2.4)

INTRODUCTION

During Task 2.4, *Determine next steps*, the assessment team recommends strategies that can be implemented after the assessment to maintain or improve current driver values. The results of Task 2.1 serve as a bridge between the assessment and any follow-on, detailed planning activities. All strategies, or next steps, identified during this task should be at an appropriate level of detail based on

- the goals of the assessment

- depth and breadth of the data collected

- knowledge, skills, and abilities of the people conducting the assessment

- expectations of stakeholders

KEY QUESTIONS

Task 2.4 answers the following questions:

- What strategies would maintain or improve current driver values?

- What are the relative benefits and limitations of each candidate strategy?

- Which strategies are recommended for implementation?

DATA FLOW

The following diagram highlights the data flow for Task 2.4.

Inputs
Mission
Objective(s)
Drivers
Current driver values
Rationales and evidence
Driver profile

**2.4
Determine next steps**

Outputs
Reviewed driver data
Candidate next steps
Next steps
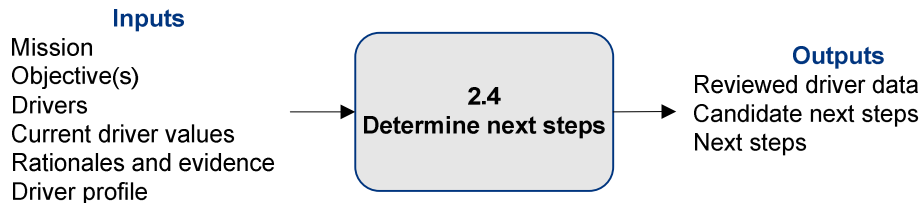
Figure 23: Data Flow for MRD Task 2.4

INPUTS

The following inputs are required by Task 2.4.

Input	Description
Mission	The fundamental purpose of the system that is being examined
Objective(s)	A tangible outcome or result that must be achieved when pursuing a mission; defines specific aspects of the mission that are important to decision makers

Input	Description
Drivers	A systemic factor that has a strong influence on the eventual outcome or result (i.e., whether or not objectives will be achieved). Each driver is phrased as a yes-no question from the success perspective; an answer of *yes* indicates the driver is in its success state, and an answer of *no* indicates it is in its failure state.
Current drivers values	The response to a driver question (yes, likely yes, equally likely, likely no, no)
Rationales and evidence	The reasoning underlying the response to a driver question (i.e., current driver value) and any proof that supports the rationale (e.g., the results of interviews with system stakeholders, references to excerpts of system documentation)
Driver profile	A visual summary of the current values of all drivers relevant to the mission and objectives being assessed

OUTPUTS   The following outputs are produced by Task 2.4.

Output	Description
Reviewed driver data	Data that have been reviewed by the assessment team prior to developing next steps, including • the response to each driver question • the rationale for each response • supporting evidence for each response • driver analysis data (from people and documentation) as appropriate
Candidate next steps	Potential strategies that could be implemented after the assessment is complete
Next steps	Strategies that the assessment team recommends for implementation

KEY ROLES   The following roles are needed to perform Task 2.4.

Role	Description
Assessment team	A small team of people responsible for conducting the assessment and reporting findings to the assessment sponsor(s) and selected system stakeholders
System stakeholders	People who have a vested interest in the system that is being assessed. System stakeholders can include people who • manage or oversee system execution • perform activities that enable system execution • provide inputs to the system • use products or services provided by the system

The following table highlights the steps performed during Task 2.4.

Step		Description	Output(s)
2.4.1	Review driver data	The assessment team reviews the following data: • the response to each driver question • the rationale for each response • supporting evidence for each response • driver analysis data (from people and documentation) as appropriate	Reviewed driver data
2.4.2	Brainstorm candidate next steps	The assessment team brainstorms candidate strategies that could be implemented after the assessment to maintain or improve current driver values. The team can consult with system stakeholders, if appropriate, when brainstorming candidate next steps.	Candidate next steps
2.4.3	Select next steps	The assessment team selects and documents strategies that it will recommend to system stakeholders. The team can consult with system stakeholders, if appropriate, when selecting next steps.	Next steps

5.4   Complete Post-Assessment Tasks (Activity 3)

INTRODUCTION

Activity 3, *Complete post-assessment tasks*, conveys the results of the assessment to key system stakeholders and identifies actions that can help the efficiency and effectiveness of the MRD method. The objective when communicating assessment results to system stakeholders is to present findings in a format that meets their needs and requirements. Different formats might be needed to communicate results to different types of stakeholders.

A postmortem is used to identify and document ways in which the MRD method and support tools can be improved.[26] Updates and improvements to the MRD procedures, artifacts, tools, and training are made as appropriate.

KEY QUESTIONS

Activity 3 answers the following questions:

- Who needs to know the results of the assessment?

- What information does each stakeholder need?

- How should information be communicated to each stakeholder?

- What lessons were learned when preparing for the assessment?

- What lessons were learned when conducting the assessment?

- How do the assessment method, support tools, and training need to be updated or improved?

DATA FLOW

The following diagram highlights the data flow for Activity 3.

Constraints
Assessment constraints

Inputs
Assessment results and plans
Assessment method, support tools, and training

3
Conduct post-assessment tasks

Outputs
Communicated assessment results
Lessons learned
Updates to assessment method, support tools, and training

Resources
Mission Risk Diagnostic method
Support tools
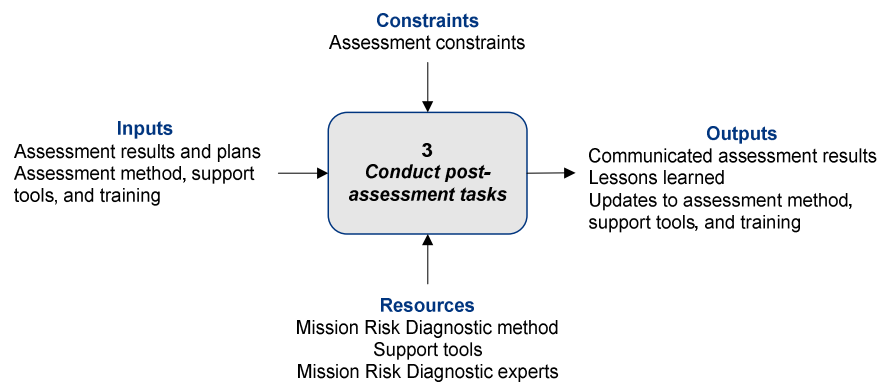Mission Risk Diagnostic experts

Figure 24: Data Flow for MRD Activity 3

---

[26]   Postmortems are usually conducted after a given assessment. However, they can also be held on a more periodic basis if multiple assessments are planned.

The following inputs are required by Activity 3.

Input	Description
Assessment results and plans	All outputs produced by the assessment, including findings and assessment data, as well as plans, budget, and schedule for conducting the assessment
Assessment method, support tools, and training	Supporting materials used to conduct the Mission Risk Diagnostic, including procedures, worksheets, databases, and training artifacts

CONSTRAINT   The following constraint affects execution of Activity 3.

Constraint	Description
Assessment constraints	Any circumstances, including logistics, personnel, schedule, and cost issues, that could affect assessment activities

RESOURCES   The following resources support execution of Activity 3.

Resource	Description
Mission Risk Diagnostic method	An approach for assessing mission risk in interactively complex, socio-technical systems, such as projects, programs, and processes
Support tools	The standard set of tools used when conducting the MRD, including worksheets, automated tools, and databases
Mission Risk Diagnostic experts	People who have experience and expertise in applying and tailoring the Mission Risk Diagnostic, including the person assigned responsibility for overseeing the MRD process as well as people who have the knowledge and ability to make changes to the MRD method and support tools

OUTPUTS   The following outputs are produced by Activity 3.

Output	Description
Communicated assessment results	Assessment results that have been conveyed to key stakeholders, including • driver values • driver profile for the program • recommended next steps • supporting data (as appropriate)

Output	Description
Lessons learned	Knowledge gained by conducting the assessment that can be used to modify and improve future assessments
Updates to assessment method, support tools, and training	Any changes, based on lessons learned, to the MRD method and support tools intended to improve the efficiency and effectiveness of future assessments

KEY ROLES

The following roles are needed to perform Activity 3.

Role	Description
MRD process owner	The person from the organization that conducted the MRD who has ultimate ownership of the MRD method and support tools
Postmortem leader	A person who has experience and expertise in applying and tailoring the Mission Risk Diagnostic and has sufficient skills to lead a postmortem session. The postmortem leader is selected by the MRD process owner.
Assessment team leader	The person who is assigned responsibility for leading the assessment team. The assessment team leader leads the planning and execution of the assessment.
Assessment team	A small team of people responsible for conducting the assessment and reporting findings to the assessment sponsor(s) and selected system stakeholders
Assessment team members	People selected to be on the assessment team. The team leader assigns team members specific tasks to perform during the assessment.
Assessment sponsor(s)	The person or group that is sponsoring the assessment
System stakeholders	People who have a vested interest in the system that is being assessed. System stakeholders can include people who • manage or oversee system execution • perform activities that enable system execution • provide inputs to the system • use products or services provided by the system

TASKS

The following table highlights the tasks performed during Activity 3.

Task	Description	Output(s)
3.1 Communicate results	The assessment team leader (or an assessment team member designated by the assessment team leader) presents the results of the assessment to the assessment sponsor(s) and selected system stakeholders.	Communicated assessment results

Task		Description	Output(s)
3.2	Conduct assessment postmortem	The postmortem leader conducts one or more meetings with the assessment team to identify the strengths and weaknesses of the MRD method and support tools and document any suggested modifications and improvements to the method and tools.	Lessons learned
3.3	Improve assessment process	The MRD process owner (or someone designated by the MRD process owner) makes changes to the MRD method and support tools, based on lessons learned. Changes can include updating procedures, artifacts, tools, and training.	Updates to assessment method, support tools, and training

6 Summary

RISK MANAGEMENT

Risk management defines a systematic approach for minimizing exposure to potential losses. It includes the following three core activities:

- **assess risk**—transform the concerns people have into distinct, tangible risks that are explicitly documented and analyzed
- **plan for controlling risk**—determine an approach for addressing each risk; produce a plan for implementing the approach
- **control risk**—deal with each risk by implementing its defined control plan and tracking the plan to completion

INADEQUATE ASSESSMENT OF RISK

Although most programs and organizations use some form of risk management when developing and operating software-reliant systems, preventable failures continue to occur. SEI field experience has yielded anecdotal evidence that programs and organizations throughout government and industry are unable to assess their risks effectively. As a result, SEI researchers undertook a project to examine and improve the practice of risk assessment. This technical note describes the results of SEI research related to risk assessment.

TACTICAL RISK ANALYSIS

Most traditional approaches for assessing risk are based on tactical risk analysis, where the goal is to evaluate a system's components for potential failures. Tactical risk analysis enables stakeholders to determine which components are most critical to a system and analyze ways in which those critical components might fail (i.e., analyze the risk to critical components). Stakeholders can then implement effective controls designed to mitigate those potential failures.

TACTICAL RISK ANALYSIS: PARTIAL PICTURE OF RISK

When analysts attempt to decompose interactively complex systems, some system-wide behaviors become lost. It is very difficult to establish the relationship between the macro-level behavior of the system and the micro-level behavior of individual components. As a result, tactical risk analysis provides a partial picture of the risks to an interactively complex system. To get a more holistic view of risk in an interactively complex system, analysts need to employ an alternative analysis approach.

MISSION RISK ANALYSIS

Mission risk analysis is based on system theory. The underlying principle of system theory is to analyze a system as a whole rather than decompose it into individual components and then analyze 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.

MISSION RISK DIAGNOSTIC (MRD)

The Mission Risk Diagnostic (MRD) employs mission risk analysis to assess risk in interactively complex, socio-technical systems across the life cycle and supply chain. The overarching goal of the MRD is to determine the extent to which a system is in position to achieve its mission and objectives.

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. This technical note examines how an external party conducts the MRD on behalf of a sponsoring organization. Here, a small team of people, called the assessment team, is responsible for conducting the assessment and reporting its findings to stakeholders.

FUTURE DIRECTIONS

SEI field experience over the past several years has shown the MRD to be an efficient and effective means of analyzing risk in interactively complex systems. To date, the SEI has employed the MRD successfully in a variety of domains, including software acquisition and development, cybersecurity, software security, and business portfolio management.

The MRD also provides a platform for future SEI research and development in the areas of software assurance and mission assurance. SEI researchers intend to refine the MRD method based on the lessons learned from piloting the method and will continue to look for opportunities to apply the MRD in different venues.

Appendix: Standard Set of Drivers for Software Acquisition and Development

This appendix provides a prototype set of driver questions for assessing software acquisition and development programs as described in Section 4.2.2. This set of drivers is derived from the following generic objective:

> By the end of the development and deployment phase (N months),
>
> - the system will provide agreed-upon services to users
> - development and deployment costs cannot exceed *X* percent of original estimates

Programmatic Drivers

1. **Program Objectives**: Are program objectives (product, cost, schedule) realistic and achievable?

2. **Plan**: Is the plan for developing and deploying the system sufficient?

3. **Process**: Is the process being used to develop and deploy the system sufficient?

4. **Task Execution**: Are tasks and activities performed effectively and efficiently?

5. **Coordination**: Are activities within each team and across teams coordinated appropriately?

6. **External Interfaces**: Will work products from suppliers, partners, or collaborators meet the program's quality and timeliness requirements?

7. **Information Management**: Is the program's information managed appropriately?

8. **Technology**: Does the program team have the tools and technologies it needs to develop the system and transition it to operations?

9. **Facilities and Equipment**: Are facilities and equipment sufficient to support the program?

10. **Organizational Conditions**: Are enterprise, organizational, and political conditions facilitating completion of program activities?

11. **Compliance**: Does the program comply with all relevant policies, laws, and regulations?

12. **Event Management**: Does the program have sufficient capacity and capability to identify and manage potential events and changing circumstances?

Product Drivers

13. **Requirements**: Are system requirements well understood?

14. **Architecture and Design**: Are the architecture and design sufficient to meet system requirements and provide the desired operational capability?

15. **System Capability**: Will the system satisfactorily meet its requirements?

16. **System Integration**: Will the system sufficiently integrate and interoperate with other systems when deployed?

17. **Operational Support**: Will the system effectively support operations?

18. **Adoption Barriers**: Have barriers to customer/user adoption of the system been managed appropriately?

19. **Operational Preparedness**: Will people be prepared to operate, use, and maintain the system?

20. **Certification and Accreditation**: Will the system be appropriately certified and accredited for operational use?

Driver 1: Program Objectives

Are program objectives (product, cost, schedule) realistic and achievable?

Considerations:
- Alignment of technical, cost, and schedule objectives
- Inherent technical risk
- Technology maturity
- Resources available

Driver 2: Plan

Is the plan for developing and deploying the system sufficient?

Considerations:
- Acquisition or development strategy
- Program plan
- Resources
- Funding
- Schedule
- Roles and responsibilities

Driver 3: Process

Is the process being used to develop and deploy the system sufficient?

Considerations:
- Process design
- Measurements and controls
- Process efficiency and effectiveness
- Acquisition and development life cycles
- Training

Driver 4: Task Execution

Are tasks and activities performed effectively and efficiently?

Considerations:
- Experience and expertise of management and staff
- Staffing levels
- Experience with the acquisition and development life cycles

---

Driver 5: Coordination

Are activities within each team and across teams coordinated appropriately?

Considerations:
- Communication
- Information sharing
- Dependencies
- Relationships
- Partners and collaborators

Driver 6: External Interfaces

Will work products from suppliers, partners, or collaborators meet the program's quality and timeliness requirements?

Considerations:
- Applications
- Software
- Systems or subsystems
- Hardware

Driver 7: Information Management

Is the program's information managed appropriately?

Considerations:
- Usability
- Confidentiality
- Integrity
- Availability

Driver 8: Technology

Does the program team have the tools and technologies it needs to develop the system and transition it to operations?

Considerations:
- Software applications
- Infrastructure
- Systems
- Databases

Driver 9: Facilities and Equipment

Are facilities and equipment sufficient to support the program?

Considerations:
- Building
- Physical work spaces
- Support equipment
- Supplies
- Other resources

Driver 10: Organizational Conditions

Are enterprise, organizational, and political conditions facilitating completion of program activities?

Considerations:
- Stakeholder sponsorship
- Actions of upper management
- Effect of laws, regulations, and policies

Driver 11: Compliance

Does the program comply with all relevant policies, laws, and regulations?

Considerations:
- Policies
- Laws
- Regulations
- Standards of care

Driver 12: Event Management

Does the program have sufficient capacity and capability to identify and manage potential events and changing circumstances?

Considerations:
- Risk management plan, process, and tools
- Schedule slack
- Funding reserve
- Risk mitigation plans
- Program continuity and contingency plans
- Opportunity management plan, process, and tools

Driver 13: Requirements

Are system requirements well understood?

Considerations:
- Customer, user, and stakeholder requirements and needs
- Functional and nonfunctional requirements
- Operational requirements
- System growth and expansion needs
- Technology maturity

Driver 14: Architecture and Design

Are the architecture and design sufficient to meet system requirements and provide the desired operational capability?

Considerations:
- Interfaces
- Dependencies
- Software and system architecture
- Operational requirements
- Technology maturity

Driver 15: System Capability

Will the system satisfactorily meet its requirements?

Considerations:
- Functional
- Performance
- Operational
- Reliability
- Security
- Safety
- Usability
- Maintainability
- Technology maturity

Driver 16: System Integration

Will the system sufficiently integrate and interoperate with other systems when deployed?

Considerations:
- Interfaces
- Applications
- Tools
- Hardware
- Data
- Technology maturity

Driver 17: Operational Support

Will the system effectively support operations?

Considerations:
- Business and operational workflows
- Support of organizational and enterprise missions
- Operational risk mitigation
- Disaster recovery, contingency, and business continuity plans
- Technology maturity

Driver 18: Adoption Barriers

Have barriers to customer/user adoption of the system been managed appropriately?

Considerations:
- User acceptance
- Stakeholder sponsorship
- Transition to operations
- User support

Driver 19: Operational Preparedness

Will people be prepared to operate, use, and maintain the system?

Considerations:
- Policies
- Procedures
- Training

Driver 20: Certification and Accreditation

Will the system be appropriately certified and accredited for operational use?

Considerations:
- Compliance with policies, laws, and regulations
- Acceptable mitigation of risk

Glossary

activity
a collection of measurable work tasks that must be completed in order to achieve a specified outcome during an assessment; an activity comprises multiple tasks

assessment team
a small team of people responsible for conducting the assessment and reporting its findings to stakeholders

condition
the current state of being or existence; conditions define the current set of circumstances that can contribute to the strengths, issues/problems, risks, and opportunities affecting an entity (e.g., program, system) and its performance over time

consequence
the result or effect produced by a risk, issue/problem, or opportunity

driver
a systemic factor that has a strong influence on the eventual outcome or result (i.e., whether or not objectives will be achieved)

driver analysis
an approach for determining how each driver is influencing the objectives

driver identification
an approach for establishing a set of systemic factors, called drivers, that can be used to measure performance in relation to a system's mission and objectives

driver profile
a visual summary of the current values of all drivers relevant to the mission and objectives being assessed

failure state
a driver exerts a negative influence on the outcome; one of two possible states a driver can assume

impact
a measure of the loss that occurs when a risk is realized

interactive complexity
the presence of unplanned and unexpected sequences of events in a system that are either not visible or not immediately understood

interactively complex system
a system whose components interact in relatively unconstrained ways

issue

a loss or adverse consequence that has occurred or is certain to occur; see *problem*

mission

the fundamental purpose of the system that is being examined

mission risk

the probability of mission failure (i.e., not achieving key objectives); the probability that a driver is in its failure state

mission risk analysis

a risk analysis that examines the aggregate effects of multiple conditions and events on a system's ability to achieve its mission

Mission Risk Diagnostic (MRD)

an approach for assessing mission risk in interactively complex, socio-technical systems, such as projects, programs, and processes

mitigation

any action taken to address a risk

objective

a tangible outcome or result that must be achieved when pursuing a mission; defines specific aspects of the mission that are important to decision makers

opportunity

the probability of realizing a gain

potential event

an occurrence or happening that alters current conditions and, as a result, changes a system's performance characteristics

probability

a measure of the likelihood that an event will occur

problem

a loss or adverse consequence that has occurred or is certain to occur; see *issue*

process

a collection of interrelated work tasks that achieves a specific result

program

a group of related projects managed in a coordinated way to obtain benefits and control not available from managing them individually; programs usually include an element of ongoing activity

project

a planned set of interrelated tasks to be executed over a fixed period of time and within certain cost and other limitations

risk

the probability of suffering harm or loss

risk management

a systematic approach for minimizing exposure to potential losses

socio-technical system

interrelated technical and social elements (e.g., people who are organized in teams or departments, technologies on which people rely) that are engaged in goal-oriented behavior

software-reliant system

a socio-technical system whose behavior (e.g., functionality, performance, safety, security, interoperability, and so forth) is dependent on software in some significant way

success state

a driver exerts a positive influence on the outcome; one of two possible states a driver can assume

system decomposition and event analysis

an analysis approach in which a socio-technical system's critical components are evaluated for potential failures

systemic risk

the probability of mission failure (i.e., not achieving key objectives); see *mission risk*

tactical risk

the probability that an event will lead to a negative consequence or loss

tactical risk analysis

a risk analysis (based on the principle of system decomposition and component analysis) that evaluates a system's components for potential failures

task

a piece of work that must be completed when performing an assessment activity

References

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

[Alberts 2002]
Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE^{SM} Approach*. Addison-Wesley, 2002.
http://www.sei.cmu.edu/library/abstracts/books/0321118863.cfm

[Alberts 2006]
Alberts, Christopher. *Common Elements of Risk* (CMU/SEI-2006-TN-014). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006.
http://www.sei.cmu.edu/library/abstracts/reports/06tn014.cfm

[Alberts 2009]
Alberts, Christopher & Dorofee, Audrey. *A Framework for Categorizing Key Drivers of Risk* (CMU/SEI-2009-TR-007). Software Engineering Institute, Carnegie Mellon University, 2009.
http://www.sei.cmu.edu/library/abstracts/reports/09tr007.cfm

[Bergey 2009]
Bergey, John K. *A Proactive Means for Incorporating a Software Architecture Evaluation in a DoD System Acquisition* (CMU/SEI-2009-TN-004). Software Engineering Institute, Carnegie Mellon University, 2009. http://www.sei.cmu.edu/library/abstracts/reports/09tn004.cfm

[Charette 1990]
Charette, Robert N. *Application Strategies for Risk Analysis*. McGraw-Hill Book Company, 1990.

[Dorofee 1996]
Dorofee, A.; Walker, J.; Alberts, C.; Higuera, R.; Murphy, R.; & Williams, R. *Continuous Risk Management Guidebook*. Software Engineering Institute, Carnegie Mellon University, 1996.
http://www.sei.cmu.edu/library/abstracts/books/crmguidebook.cfm

[Dorofee 2008]
Dorofee, Audrey; Marino, Lisa; & Alberts, Christopher. *Lessons Learned Applying the Mission Diagnostic* (CMU/SEI-2008-TN-004). Software Engineering Institute, Carnegie Mellon University, 2008. http://www.sei.cmu.edu/library/abstracts/reports/08tn004.cfm

[Gallagher 1999]
Gallagher, Brian. *Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook Version 1.02* (CMU/SEI-99-HB-001). Software Engineering Institute, Carnegie Mellon University, 1999. http://www.sei.cmu.edu/library/abstracts/reports/99hb001.cfm

[Gallagher 2005]
Gallagher, B.; Case, P.; Creel, R.; Kushner, S.; & Williams, R. *A Taxonomy of Operational Risks* (CMU/SEI-2005-TN-036). Software Engineering Institute, Carnegie Mellon University, 2005.
http://www.sei.cmu.edu/library/abstracts/reports/05tn036.cfm

[Kloman 1990]

Kloman, H. F. "Risk Management Agonists." *Risk Analysis 10,* 2 (June 1990): 201–205.

[Leveson 2004]

Leveson, Nancy. "A New Accident Model for Engineering Safer Systems." *Safety Science 42*, 4 (April 2004): 237–270. http://sunnyday.mit.edu/accidents/safetyscience-single.pdf

[Perrow 1999]

Perrow, Charles. *Normal Accidents: Living with High-Risk Technologies*. Princeton University Press, 1999.

[Sharp 2001]

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

[Williams 1999]

Williams, R.; Pandelios, G.; & Behrens, S. *Software Risk Evaluation (SRE) Method Description (Version 2.0)* (CMU/SEI-99-TR-029). Software Engineering Institute, Carnegie Mellon University, 1999. http://www.sei.cmu.edu/library/abstracts/reports/99tr029.cfm

REPORT DOCUMENTATION PAGE

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE February 2012	3. REPORT TYPE AND DATES COVERED Final

4. TITLE AND SUBTITLE Mission Risk Diagnostic (MRD) Method Description	5. FUNDING NUMBERS FA8721-05-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2012-TN-005

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

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. In particular, Carnegie Mellon® Software Engineering Institute (SEI) field experience indicates that programs and organizations throughout government and industry are unable to assess their risks effectively. For example, SEI independent assessments routinely uncover significant risks that have not been brought to the attention of key decision makers. When decision makers are unaware of significant risks, they are unable to take action to mitigate those risks. As a result, SEI researchers undertook a project to examine and improve the practice of risk assessment. The SEI has developed the Mission Risk Diagnostic (MRD) to assess risk in interactively complex, socio-technical systems across the life cycle and supply chain. To date, the SEI has employed the MRD in a variety of domains, including software acquisition and development, cybersecurity, software security, and business portfolio management. This technical note provides an overview of the MRD method.

14. SUBJECT TERMS

Risk, risk management, complex systems, risk analysis tools, risk analysis techniques, risk management tools, risk management techniques, managing complexity, complex systems management, risk analysis, software assurance, mission assurance, acquisition risk, software risk, security risk

15. NUMBER OF PAGES

91

16. PRICE CODE

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

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102