Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Risk Assessment Methodology and Excel Tool for Acquisition Programs	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **RAND Corporation,National Defense Research Institute,1776 Main Street, PO Box 2138,Santa Monica,CA,90407-2138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**48**	

This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.

A Risk Assessment Methodology and Excel Tool for Acquisition Programs

Lauren A. Fleishman-Mayer, Mark V. Arena, Michael E. McMahon

NATIONAL SECURITY RESEARCH DIVISION

A Risk Assessment Methodology and Excel Tool for Acquisition Programs

Lauren A. Fleishman-Mayer, Mark V. Arena, Michael E. McMahon

Prepared for the Office of the Secretary of Defense

This research was conducted within the Acquisition and Technology Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

Library of Congress Cataloging-in-Publication Data

Fleishman-Mayer, Lauren A.
A risk assessment methodology and Excel tool for acquisition programs / Lauren A. Fleishman-Mayer, Mark V. Arena, Michael E. McMahon.
pages cm
Includes bibliographical references.
ISBN 978-0-8330-8060-8 (pbk. : alk. paper)
1. United States—Armed Forces—Weapons systems-—Costs—Evaluation—Methodology.
2. United States. Department of Defense—Procurement—Costs—Evaluation—Methodology.
3. United States. Department of Defense—Procurement—Data processing. 4. Weapons systems—United States—Costs—Forecasting. 5. Systems integration—Risk assessment—Methodology. I. Arena, Mark V. II. McMahon, Michael E. III. Title.
UF503.F54 2013
355.6'20973—dc23

2013037120

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Support RAND—make a tax-deductible charitable contribution at www.rand.org/giving/contribute.html

RAND® is a registered trademark.

RAND OFFICES

SANTA MONICA, CA • WASHINGTON, DC

PITTSBURGH, PA • NEW ORLEANS, LA • JACKSON, MS • BOSTON, MA

DOHA, QA • CAMBRIDGE, UK • BRUSSELS, BE

www.rand.org

Preface

The Department of Defense (DoD) relies on risk management analysis when acquiring large defense acquisition programs. Risk management helps decisionmakers ensure objectives related to cost, schedule, and performance are met according to program goals. To that end, a team of RAND researchers created a Microsoft Excel–based tool (the Assessor Tool) to help DoD acquisition specialists identify system integration risk areas at any point in the acquisition process. This report describes the methodology, calculations, and assumptions used in the Assessor Tool. It also provides a discussion of the types of questions for which the Assessor Tool and methodology could be adapted for different applications.

This work should be of interest to those readers interested in risk assessment of major defense programs. The document does not assume an understanding of the DoD acquisition system. The users' manual for the Assessor Tool is available in a companion document, *An Excel Tool to Assess Acquisition Program Risk* (by Lauren A. Fleishman-Mayer, Mark V. Arena, and Michael E. McMahon, TL-113-OSD, 2013). This research was conducted within the Acquisition and Technology Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

For more information on the Acquisition and Technology Policy Center, see http://www.rand.org/nsrd/ndri/centers/atp.html or contact the director (contact information is provided on the web page).

Obtaining the Assessor Tool

As of this writing, the Assessor Tool has not yet been validated in a real-world setting. As such, we have not made the tool generally available for download from the RAND website. However, we are very interested in providing the tool to prospective users on a trial basis. If you would like to request a copy of the Assessor Tool, please contact the director of the Acquisition and Technology Policy Center via the contact information provided at http://www.rand.org/nsrd/ndri/centers/atp.html

Contents

Figures and Tables

Figures

Tables

Summary

Implementing risk management principles to manage large defense acquisition programs is a priority for the U.S. defense acquisition. In 2006, the U.S. Department of Defense (DoD) released an official risk management guide for acquisition professionals. Furthermore, the 2009 Weapon Systems Acquisition Reform Act (WSARA) mandated that critical technologies undergo a periodic review and assessment regarding technological maturity and integration risk.[1]

To assist those decisionmakers responsible for identifying the risk associated with major weapons programs, RAND researchers developed a methodology and accompanying Excel, information-based risk tool (the "Assessor Tool"). The package offers an approach to the evaluation and measurement of system integration risk for assessors, such as Office of the Secretary of Defense (OSD) staff, who may not be especially familiar with the specific program under evaluation but still may need to make judgments about a program's risk. The Assessor Tool and its methodology are also generalizable to an entire set of information-based risk assessment applications. As of this writing, the Assessor Tool has not yet been validated in a real-world setting. As such, the tool is not yet generally available for download. However, the tool is available for prospective users on a trial basis. Instructions for requesting a copy of the Assessor Tool can be found in the Preface. The users' manual for the Assessor Tool is available in a companion document (see Fleishman-Mayer, Arena, and McMahon, 2013).

The Assessor Tool Offers an OSD-Level Valuation of Program Risk

The Assessor Tool offers a valuation that is different from detailed engineering reviews. The team reviewed other acquisition risk assessment methods and tools in use or under development. While designed on sound risk management principles, each method and tool were technically focused. This approach makes a quick and useful OSD-level valuation of risk and programmatic effectiveness difficult to derive. The Assessor Tool is designed for those staff involved more generally with weapon systems acquisition who need access to a systematic method of determining a program's ability to meet its goals and manage risks, and to provide one basis to report on the success of the department's compliance with system integration risk management as directed by WSARA.

[1] Weapon Systems Acquisition Reform Act of 2009, 2009.

The Assessor Tool Design Is Based Upon OSD-Level Assessment Questions and Utility Theory

The calculations and assumptions existing within the Assessor Tool are based on expected utility methods. The methodology assumes that a set of knowledge-based standards has been developed against which to measure program risk and that a risky outcome may result if a question is not satisfied. The knowledge-based standards are based on the existence and completeness of DoD artifacts and checklists that would be readily available to an assessor at the OSD level. Questions that measure these standards are assigned (1) an importance (i.e., magnitude of the negative consequence that could occur in terms of program-related risks if the question-related standard was not addressed), and (2) a level of completeness (i.e., the level to which it has been ensured that the question-related standard has been met). The sum product of the importance and completeness for a set of assessment questions provides a measure of the relative risk of the program under question.[2] The Assessor Tool is set up to assess risk for a program with multiple phases. Thus, the functionality allows for two types of questions: phase-specific questions and global questions, which may include programmatic issues across a number of phases.

The risk score calculated by the methodology described in this document produces a *relative* risk score, which is also normalized to a range between 0 and 1. As more programs are evaluated using the methodology set out in this document, the relative risk values will begin to carry more meaning. Trends of relative risk scores for a number of programs can be compared to the cost and schedule growths and performance metrics of that program. This will provide for benchmarking and validation of the risk methodology.

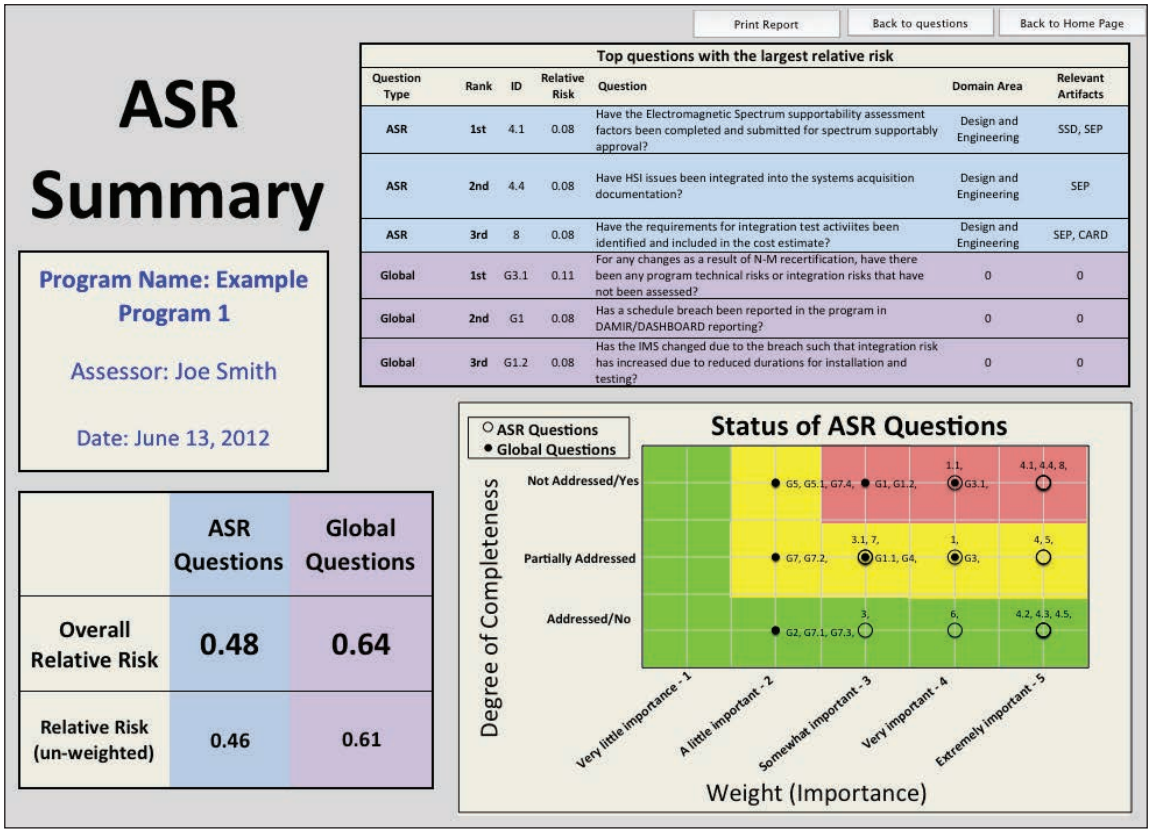
Figure S.1 is an example of the results tab for the Assessor Tool configured to measure integration risk. The relative risk results for both the program phase (ASR or Alternative Systems Review in the example) and global questions are shown prominently on the lower left side of the tab. In addition to these summary values, the upper right area of the results tab shows the three phase-specific and the three global questions that constitute the greatest relative risk for that program phase. Finally, the lower right area of the results tab includes a visualization of the relative risk for the phase-specific and global questions. Results can be summarized for each phase in the acquisitions process.

The Assessor Tool Can Be Adapted for Additional Risk-Related Assessments

The template provides a straightforward means of adapting the Assessor Tool for other applications. For example, the template and methodology could be considered for program office reporting during other acquisition reviews, such as for the OSD Defense Acquisition Executive Summary and Overarching Integrated Product Team reviews, and for adaptation into other program assessment tools, such as the Probability of Program Success tool. The fully developed integration risk Assessor Tool can also be tailored to insert user-determined review elements that are specific to previously identified technical or integration risk issues. For example, if the Under Secretary of Defense for Acquisition, Technology, and Logistics formally directs a sepa-

[2] Since the risk score is relative, it is only relevant in the context of other risk scores calculated by the same methodology and will require validation for it to become more meaningful.

Figure S.1
Assessor Results Page for Sample Run



NOTE: All abbreviations can be found in the Abbreviations list.

RAND *RR262-S.1*

rate review of a subsystem, such as a radar or aircraft engine under development, a user can tailor specific questions in the Assessor Tool to capture integration risk for that subsystem. In this sense, the Assessor Tool may be aligned to system integration risk areas identified at any point in the acquisition process.

Acknowledgments

The authors would like to thank Brian Sauser and RAND colleague Elliot Axelband for their thoughtful and constructive reviews of this document; Paul Deluca for his comments on an earlier draft of the report; and Kate Giglio for her editing, reorganization, and additions to the report.

Abbreviations

ADM	Acquisition Decision Memorandum
AoA	analysis of alternatives
ASR	Alternative Systems Review
AT&L	Acquisition, Technology, and Logistics
CARD	Cost Analysis Requirements Description
CDD	Capability Development Document
CDR	Critical Design Review
CONOP	concept of operations
COTS	commercial off-the-shelf
CPD	Capability Production Document
DAES	Defense Acquisition Executive Summary
DAMIR	Defense Acquisition Management Information Retrieval
DIACAP	DoD Information Assurance Certification and Accreditation Process
DMSMS	diminishing manufacturing sources and material shortage
DoD	U.S. Department of Defense
DOT&E	Director, Operational Test and Evaluation
EMC	electromagnetic compatibility
EMI	electromagnetic interference
FoS	Family of Systems
FRP	Full-Rate Production
H, M, L	high, medium, low
HSI	human-system interface
ICD	interface control document

IEEE	Institute of Electrical and Electronics Engineers
IMS	Integrated Master Schedule
IPT	Integrated Product Team
IRL	Integration Readiness Level
IRR	Integration Readiness Review
KPP	key performance parameter
MDD	Material Development Decision
MS	milestone
N-M	Nunn-McCurdy
OIPT	Overarching Integrated Product Team
OSD	Office of the Secretary of Defense
OV	operational view
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PESHE	programmatic environment, safety, and occupational health evaluation
POPS	Probability of Program Success
PRR	Production Readiness Review
SE	systems engineering
SEP	Systems Engineering Plan
SI	system integration
SoS	system of systems
SFR	System Functional Review
SRL	system readiness level
SRR	system requirements review
SSD	Spectrum Supportability Determination
SUBSAFE	Submarine Safety Program
SVR	system verification review
TDS	Technology Development Strategy
TEMP	test and evaluation master plan
TRL	Technology Readiness Level

TRR	Test Readiness Review
WSARA	Weapon Systems Acquisition Reform Act

CHAPTER ONE

Introduction

On May 22, 2009, President Obama signed into law the Weapon Systems Acquisition Reform Act (WSARA) to improve program costs and schedules associated with the delivery of major weapon systems. Some of the oversight changes called for by WSARA depend on a program team's ability to measure and manage the various risks associated with system integration (SI). Because SI may be influenced by all elements of the acquisition process, there exists a wide range of sources for SI risk. At any point, problems with hardware or software, design maturity, timely funding, test plan execution and personnel, facilities, and supplier capabilities can negatively affect program cost, timelines, and performance goals. Historically, integration risks at various phases of the acquisition process have contributed in part to program delays and cost overruns. In response, the U.S. Department of Defense (DoD) has worked toward improving defense program management overall through program and contractor-level risk management practices (DoD, 2006).

Large defense programs can have many technical, legal, and political consequences. Thus, there are many stakeholders across DoD who need to identify the risks associated with DoD's overall weapons programs, as well as the individual technology projects within a program. To date, personnel from the Office of the Secretary of Defense (OSD) who have been more generally involved with weapon systems acquisition—but not necessarily involved with individual programs—have had no access to an OSD-level systematic method of determining a program's ability to meet its goals, or to monitor the success of the defense sector's compliance with WSARA over the acquisition lifecycle. The methods currently available to OSD personnel are too technically focused and are relevant only to personnel who have detailed knowledge at the individual program level.

The Excel information-based risk tool (referred to as the "Assessor Tool," or "tool" for short, for the remainder of the report) described in this document is designed to assist the DoD acquisition community in assessing weapon SI risk in accordance with WSARA. The package offers an OSD-level approach to the evaluation and measurement of SI risk. That is, it is meant for assessors, such as OSD personnel, who may not be especially familiar with the specific program under evaluation but still may need to make judgments about the program's risk. The tool is a custom-designed software package in Excel that allows for easy accessibility of an OSD-level audience. Other systems engineering (SE) risk management software tools, such as a COTS (commercial off-the-shelf) SE tool (e.g., Lebron, Rossi, and Foor, 2000), may not be appropriate or easily available for this audience. While potentially not unique, the tool is tailored specifically to OSD personnel, allowing for its ease of use.

The Assessor Tool, developed by RAND researchers, is based on a tractable and comprehensive set of questions that can help evaluate integration risk at each point in the acquisi-

tion process. More specifically, the tool enables users to see how well integration risk is being managed by providing a standards-based valuation of integration issues that can lead to cost growth, schedule growth, and program performance shortfalls. These standards are based on the existence and completeness of DoD artifacts and checklists that would be readily available to an assessor at the OSD level. As requested by the OSD sponsor, we developed the tool and its methodology to help OSD-level acquisition professionals address these potential risks to major programs; early identification and reconciliation of SI issues as mandated by WSARA can reduce the likelihood and magnitude of the complications that frequently affect major weapons acquisition programs (Conrow, 1995). While we describe the Assessor Tool and its methodology in terms of their appropriateness for major weapon systems acquisitions analysis, it should be noted that both are also generalizable to an entire set of OSD-level information-based risk assessment applications.

In the remainder of this chapter, we describe the risks specific to integration activities during the weapon systems acquisitions process. We also discuss several recent attempts to meet the need for an evaluation of the integration risks that can result in higher costs, schedule delays, and questionable performance over the life of a program.

Integration Issues During the Acquisition Process Pose Significant Risk

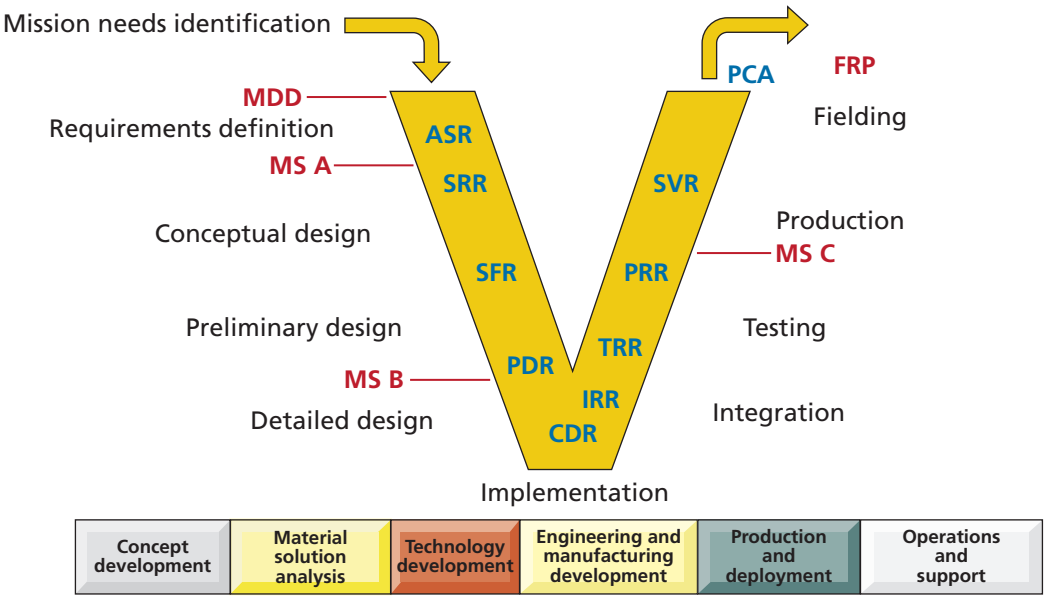
The acquisition of major weapon systems follows a prescribed formal process that typically spans about ten years from concept development to system employment for initial operational capability. Such systems involve many interdependent subsystems, components, and elements and involve the coordinated efforts of multiple defense industry and military participants. One example of the engineering community's formal definition of *system* underscores the interdependencies and coordination involved:

> [A system is an] arrangement of elements [people, products (hardware and software) and processes (facilities, equipment, material, and procedures)] that are related and whose behavior satisfies customer/operational needs, and provides for the life cycle sustainment of the products (IEEE, 2005).

A holistic management and engineering approach is needed to manage these interdependencies and coordination activities. The discipline of SE was developed for this purpose. It is a process-oriented means of designing a system that meets the needs of the user while minimizing the risks related to system performance and cost and schedule overruns.

For DoD, SE processes apply across the acquisition life cycle and are the set of overarching processes that a program team applies to design and implement an operationally effective and suitable system for a stated capability need. The approach is both interdisciplinary and iterative and involves a structured, disciplined, and documented technical effort. The application of a rigorous system engineering discipline is paramount to the DoD's ability to meet the challenge of developing and maintaining needed warfighting capability (Defense Acquisition University, 2011). Figure 1.1 depicts the SE process as commonly represented by a "V." The V is superimposed with the defense acquisition phases, such as alternative systems review (ASR) and system requirements review (SRR), as well as the checkpoints the program will need to pass (referred to in the V as Milestone A (MS A), MS B, etc.).

Figure 1.1
System Engineering "V" and the Defense Acquisition Process



NOTE: All abbreviations can be found in the Abbreviations list.

RAND *RR262-1.1*

The "V" represents the life cycle of a system (or program that realizes the system) beginning with "Mission needs identification" in the upper left corner, following down to "Implementation" and then returning up again to "Fielding." The left side of the V portrays a top-down design that occurs as user requirements are initially assigned at a system level down to lower-level components. The right side of the V represents a bottom-up process, showing the realization from lowest-level components to higher assemblies to achieve the complete system (Defense Acquisition University, 2011). While there are many ways to interpret and portray the V for SE, we chose the one shown in Figure 1.1 after discussions with Acquisition, Technology, and Logistics (AT&L) because it is a top-level, generalizable configuration that allows for the overlay of the DoD acquisition process.

Each step of the process may have both common and specific sources of risks associated with that phase.[1] While the physical integration and system testing generally occurs at a relatively late phase in the overall SE process, integration activities pose multiple risks that can occur throughout a program's acquisition process. Thus, a distinction is necessary here between the integration phase of the SE process and the integration risk that is the focus of the methodology presented in this report. During the integration phase of the SE process, lower-level system elements are integrated into higher-level system elements in the physical architecture (Defense Acquisition University, 2011). The integration activities that are the focus of this methodology include the integration of lower-level system elements into higher-level elements but, in addition, include activities related to integration of hardware, software, products,

[1] We recognize that the SE process is inherently iterative; if one step of the process is not fulfilled, this may require returning to multiple previous steps.

services, business processes, and human systems (Grady, 1994; Jain, Chandrasekaran, and Erol, 2010).

Integration risk has been defined as a measure of future uncertainty in the ability or inability to achieve program objectives within costs, schedule, and technical performance parameters due to issues related to integration (Defense Acquisition University, 2008). Early identification of integration risks is critical but challenging. Integration difficulty is often underestimated, while the maturity of items that require integration is simultaneously overestimated. Furthermore, there are many components in the SE process that must all be coordinated and evaluated for integration risk. The result for government programs (e.g., DoD and NASA) is often nontrivial cost and/or schedule growth, while performance degradation is typically small (Conrow, 1995). Early identification of integration risk can significantly reduce these cost and schedule growths.

Other Risk Measurement Approaches Are Proposed in the Literature

Integration risks not only need to be identified, but they also need to be assessed for the significance of each risk in terms of its likelihood and consequences on the acquisition program's cost, schedule, and ability to meet the performance needs. This integration risk assessment can take many forms, but in general it is a systematic process for identifying and evaluating integration-related events (i.e., possible risks and opportunities) that could positively or negatively affect the achievement of a program's objectives. Such assessments may have the greatest impact if carried out early, when an agency can more easily alter its acquisition plans and strategy to manage and control the identified risks (DoD, 2006).

Several researchers have proposed approaches to assessing SI risk. We briefly describe these approaches as well as their capability to provide an OSD-level valuation of program performance at the integration level.

Service Technical Reviews

An overall risk assessment approach used by the services at the OSD executive level is a checklist process of questions tailored to different acquisition phases.[2] These reviews are used at certification events (e.g., Preliminary Design Review [PDR] and Critical Design Review [CDR]) and cover the whole program scope (not just SI issues). These checklists have typically been implemented in spreadsheet tools and are used to highlight areas of potential risk or noncompliance. For example, a question about testing requirements from the DoD Preliminary Design Review Checklist is, "Are test requirements tied to verification requirements, and is there a method to ensure traceability of test requirements to the verification requirements?" The implication is that a negative response to the question would indicate program risk with respect to the test plan and that the requirements are not fully understood in terms of technical performance.

The checklist approach is already in use by the services, and thus there is an advantage to leveraging the process. There are numerous questions that specifically address issues related

[2] See for example, U.S. Air Force, 2008; and Naval Air Systems Command, 2008. Note that at the weapon system program office level, a more detailed risk discussion is conducted. Here, we refer to the OSD-level reviews that are conducted only annually or bi-annually.

to SI. Using a subset of the checklists to evaluate SI risk would not place additional burden on OSD personnel tasked to perform the evaluation. Moreover, the tools already exist such that minimal development would be required. However, these checklist approaches are technically focused and therefore may miss some of the important management aspects of integration risk. Also, because each service approaches the risk assessment differently, the reporting is not comparable. Therefore, some standardization would need to take place to adapt these checklists to DoD-wide application.

Layered Matrix Approach

This approach has evolved over the past few years and has been proposed by OSD as a possible way to measure SI risk.[3] The layered approach is a combination of qualitative checklists and quantitative metrics for tacking SI risk. The "layered" portion comes from the different aspects of integration risk that the method evaluates: functional, physical, management, disciplines, and system-of-systems (SoS) integration.[4] For each layer, there is a matrix of issues (or risk areas, both qualitative and quantitative) tracked against different technical deliverables (such as the Capability Development Document [CDD], functional specifications, and the Capability Production Document [CPD]).

The main advantage of this approach is that it is comprehensive, focused on SI issues, and able to track trends over the program life cycle. However, this approach is difficult to implement in a uniform model and is quite labor intensive for the assessor.

Integration Readiness Levels

In a series of papers and presentations, Sauser et al. explore the concept of a "system readiness level" (SRL) index as a way to evaluate overall system development risk.[5] Their approach is to define a risk scale that leverages the Technology Readiness Level (TRL) scale that is in wide use in DoD as a measure of technology risk. The SRL is a combination of the TRL for each technology and an Integration Readiness Level (IRL) scale for each interface between the various technologies. The SRL index is a combination of both the TRL and IRL measures for the system that reflects the degree of interconnectedness between the various technologies.

In defining the IRL scale, the authors adapted a scale used in computing networking. This adapted scale is reproduced in Table 1.1.

The IRL approach to integration risk assessment is already in use in DoD. However, DoD does not formally require this approach. Assigning IRLs to every interface would allow for a documented and reproducible way to review the integration risk of the system. It is also a relatively simple scale to assess. The further advantage is that it can be combined with technology risk (the TRLs) to assess an overall system risk. However, this approach requires one to assess each interface and determine an overall system network of interactions. Thus, this approach might be time consuming to implement on a very complex system.

---

[3] See, for example, Thompson et al., 2009, 2010; and Kranz, 2009.

[4] Earlier versions of this approach focused on layers that are more functionally focused (see Kranz, 2009).

[5] See, for example, Sauser et al., 2006a, 2006b, and 2010.

Table 1.1
Integration Readiness Level Scale

IRL	Definition
9	Integration is ***mission proven*** through successful mission operations.
8	Actual integration completed and ***mission qualified*** through test and demonstration, in the system environment.
7	The integration of technologies has been ***verified and validated*** with sufficient detail to be actionable.
6	The integrating technologies can ***accept, translate, and structure information*** for its intended application.
5	There is sufficient ***control*** between technologies necessary to establish, manage, and terminate the integration.
4	There is sufficient detail in the ***quality and assurance*** of the integration between technologies.
3	There is ***compatibility*** (i.e., common language) between technologies to orderly and efficiently integrate and interact.
2	There is some level of specificity to characterize the ***interaction*** (i.e., ability to influence) between technologies through their interface.
1	An ***interface*** (i.e., physical connection) between technologies has been identified with sufficient detail to allow characterization of the relationship.

SOURCE: Sauser et al., 2010.

Other Methods Lack OSD-Level Valuations

We explored the methods summarized above for use in an integration risk assessment tool. However, based on multiple briefings with OSD AT&L, we concluded that these other methods and tools in use or under development are likely too detailed and technically focused for use by acquisition leaders to quickly gain an OSD-level valuation of SI and programmatic risk. Accountability in these methods is presupposed to primarily rest with one individual, the program manager, but also with the Program Executive Officer or Service Acquisition Executive, the team of responsible individuals who guide the program toward completion, as well as the groups of contractor personnel involved with the program's technology projects. Personnel working within and with the wider DoD acquisitions community need to address a wide range of concerns that fall under the umbrella term "risk management." These concerns include risk planning for future programs and assessing and monitoring DoD-wide acquisition performance through a program-by-program understanding. An OSD-level approach to evaluate and measure SI risk is needed. Such a tool must be largely, but not exclusively, a WSARA-compliance assessment that highlights the ways in which risks unique to the integration phase are being managed.

Organization of This Report

In the following chapters, we describe the methodology and assumptions underlying the Assessor Tool and demonstrate its analytical procedures through example. Chapter Two presents a detailed description of the underlying theory behind the information-based risk assessment methodology and Assessor Tool. Chapter Three provides an example application of the Assessor Tool that assesses compliance risk associated with SI activities during the weapon systems

acquisition process. Here, we describe the interactive interfaces of the tool and its output. Chapter Four provides a final discussion and thoughts for further applications of the tool and methodology. Finally, Chapter Five briefly summarizes the purpose of the report.

CHAPTER TWO

Assessor Tool Methodology

This chapter describes the analytical and research basis of the Assessor Tool. In the process of developing the Assessor Tool, we held discussions with OSD AT&L for comments and suggestions as to how to leverage previous work in this area. Suggestions were incorporated into the methodology and design of the Assessor Tool.

Assessor Tool Design Is Based upon OSD-Level Assessment Questions

The Assessor Tool and its information-based risk assessment methodology are built upon a framework of OSD-level assessment questions. The methodology assumes that questions are general enough that OSD-level program assessors who are not intimate with the program and conduct program assessments only infrequently can answer them with the right set of documentation and reported data and metrics. Thus, the questions generally measure knowledge-based standards that are established by existing DoD program assessment checklists or other artifacts. In this way, the linking of questions to established documentation allows for a level of traceability, verifiability, and objectiveness.

There are certainly standards, other than existing DoD checklists and artifacts, against which integration risk could be measured. Indeed, some are highlighted in the review in the first chapter. The standards for this methodology were chosen after discussions with OSD AT&L, as the desire was to use a set of DoD-based measures that could be evaluated with ease by the assessor.

Utility Theory Provided Methodological Framework

The computations underlying the assessment of questions in the Assessor Tool are based on the concept of *utility*. Utility theory states that a rational person makes decisions between a set of options by choosing the option that provides them with the most utility (von Neumann and Morgenstern, 1947; Savage, 1954). This concept is often extended to consider options with uncertain or risky outcomes in a theory named *expected utility theory*. Under this concept, an uncertain option may have multiple possible outcomes, each with different expected probabilities of occurrence. The expected utility for the option is the sum-product of the probability and the utility for each outcome (von Neumann and Morgenstern, 1947; Savage 1954).

The calculations and assumptions existing within the tool are based on expected utility methods. The methodology assumes that a set of knowledge-based standards has been devel-

oped against which to measure program risk and that a risky outcome may result if a question is not satisfied. These outcomes are treated as analogous to the outcomes in expected utility theory. Each outcome, and in turn its related assessment question, are assigned (1) an importance, analogous to utility value, and (2) a level of completeness, analogous to a probability. For this methodology, importance of the question is defined as the magnitude of the negative consequence that could occur in terms of program-related risks if the question-related standard was not addressed. Completeness is defined as the level to which it has been ensured that the question-related standard has been met. Thus, the sum-product of the importance and completeness for a set of assessment questions provides a measure of the relative risk of the program under question.

There are certainly risk methodologies, other than those based on utility theory, that could have been useful for evaluating integration risk. Based on discussions with AT&L, the desired output of such an effort was a "risk score." This desire, along with the need to use DoD standards-based questions, prompted us to choose methods based on utility theory that could be straightforwardly translated to address the integration risk evaluation.

Assessment Is Structured by Global and Phase-Specific Questions

The tool is set up to assess risk for a program with multiple phases. Thus, the functionality allows for two types of questions:

- **Global questions** may include programmatic issues across a number of phases. Examples of global questions in the integration risk Assessor Tool include "Has a major subsystem or technology vendor failure occurred or vendor been disqualified or changed?" and "Have funding changes increased integration risk due to inadequate funds for testing or resulted in delays for technology insertion?"
- **Phase-specific questions** are tied to "relevant artifacts" or documentation that an OSD-level assessor can use to objectively answer the question. For example, the integration risk Assessor Tool includes questions such as, "Has a Systems Engineering Plan [SEP] been updated to reflect the changes in the program baseline since [the previous program phase of] ASR?" and "Does the program plan reflect adequate time allotted for test and evaluation?" Both questions reference appropriate documentation (e.g., a SEP).

Both global and phase-specific questions were designed in ways that provide a reference to relevant artifacts; this allows for the methodology to be relatively traceable, verifiable, and objective.

Within the phase-specific questions specifically, the methodology further organizes them into a hierarchy. Some questions may be at a very high level, while others may be more specific or focus on a particular area. The high-level questions are designated in the tool as "primary" questions. Related and more detailed questions are designated as "secondary" questions and grouped with the appropriate primary question. For example, the primary question, "Has a Systems Engineering Plan been updated to reflect the changes in the program baseline since [the previous program phase of] Alternative System Review (ASR)?" contains a number of secondary questions, including "Have the interface control specifications been clearly defined and put under configuration control?" and "Have appropriate modeling and simulation tools been

identified?" Both of these secondary questions include additional important details related to the primary question.

The advantage of the primary-secondary grouping structure is that one can reduce the number of weights the user must specify (as discussed further on, only primary questions are weighted in terms of importance). Also, if the assessor believes a primary question is not applicable to the program under assessment, the secondary question(s) under this primary question are also considered not applicable. Thus, the primary questions serve as a screen for the secondary ones.

In addition to tagging questions to accessible documentation, questions are designed to be answered in a consistent format. Namely, phase-specific questions are framed such that they can be answered by an assessment of "Not Addressed/Partially Addressed/Addressed." Global questions are framed to be answered in the form of "Yes/Somewhat/No" or "High/Medium/Low," where the "Yes/High" end of the scale results in a score that increases the overall relative risk. This is discussed further below in a section on question responses.

Answers to Questions Are Weighted According to a Unique Risk Scoring Method

As indicated previously, the information-based risk assessment methodology adopted for the tool requires two assignments for each question: (1) the question's importance, and (2) its level of completeness. These two assignments are combined to result in a numerical risk score. In this section, the baseline assumptions and scoring rules that dictate the numerical risk score results are described.

Weightings by Question Importance

In this analysis, the importance of each information-based question is treated as a weighting, relative to other questions. Thus, questions of greater importance will be weighted more heavily, causing the overall risk to be more sensitive to whether that question has been addressed. All primary questions are assigned a rating between 1 (Very Little Importance) and 5 (Extremely Important).[1] As indicated previously, this rating signifies the consequence this question will have on the overall risk for the program under evaluation if the question were to be answered, "not addressed." Secondary questions receive the same importance rating as their corresponding primary question. These importance ratings are converted to question weights through a normalization[2] of all question weights within a program phase. Global questions are normalized separately from the program-specific questions.

Assessments of Question Completeness

Questions are also assessed for their level of completeness, such that the less a question has been addressed, the more it will contribute to risk. All primary and secondary questions are

[1] We chose to use "Very Little Importance" over the more standard Likert Scale anchor of "Not at All Important" because within the context of the checklist questions, if one question was unimportant, it would already be marked as "Not Applicable."

[2] Dividing each value by the sum of the entire set or values will normalize each value within a set. The set of normalized values will then sum to 1.

assessed separately for level of completeness. Questions may be answered with the following responses and corresponding scores: (a) Not addressed/No/High, which is scored as 1; (b) Partially addressed/Partially/Medium, scored as 0.5; and (c) Addressed/Yes/Low, scored as 0. An additional response of "Not applicable" is included for questions that do not apply to the particular program under evaluation.

Risk Scoring Method Omits "Not Applicable" Answers

The one exception to the risk scoring rules iterated above is for questions answered as "Not applicable." "Not applicable" questions are completely omitted from the relative risk score for a program phase. They receive a score of 0 and are also automatically weighted as 0. Since the question weighting is normalized over the entire set of questions, when one question is omitted, all other questions within the program phase will automatically be given more importance. When a primary question is answered as "Not applicable," the secondary questions will automatically be scored as "Not applicable," while secondary questions that are answered as "Not applicable" will not dictate the completeness of the corresponding primary question.

Calculations Are Formulated at the Program-Phase Level

The relative risk for each question is calculated as the product of the question's normalized weight and level of completeness. Relative risks are additive and are rolled up to the program phase level. Global questions and phase-specific questions are summed separately for two relative risk scores. An unweighted relative risk score is also calculated to present a relative risk when assuming all questions are of equal importance. This unweighted score may be useful to the assessor to better understand the sensitivity of the relative risk score to the weights chosen. There is also a substantial literature that suggests unweighted linear models (such as the additive expected utility function used in this method) perform better than weighted linear models (Dawes, 1979; Dana and Dawes, 2004).

Since the weightings are normalized at the phase level, all phase-level relative risk scores (i.e., weighted and unweighted; phase-specific and global) will be in the range between 0 and 1. That is, if all questions within a phase are answered as "Addressed," then the relative risk score of that phase will be 0. Similarly, if all questions within a phase are answered as "Not Addressed," the relative risk score of that phase will be 1. These risk scores hold regardless of the weights given to the individual questions.

These calculations are formalized below at the program phase level:

- Let n be the number of primary questions, and let m_i be the number of secondary questions within the i^{th} primary question.
- Let x_i be the assigned importance for the i^{th} primary question in a program phase, such that $i = 1, 2, \ldots, n$.
- Let p_i be the level of completeness for the i^{th} primary question in a program phase, such that $i = 1, 2, \ldots, n$. And let $s_{i,j}$ be the level of completeness for the j^{th} secondary question within the i^{th} primary question, such that $j = 1, 2, \ldots, m_i$.
- Then the normalized weight, w_i, of the i^{th} question can be found:

$$w_i = \frac{x_i}{\sum_{i=1}^{n} x_i}, \tag{2.1}$$

where $x_i = 0$ for all corresponding p_i = "Not applicable."

- When calculating an unweighted risk score, normalized weights are calculated as:

$$w_i = \frac{1}{\sum_{i=1}^{n} x_i}, \tag{2.2}$$

where $x_i = 0$ for all corresponding p_i = "Not applicable."

- Then the relative risk, r, for the questions within a program phase can be found:

$$r = \sum_{i=1}^{n} \sum_{j=1}^{m_i} w_i \left(p_i + s_{i,j} \right). \tag{2.3}$$

Scores Should Be Interpreted as Relative, Not Absolute

The risk score calculated by the methodology described in this document produces a *relative* risk score. That is, the relative risk score is only relevant in the context of other risk scores calculated by the same methodology. For instance, if the relative risk of the program at one program phase is 0.40 and the previous program phase had a relative risk of 0.80, then the program's risk would be considered to decrease by an order of two from one phase to the next (0.80 to 0.40). Alone, the 0.80 and 0.40 values have no meaning, but when compared to each other, risk can be assessed as a program moves through its phases. Relative risks may also be compared between programs for the same program phase.

As more programs are evaluated using the methodology set out in this document, the relative risk values will begin to carry more meaning. Trends of relative risk scores for a number of programs can be compared to the cost and schedule growths and performance metrics of that program. This will provide for a benchmarking and validation of the risk scale. Validation may be especially important given that the underlying assessments (i.e., level of completeness and importance) of the risk scale are subjective. Subjective assessments of this kind tend to be human-intensive and potentially error-prone (Sauser et al., 2008). Validation will ensure that the risk score will provide quality information to inform OSD personnel decisionmaking.

CHAPTER THREE

An Example Application of the Risk Assessor Tool

In this chapter, we present an example application of the Assessor Tool. The test case calls for an assessment of compliance risk associated with SI activities during the weapon systems acquisition process. That application of the methodology and tool as presented here would permit both individual program and portfolio characterization of weapon systems integration risk. As discussed in the first chapter, this is part of the annual reporting required by WSARA.

Questions in the Test Case Are Based upon Existing DoD Program Assessment Checklists

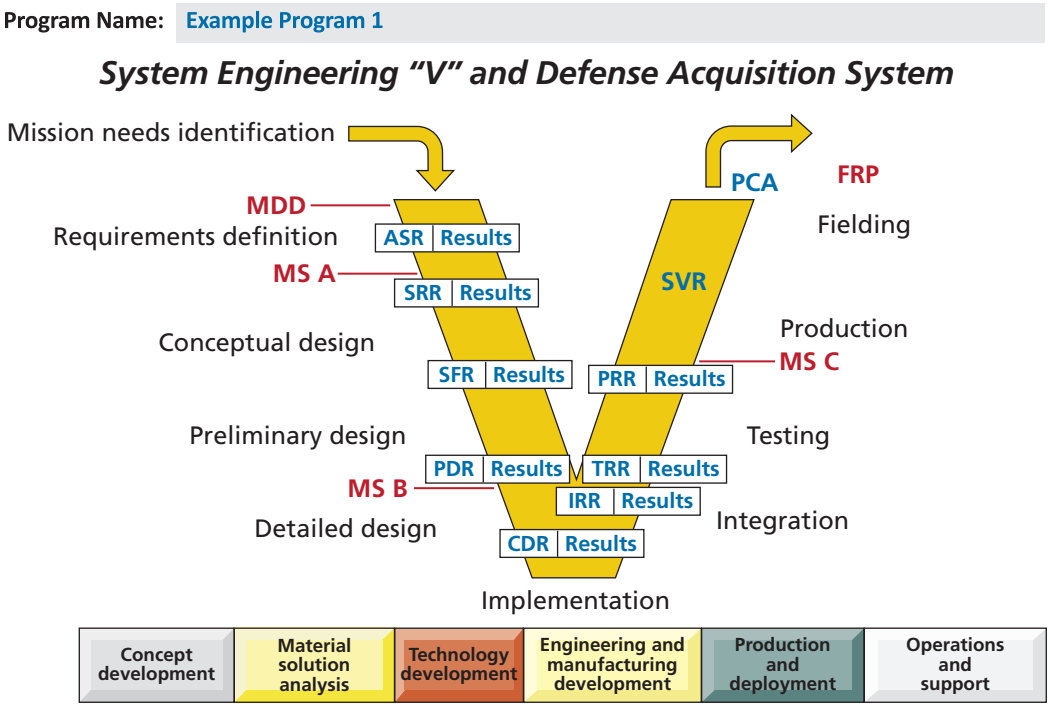
Based upon discussions with AT&L, we drew upon existing material and checklists already in use by DoD and the services to develop a set of questions relevant to integration risk. These organizations already had established processes for reviewing programs at each defense acquisition phase (e.g., CDR and PDR). By leveraging existing questions for each of these program phases, it would be easy for all parties to conduct an integration risk assessment.

Questions were further organized into domain areas (e.g., design and engineering, program management, logistics) and assigned as either "primary" or "secondary." Finally, each question was tagged for the relevant artifacts or documents (e.g., interface control documents [ICDs], SEP, test and evaluation master plan [TEMP], etc.) that could be associated with that question. That is, most integration risk questions can be evaluated against these relevant documents to determine if the knowledge-based standard defined in the question has been satisfied. Assigning a reference document for each question allows the methodology to be reviewed by an OSD-level assessor who may not be particularly knowledgeable about the specific weapon system being evaluated. Referencing documentation in this way allowed for a level of traceability to the questions' responses.

The Assessor Tool Is Designed According to Systems Engineering V

The Assessor Tool includes an overview tab (see Figure 3.1), and, for each program phase that aligns to steps in the SE "V," there is one tab each for assessor input and for results reporting. The Overview Tab, shown in Figure 3.1, acts as the home page for this Assessor Tool. At the top of the page, a program name can be entered that will be carried through to each of the input and output tabs. Buttons to each program phase (referred to as a technical review by DoD) are overlaid upon the SE "V," which is a framework used in acquisition programs. The

Figure 3.1
Overview Tab of the Assessor Tool



NOTE: All abbreviations can be found in the Abbreviations list.
RAND *RR262-3.1*

first button is named for the program phase. It will take the user to the assessment questions for that program phase. The second button, labeled "Results," will take the user directly to the results tab (for the corresponding program phase), which summarizes the assessor's input into its corresponding assessment question tab.

The User Customizes the Assessor Input Forms

Table 3.1 displays the top half of the assessment questions for a program at the ASR program phase. At the top, the program name is shown as entered on the overview tab. Following to the right, the page allows the assessor to enter his or her name and the date of the assessment, which will be carried onto the results tab. Questions are listed in rows, shown in the second column, with the first column presenting the questions' associated ID number. ID numbers for primary questions are listed as whole numbers, with their secondary questions indented and listed as decimals (e.g., 1.1, 1.2, and 2.1). The fourth and fifth columns, respectively, present the relevant artifacts upon which to assess that question and the question's domain area.

Assessor inputs are found in the sixth and seventh columns, labeled "Importance" and "Assessment." Each column includes drop-down menus for the user's input. The drop-down menu for Importance presents a scale from 1 (Very Little Importance) to 5 (Extremely Important). Since secondary questions adopt the importance of their primary question, there are no drop-down menus provided for the importance of secondary questions. The drop-down

menu for Assessment presents a scale with 0 (Addressed), 0.5 (Partially Addressed) and 1 (Not Addressed). A "Not applicable" option is also available in this drop-down menu.

Columns eight and nine present the output for the Assessment and Importance columns, respectively. The Assessor Tool converts these values, as indicated in Chapter Two, to the relative risk and unweighted relative risk shown in the final two columns. Also as indicated in Chapter Two, relative risk is additive and is rolled up for all phase-specific assessment questions in this program phase tab. The total relative risk value is highlighted in yellow at the bottom of Table 3.1. Overall relative risk scores for any program phase are on a scale from 0 (very little relative risk) to 1 (very high relative risk).

Finally, every program phase can be customized with questions applicable to the program under consideration. The blank rows at the bottom of the ASR assessment questions tab shown in Table 3.1 allow for this customization. When the assessor fills out the ID and question, any questions added will automatically be incorporated into the relative risk in the same manner as the other questions.

Table 3.2 displays a similarly structured set of questions, which are found at the bottom of the ASR tab of the Assessor Tool. These are the global questions, which do not change between program phases. While these global questions are the same on each assessor input tab, they may be assessed differently at each program phase. All columns shown in Table 3.2 are analogous to those in Table 3.1. Additionally, there are four blank rows provided to allow for additional questions to be added as applicable. The "Total Global Relative Risk" score is the sum of the relative risks for all global questions. Buttons shown below Table 3.2 allow the user to move directly onto the corresponding results page or to go back to the home page.

Assessor Tool Summarizes Results in Three Ways

Figure 3.2 displays the results tab that corresponds to the ASR program phase questions shown in Tables 3.1 and 3.2. The ASR results tab carries over the program name, entered on the overview tab, and the assessor name and date from the ASR assessor input tab. The relative risk results (weighted and unweighted) for both the ASR program phase and global questions are shown prominently on the left side of the tab. In addition to these summary values, the results tab shows the three ASR and three global questions that constitute the greatest relative risk for that program phase. These results report the questions that influence the relative risk score the most, and therefore, identify the areas that will need the most attention to reduce compliance risk of the program.

Finally, the results tab includes a visualization of each of the ASR and global questions in a risk cube–type format. Acquisition program risk is managed and presented in various ways prescribed in acquisition governance directives with such a risk cube type format being common and, in fact, incorporated into the formal program manager program reporting requirement into the Defense Acquisition Management Information Retrieval (DAMIR) system. The importance of the questions increase along the x-axis, while the y-axis presents those questions that are considered to be less complete/not addressed as higher on the scale. Questions are plotted on the graph by the assessor inputs. Global questions are shown as open circles, while phase-specific questions are shown as closed circles. Question ID values for the ASR and global questions are shown above and to the right of the circles, respectively. In this way, the format mimics that of a risk cube, where the riskiest questions are in the upper right

Table 3.1
Sample ASR Assessor Data Entry Phase

Program Name: Example Program 1 Assessor Name: Joe Smith Date: 6/13/2012

ID	Question	Technical Review	Relevant Artifacts	Domain Area	Importance	Assessment	Score	Weight	Relative Risk	Relative Risk (un-weighted)
1	Does the CONOPs identify the relationships, dependencies and desired interfaces envisioned between new or upgraded systems and other existing or planned systems?	ASR	CONOPs, OV-1, TDS	Design and Engineering	4 - Very Important	Partially Addressed	0.5	4	0.04	0.04
1.1	Does the operational views (OV-1) frame the operation concept (what happens, who does what, in what order, to accomplish what goal) and highlight interactions to the environment and other external systems?	ASR	OV-1	Design and Engineering		Not Addressed	1	4	0.08	0.07
2	Does the Initial Capabilities Document explain how the required capabilities are dependent upon interface with other systems? Does it also define interoperability requirements of the capabilities in terms of high-level Operational View (OV-1)?	ASR	Initial capabilities document, OV-1	Design and Engineering	2 - A little important	Not Applicable	0	0	0.00	0.00
3	Are the system and/or FoS/SoS reliability, maintainability, availability performance parameters identified?	ASR	SEP, initial capabilities document, CONOPs, OV-1	Logistics and Maintainability	3 - Somewhat important	Addressed	0	3	0.00	0.00
3.1	Has a formal DMSMS program been established?	ASR		Logistics and Maintainability		Partially Addressed	0.5	3	0.03	0.04
4	Has a draft Systems Engineering Plan been Developed?	ASR	SEP	Program Management	4 - Very Important	Partially Addressed	0.5	4	0.04	0.04
4.1	Has the Electromagnetic Spectrum supportability assessment factors been completed and submitted for spectrum supportably approval?	ASR	SSD, SEP	Design and Engineering		Not Addressed	1	4	0.08	0.07
4.2	Does the integrated architecture adhere to the DoD net-centric strategies?	ASR	Net Centric Data Strategy	Design and Engineering		Addressed	0	4	0.00	0.00
4.3	Is the system's architecture explicitly documented to the same level as the systems requirements? Does the architecture documentation describe the rationale for partitioning functionality and for placing key architectural attributes within or across a subset of architectural boundaries?	ASR	SEP	Design and Engineering		Addressed	0	4	0.00	0.00
4.4	Have HSI issues been integrated into the systems acquisition documentation?	ASR	SEP	Design and Engineering		Not Addressed	1	4	0.08	0.07
4.5	Does the program have a SoS engineering IPT?	ASR	SEP	Program Management		Addressed	0	4	0.00	0.00
5	Have software testing requirements been identified?	ASR	SEP, CARD	Test and Evaluation	5 - Extremely Important	Partially Addressed	0.5	5	0.05	0.04
6	Have the requirements for an integrated test facility been identified?	ASR	SEP, CARD	Test and Evaluation	4 - Very Important	Addressed	0	4	0.00	0.00
7	Did the AoA performance assessment adequately evaluate integration issues/FoS/SoS?	ASR	AoA	Design and Engineering	3 - Somewhat important	Partially Addressed	0.5	3	0.03	0.04
8	Have the requirements for integration test activites been identified and included in the cost estimate?	ASR	SEP, CARD	Test and Evaluation	3 - Somewhat important	Not Addressed	1	3	0.06	0.07
9		ASR			1 - Very Little Importance	Addressed	0	0	0.00	0.00
10		ASR			1 - Very Little Importance	Addressed	0	0	0.00	0.00
11		ASR			1 - Very Little Importance	Addressed	0	0	0.00	0.00
12		ASR			1 - Very Little Importance	Addressed	0	0	0.00	0.00
13		ASR			1 - Very Little Importance	Addressed	0	0	0.00	0.00
					Total ASR Relative Risk				0.46	0.46

NOTE: All abbreviations can be found in the Abbreviations list.

Table 3.2
Sample ASR Assessor Data Entry Phase, Global Questions

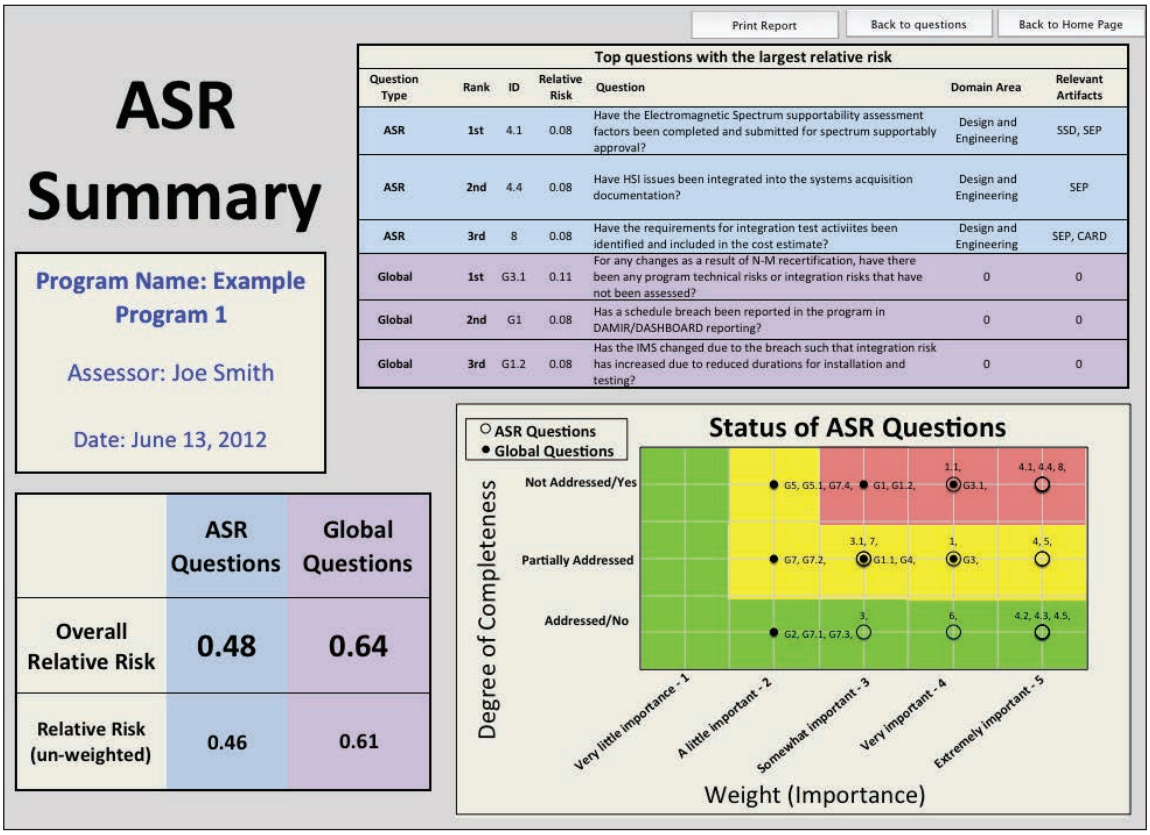
Program Name: Example Program 1 Assessor Name: Joe Smith Date: 6/13/2012

ID	Question	Technical Review	Relevant Artifacts	Domain Area	Importance	Assessment	Score	Weight	Relative Risk	Relative Risk (un-weighted)
G1	Has a schedule breach been reported in the program in DAMIR/DASHBOARD reporting?	ASR			3 - Somewhat important	Yes	1	3	0.08	0.07
G1.1	Was the schedule breach due to major system development, deliveries or production that increase integration risk?	ASR				Somewhat	0.5	3	0.04	0.04
G1.2	Has the IMS changed due to the breach such that integration risk has increased due to reduced durations for installation and testing?	ASR				Yes	1	3	0.08	0.07
G2	Have funding changes increased integration risk due to inadequate funds for testing or resulted in delays for technology insertion?	ASR			2 - A little important	No	0	2	0.00	0.00
G3	Has the program been identified for a Nunn-McCurdy breach?	ASR			4 - Very Important	No	0.5	4	0.06	0.04
G3.1	For any changes as a result of N-M recertification, have there been any program technical risks or integration risks that have not been assessed?	ASR				Yes	1	4	0.11	0.07
G4	Are there any technology risk issues identified in the most recent ADM that have not been addressed by the program?	ASR			3 - Somewhat important	Somewhat	0.5	3	0.04	0.04
G5	What is the DOT&E risk assessment for the program (H, M, L)?	ASR			2 - A little important	High	1	2	0.06	0.07
G5.1	Has any of the TEMP *not* been concurred and funded?	ASR				Yes	1	2	0.06	0.07
G6	Has a major sub-system or technology vendor failure occurred or vendor been disqualified or changed?	ASR			1 - Very Little Importance	Not Applicable	0	0	0.00	0.00
G6.1	What is the associated integration risk effect on the program (H,M,L)?	ASR				Medium	0	0	0.00	0.00
G7	Have all required certifications or the planning to achieve required certifications at the appropriate time been addressed?	ASR			2 - A little important	Some	0.5	2	0.03	0.04
G7.1	Information Assurance (e.g. DIACAP and NSA Cryptographic Certification) ?	ASR				All	0	2	0.00	0.00
G7.2	Interoperability (e.g. Net Ready KPP, Joint Interoperability Test Certificate)?	ASR				Some	0.5	2	0.03	0.04
G7.3	Spectrum Management (e.g. EMI / EMC Cert., Spectrum Cert.)?	ASR				All	0	2	0.00	0.00
G7.4	Safety (e.g. Airworthiness, SUBSAFE, PESHE)?	ASR				None	1	2	0.06	0.07
G8		ASR			1 - Very Little Importance	Yes	1	0	0.00	0.00
G9		ASR			1 - Very Little Importance	Yes	1	0	0.00	0.00
G10		ASR			1 - Very Little Importance	Yes	1	0	0.00	0.00
G11		ASR			1 - Very Little Importance	Yes	1	0	0.00	0.00
					Total Global Relative Risk				0.64	0.61

Results Back to Home Page

NOTE: All abbreviations can be found in the Abbreviations list.

Figure 3.2
Results Page for Sample Run



RAND *RR262-3.2*

hand corner. Since the relative risk measured by this methodology is generally equivalent to a compliance assessment, any question that has been addressed, as well as any question that is deemed to be of very little importance, is considered to be "green" on the risk cube.

CHAPTER FOUR

Further Applications

As demonstrated in the previous chapter, this Assessor Tool is appropriate for OSD-level information-based acquisition risk assessments. In addition, as we describe in this chapter, the tool has several other potential uses for the acquisitions community.

The Assessor Tool May Be Useful for Compliance Reporting

Using the integration risk application described in this report, the tool and methodology permit both individual program and portfolio characterization of weapon systems integration risk as part of the annual reporting required by WSARA. As programs are evaluated using the methodology set out in this document, trends of relative risk scores can be benchmarked against the cost and schedule growths and performance metrics of that program.

The Assessor Tool May Be Useful for Other OSD-Level Risk Assessments

While the tool and methodology were developed to assess SI risks on major programs, they are also generalizable to an entire set of information-based risk assessment applications. The tool could easily be tailored to insert user-determined review elements specific to previously identified technical or integration risk issues. For example, if a subsystem of a weapon system was a developmental radar or aircraft engine and OSD (AT&L) had formally directed separate review or reporting of the subsystem in an Acquisition Decision Memorandum, the user could tailor specific questions in the Assessor Tool to capture integration risk for that subsystem. In this sense, the tool may be aligned to SI risk areas identified at any point in the acquisition process.

Using the blank template of the tool, a user could adapt it to evaluate risk related to many other types of programs with documented knowledge-based standards in place. For example, the reproducible and documented tool could be considered for program office reporting during other acquisition reviews, such as the OSD Defense Acquisition Executive Summary (DAES) and Overarching Integrated Product Team (OIPT) reviews, and for adaptation into other program assessment tools, such as the Probability of Program Success (POPS) tool. “Pushing” out the methodology and tool would be required to enable program manager evaluation to be included as a template in the POPS format.

Further Validation May Enhance Usability of the Assessor Tool

Overall, the methodology and tool have many strengths, including being based on well-grounded theories, allowing for reproducibility and traceability, and the extensive flexibility to be used to evaluate risk for many different types of programs. Potential limitations include the need for a benchmarking and validation of the relative risk scores calculated by the tool. Therefore, potential future work could include the tool's validation by tracking its output against a program's performance. This would require that the Assessor Tool be connected to a database that could store the results from the tool. Performance metrics of the program could then be input into the database. Statistical tests could measure the strength and manner of the relationship between the relative risk values and performance metrics. Validation of the methodology and benchmarking of relative risk scores would strengthen the defensibility of the tool and improve its attractiveness for future use.

CHAPTER FIVE

Conclusion

This report presented a methodology and Assessor Tool that can facilitate an OSD-level information-based risk assessment for acquisition or other major programs. It described a generalizable form of the Assessor Tool, using the integration risk Assessor Tool as an example application. The reproducible and documented tool for integration risk assessment may be considered for program office reporting to meet WSARA compliance as well as for other acquisition reviews, such as the OSD DAES and OIPT reviews, and for adaptation into other program assessment tools, such as the POPS tool. As of this writing, the Assessor Tool has not yet been validated in a real-world setting. As such, the tool is not yet generally available for download. However, the tool is available for prospective users on a trial basis. Instructions for requesting a copy of the Assessor Tool can be found in the Preface. The users' manual for the Assessor Tool is available in a companion document (see Fleishman-Mayer, Arena, and McMahon, 2013).

References

Application Professionals, *XY Chart Labeler*, Version 7.1, not dated. As of March 25, 2013: http://www.appspro.com/Utilities/ChartLabeler.htm

Conrow, Edmund H., "Some Long-Term Issues and Impediments Affecting Military Systems Acquisition Reform," *Acquisition Review Quarterly*, Vol. 2, No. 3, Summer 1995, pp. 199–212.

Dana, Jason, and Robyn Dawes, "The Superiority of Simple Alternatives to Regression for Social Science Predictions," *Journal of Educational and Behavioral Statistics,* Vol. 29, No. 3, Fall 2004, pp. 317–331. As of March 20, 2013: http://www.jstor.org/stable/10.2307/3701356

Dawes, Robyn M., "The Robust Beauty of Improper Linear Models in Decision Making," *American Psychologist*, Vol. 34, No. 7, 1979, pp. 571–582. As of February 6, 2013: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.188.5825&rep=rep1&type=pdf

Defense Acquisition University, *Risk Assessment*, 2008. As of April 1, 2013: https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=df96b20d-4e88-4a61-bb35-898893867250

———, *Defense Acquisition Guidebook*, July 29, 2011. As of September 12, 2012: https://dap.dau.mil

Department of Defense (DoD), *Risk Management Guide for DOD Acquisition,* Sixth Ed., Version 1.0, August 2006. As of September 12, 2012: http://www.acq.osd.mil/se/docs/2006-RM-Guide-4Aug06-final-version.pdf

Fleishman-Mayer, Lauren A., Mark V. Arena, and Michael E. McMahon, *An Excel Tool to Assess Acquisition Program Risk*, Santa Monica, Calif.: RAND Corporation, TL-113-OSD, 2013. As of July 1, 2013: http://www.rand.org/pubs/tools/TL113.html

Grady, Jeffry O., *Systems Integration*, Boca Raton: CRC Press, 1994.

Institute of Electrical and Electronics Engineers (IEEE), *Standard for Application and Management of the Systems Engineering Process,* IEEE 1220, 2005.

Jain, Rashmi, Anithashree Chandrasekaran, and Ozgur Erol, "A Framework for End-to-End Approach to Systems Integration," *International Journal of Industrial and Systems Engineering*, Vol. 5, No. 1, 2010, pp. 79–109.

Kranz, Gordon M., *Systems Engineering and Integration Challenges and Opportunities*, briefing, July 2, 2009.

Lebron, Ruben A., Jr., Robert Rossi, and William Foor, "Risk-Based COTS Systems Engineering Assessment Model: A Systems Engineering Management Tool and Assessment Methodology to Cope with the Risk of Commercial Off-the-Shelf (COTS) Technology Insertion During the System Life Cycle," in *Strategies to Mitigate Obsolescence in Defense Systems Using Commercial Components,* Defense Technical Information Center, October 2000. As of September 12, 2012: http://handle.dtic.mil/100.2/ADP010964

Naval Air Systems Command, *Systems Engineering Technical Review Process*, Instruction NAVAIRINST 4355.19D, August 2008.

Sauser, Brian, Ryan Gove, Eric Forbes, and Jose Emmanuel Ramirez-Marquez, "Integration Maturity Metrics: Development of an Integration Readiness Level," *Information Knowledge Systems Management,* Vol. 9, 2010, pp. 17–46.

Sauser, Brian, Jose Ramirez-Marquez, Dinesh Verma, and Ryan Gove*, From TRL* [Technology Readiness Level] *to SRL* [Systems Readiness Level]*: The Concept of Systems Readiness Levels*, Hoboken, N.J.: Stevens Institute of Technology, Systems Engineering and Engineering Management, Paper #126, 2006a.

———, *Determining System Interoperability Using an Integration Readiness Level*, Hoboken, N.J.: Stevens Institute of Technology, Systems Engineering and Engineering Management, October 2006b. As of April 19, 2013:
http://www.dtic.mil/ndia/2006systems/Thursday/sauser.pdf

Sauser, Brian, Jose E. Ramirez-Marquez, Romulo Magnaye, and Tan Weiping, "A Systems Approach to Expanding the Technology Readiness Level Within Defense Acquisition," *International Journal of Defense Acquisition Management*," Vol. 1, 2008, pp. 39–58.

Savage, L. J., *The Foundations of Statistics*, New York: John Wiley, 1954.

Thompson, Jim, Lawrence Gresko, Ray Lowe, and Peter Nolte, *System Readiness: Assessing Technical Risk Throughout the Lifecycle*, PowerPoint Presentation, Office of the Under Secretary of Defense, Department of Defense: Research and Engineering Enterprise, (Systems Engineering), October 2009.

Thompson, Jim, Lawrence Gresko, Larry Schluderberg, Ray Lowe, and Peter Nolte, *Integration Risk Assessment: Assessing Integration Risk Throughout the Lifecycle*, pdf presentation, Office of the Under Secretary of Defense, Department of Defense: Research and Engineering Enterprise, (Systems Engineering), October 28, 2010.

U.S. Air Force, "Developing and Sustaining Warfighting Systems Process, Technology Development Subprocess," *Risk Identification: Integration & Ilities (RI3) Guidebook*, Version 1.2, December 2008.

Von Neumann, J., and O. Morgenstern, *Theory of Games and Economic Behavior*, 2nd ed., Princeton, N.J.: Princeton University Press, 1947.

Weapon Systems Acquisition Reform Act of 2009, S. 454, 111th Congress, February 23, 2009. As of September 12, 2012:
http://www.govtrack.us/congress/bills/111/s454

Implementing risk management principles to manage large defense acquisition programs is a priority for the U.S. defense acquisition community. To assist those decisionmakers responsible for identifying the risk associated with major weapons programs, RAND researchers developed a methodology and accompanying Excel, information-based risk tool (the "Assessor Tool"). The Assessor Tool offers an Office of the Secretary of Defense (OSD)-level approach to the evaluation and measurement of system integration risk. That is, it is meant for assessors, such as OSD personnel, who may not be especially familiar with the specific program under evaluation but still may need to make judgments about the program's risk. It is based on a tractable and comprehensive set of questions that can help evaluate integration risk at each point in the acquisition process. More specifically, the tool enables users to see how well integration risk is being managed by providing a standards-based valuation of integration issues that can lead to cost growth, schedule growth, and program performance. The users' manual for the Assessor Tool is available in a companion document, *An Excel Tool to Assess Acquisition Program Risk* (by Lauren A. Fleishman-Mayer, Mark V. Arena, and Michael E. McMahon, TL-113-OSD, 2013). The Assessor Tool and its methodology may also be generalizable to an entire set of information-based risk assessment applications. Overall, the methodology and tool have many strengths, including being based on well-grounded theories, allowing for reproducibility and traceability, and the extensive flexibility to be used to evaluate risk for many different types of programs. To provide a benchmarking and validation of the risk scores calculated by the tool, future work could include the tool's validation by tracking its output against a program's performance.

NATIONAL SECURITY RESEARCH DIVISION

www.rand.org

RR-262-OSD