2014-09

Incorporating trust into Department of Defense acquisition risk management

Reighard, Daniel K., II

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INCORPORATING TRUST INTO DEPARTMENT OF DEFENSE ACQUISITION RISK MANAGEMENT

by

Daniel K Reighard II

September 2014

Thesis Advisor: Gary Langford
Second Reader: Walter Owen

Approved for public release; distribution unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
INCORPORATING TRUST INTO DEPARTMENT OF DEFENSE ACQUISITION RISK MANAGEMENT

5. FUNDING NUMBERS

6. AUTHOR(S) Daniel K Reighard II

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.

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

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Risk management has been proven to be a valuable tool to identify and mitigate risks early in the program life-cycle. Modernization and communication advances have recently changed the commercial economy from national to global. Companies are starting to venture into new partnerships with foreign companies. However, there has also been an increase in business corruption, like Fannie Mac and Enron, which has raised skepticism in entering new partnerships. Industry is addressing this fact by no longer exclusively depending on science as the determining factor in risk assessment and starting to include trust as a factor in risk management. Qualitative measurements are being analyzed in attempted to address these uncertainties by incorporating "trust" into the risk management process. The purpose of this paper was to determine whether it was feasible and advantageous to incorporate "trust" into the risk management process for Department of Defense (DOD) acquisition. The premise of this research was that there were hidden risk factors attributed to qualitative measures that were not being identified in current DOD risk management processes. A preliminary conclusion of this thesis is that trust is a valuable factor in the risk assessment process that can help identify qualitative risk elements.

14. SUBJECT TERMS risk, trust, risk management, uncertainty, confidence, vulnerability	**15. NUMBER OF PAGES** 85
	16. PRICE CODE

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

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution unlimited.

INCORPORATING TRUST INTO DEPARTMENT OF DEFENSE ACQUISITION RISK MANAGEMENT

Daniel K Reighard II
Civilian, Department of the Navy
B.S., The Pennsylvania State University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2014

Author: Daniel K Reighard II

Approved by: Dr. Gary Langford
Thesis Advisor

Dr. Walter Owen
Second Reader

Dr. Clifford Whitcomb
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Risk management has been proven to be a valuable tool to identify and mitigate risks early in the program life-cycle. Modernization and communication advances have recently changed the commercial economy from national to global. Companies are starting to venture into new partnerships with foreign companies. However, there has also been an increase in business corruption, like Fannie Mac and Enron, which has raised skepticism in entering new partnerships. Industry is addressing this fact by no longer exclusively depending on science as the determining factor in risk assessment and starting to include trust as a factor in risk management. Qualitative measurements are being analyzed in attempted to address these uncertainties by incorporating "trust" into the risk management process. The purpose of this paper was to determine whether it was feasible and advantageous to incorporate "trust" into the risk management process for Department of Defense (DOD) acquisition. The premise of this research was that there were hidden risk factors attributed to qualitative measures that were not being identified in current DOD risk management processes. A preliminary conclusion of this thesis is that trust is a valuable factor in the risk assessment process that can help identify qualitative risk elements.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACQ	acquisition
CGI	Conseillers en Gestion et Informatique (French)
CMMI	Capability Maturity Model Integration
DOD	Department of Defense
EVM	earned value management
GA	Global Aeronautica
INCOSE	International Council on Systems Engineering
IPT	Integrated Program Team
IR	infra-red
ISO	International Organization for Standardization
IT	information technology
R&D	research and development
SEI	Software Engineering Institute
SETR	System Engineering Technical Review
UV	ultra-violet
WBS	work breakdown structure

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Risk management has been proven to be a valuable tool to identify and mitigate risks early in the program life-cycle. Modernization and communication advances have recently changed the commercial economy from national to global. Companies are starting to venture into new partnerships with foreign companies. However, there has also been an increase in business corruption, like Fannie Mac and Enron, which has raised skepticism in entering new partnerships. Industry is addressing this fact by no longer exclusively depending on science as the determining factor in risk assessment and starting to include trust as a factor in risk management. Ronald Regan once said, "Trust, but verify" when he was entering into the Intermediate-Range Nuclear Forces Treaty with his new foreign partner Russia (Massie 2013).

The purpose of this paper was to determine whether it was feasible and advantageous to incorporate "trust" into the risk management process for Department of Defense (DOD) acquisition. The premise of this research was that there were hidden risk factors attributed to qualitative measures that were not being identified in current DOD risk management processes. These qualitative measures of risk could be directly linked to trust elements. This research paper presents an argument on why trust should be incorporated into the risk management process for DOD acquisition programs. Various social, behavior, theological, and technical expert definitions on the term trust were used to decompose trust, in the field of risk, into three key elements; confidence, vulnerability, and uncertainty. The three trust elements: confidence, vulnerability and uncertainty, were further defined and correlated with current industry program risk management practices. Based on the analysis of the three trust elements, trust was defined for the purpose and use in risk management. Trust for risk management was defined as the subjective probability of a positive outcome from an agreement between two or more parties for a domain specific task based on the capability and goodwill of the trustee and predictability of a positive outcome within the defined technical, cost, and schedule boundaries.

Modernization of communication paths (i.e., e-mail and video teleconferencing), and quick technology advancement have opened industry to new partners in a global

economy. In addition, an influx of business corruption has left people and companies skittish about openly trusting their partners. New business partners lead to possible confidence, vulnerability, and uncertainty concerns. Companies have to weigh these trust elements when entering new partnerships and throughout the contract. To accentuate the point of global business partnership trust based risks, this thesis analyzed a case study on the Boeing 777 Dreamliner program which had an unprecedented scale of development outsourcing—65 percent of the development work was outsourced to more than 100 suppliers from 12 countries (Exostar 2007; Horng and Bozdogan 2007). Prior to the case study analysis, a validation of the case study was conducted against Robert Yin's research on case study design and methods (Yin 2009) and Gary Langford's research on engineering methods (Langford 2012). The case study was concluded as valid and appropriate for analysis for the topic of this research on trust in risk management. The analysis of the case study determined there were risk items associated with each trust element (confidence, vulnerability, and uncertainty) that could have been identified earlier if trust had been incorporated into Boeing's risk management process.

Research was also conducted on the feasibility of incorporating the trust elements of risk into the risk management process for DOD acquisition. The relationship between trust and risk was defined from social science research and using scientific methods. By examining social science research it was determined that to capture the likelihood and consequence of an action that requires dependence on other individuals to take action, the element of trust should be assessed. Through logic and psychometrics studies of risk and trust, it was determined that risk and trust were inversely related. The Dempster-Shafer theory was used to prove that trust elements could be added as long as there is no major conflict between the sources. The principle of indifference (Keynes 1921) supported the theory that each element should be weighed equally since we have no idea which element is more plausible. Alexander McNeil's (2005) research on the axiom of coherence was applied to conclude that risk and trust elements were additive. However, the process is not simple mathematical addition, since trust and risk are inversely related. Gary Langford's (2007) method for managing complexity warranted the use of geometric relationships to combine risk and trust into a matrix report.

The current Risk Management Guide for DOD Acquisition (DOD 2006) was studied and the process was decomposed to determine how and where the qualitative measures (trust factors) of risk could be addressed. The most practical place for the trust elements of risk to be analyzed was during the analysis of the quantitative measurement of risk. A detailed step by step example of how to take a risk item through the proposed risk and trust management process for DOD acquisition was described. Qualitative assessment measurement definitions for all three trust elements; confidence, vulnerability, and uncertainty were created. Example questions were also provided to assist in identifying trust risks. The risk management example highlighted how a risk item that was assessed quantitatively as a low risk was raised to a medium risk when qualitative measurements (trust) were included in the evaluation.

In conclusion, this research paper posits that the incorporation of trust into the risk management process for DOD acquisition is feasible and advantageous. The proposed risk and trust management process will provide the program manager more insight into the root cause of the risk. Clearer insight into the root cause will aid in management of risk and resource allocation for mitigating risk.

References

Department of Defense (DOD). 2006. *Risk Management Guide for Department of Defense Acquisition*, v 1.0. URL. http://www.acq.osd.mil/se/docs/2006-RM-Guide-4Aug06-final-version.pdf .

Exostar, LLC (2007). *Boeing 787: global supply chain management takes flight*. www.exostar.com/WorkArea/DownloadAsset.aspx?id=684.

Horng, Tzu-Ching, and Kirk Bozdogan 2007. "Comparative analysis of supply chain management practices by Boeing and Airbus: long-term strategic implications." Presentation at the MIT Lean Aerospace Initiative, Monterey, CA, April 18.

Keynes, John Maynard. 1921. "Fundamental Ideas." In *A Treatise on Probability*. London: Macmillan and Co., Limited, 4.

Langford, Gary and Huynh, Thomas. 2007. "A Methodology for Managing Complexity," Systems Engineering Test and Evaluation SETE Conference, Complex Systems and Sustainability, 24–27 September, Sydney, Australia. Paper published and archived, SETE Conference Proceedings.

Langford, Gary O. 2012. *Engineering Systems Integration Theory, Metrics, and Methods*. Boca Raton: CRC Press, 2012.

Massie, Suzanne. 2013 *Trust but verify: Reagan, Russia and me: a personal memoir*. Rockland, Maine: Maine Authors Publishing.

McNeil, Alexander J., Rüdiger Frey, and Paul Embrechts. 2005. *Quantitative risk management: concepts, techniques and tools*. Princeton, NJ: Princeton University Press. Print.

Yin, Robert K. 2009. *Case Study Research: Design and Methods*. Thousand Oaks, Calif.: Sage Publications. 4.

ACKNOWLEDGMENTS

I would like to thank Dr. Gary Langford for his extraordinary support in this thesis process. His guidance and knowledge on the subject were invaluable in keeping me focused and nudging me in the proper direction. This project would have been impossible without the support of NAVAIR and the Assistant Secretary of the Navy scholarship for the Joint Executive System Engineering Management program at the Naval Postgraduate School. A special thanks to Karley and Jason Reighard for their patience and understanding of the time commitment required of their father while preparing this report.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Risk management has been proven to be a valuable tool to identify and mitigate risks early in the program life-cycle. World-wide modernization and communication advances have recently changed the commercial economy from national to global. Companies are starting to venture into new partnerships with foreign companies to increase their market share (Marzec 2014). However, there has also been an increase in business corruption, like Fannie Mac and Enron, which has raised skepticism in entering new partnerships. Industry is addressing this fact by no longer exclusively depending on science as the determining factor in risk assessment and starting to include trust as a factor in risk management. Ronald Regan once said, "Trust, but verify" when he was entering into the Intermediate-Range Nuclear Forces Treaty with his new foreign partner Russia (Massie 2013). This research paper explores the various industries' approaches to incorporating trust into the risk management process and extracts those ideas and processes that could be employed into the Department of Defense (DOD) acquisition risk management process. A preliminary conclusion of this thesis research paper is that trust is a valuable factor in the risk assessment process that can help identify additional (hidden) risks. The information gathered in this research is formulated into a measurable weighted metric of "trust" that may be incorporated into the DOD acquisition risk management process in an attempt to highlight program qualitative risks that were previously overlooked.

B. PURPOSE

The purpose of this paper was to determine whether it was feasible and advantageous to incorporate "trust" into the risk management process for Department of Defense (DOD) acquisition. The premise of this research was that there were hidden risk factors attributed to qualitative measures that were not being identified in current DOD risk management processes. These qualitative measures of risk could be directly linked to trust elements. The ability to identify areas where trust can lead to risk will enable

program management to apply the resources and oversight required to mitigate these epistemic risks to minimize cost or schedule loss.

C. RESEARCH QUESTIONS

There is an enormous amount of research material on the topic of trust and risk management. In order to focus this research on the purpose of incorporating trust into the risk management process for DOD acquisition the following research questions are posed.

First, define trust. Specifically, in what ways and in what contexts has trust been defined, as related to risk assessment?

Second, determine what has changed in society that has made "trust" a larger factor in the risk management process. Was there some event or invention that has caused companies to elevate the factor of trust?

Third, in what ways has trust been incorporated in commercial sector risk assessment process? Research focuses on how various industries are identifying trust issues and mitigating them as part of the risk management process.

Fourth, determine the relationship between trust and risk. Can the element of trust and risk be combined into a single solution set?

The final research question is targeted at determining whether the process of incorporating trust into the DOD acquisition risk management process is feasible. In addition, are there benefits in identifying, analyzing, monitoring and managing qualitative risks that would be highlighted by incorporating trust?

D. BENEFIT OF STUDY

This research can be used to improve the DOD acquisition risk management process through the incorporation of trust. A qualitative and quantitative science based methodology will be used to determine the feasibility of combing trust and risk. The proposed risk and trust management process will provide the program manager improved insight into the root cause of the risk. Clearer insight into the root cause of risk will

enhance the ability of program management to mitigate risk and prevent cost over runs or schedule loss.

E. METHODOLOGY

This research paper examines various social science expert definitions of trust, creates a decomposition of the trust definitions, and then develops a standard definition of "trust" for risk management. This research paper explores various reasons why industry has turned to explore trust as an element of risk in its business practices. Multiple experts' views, in the field of trust and risk research, were investigated to determine the feasibility of incorporating trust into a risk management process. Additional research was conducted to explore the possible methods to combine trust and risk into the risk management process. These methods were translated into a process that could be employed into the DOD acquisition risk management process. The information gathered was formulated into a measurable weighted matrix of "trust" that may be incorporated into the DOD acquisition risk management process in an attempt to highlight program risks that were previously overlooked. A contemporary case study of the Boeing 787 Dreamliner manufacturing program was validated then investigated to demonstrate the value of trust in the risk management process.

The purpose, methodology and research questions stated above guided this research paper. The following paragraphs will lead the reader through the research findings and conclusions. The next chapter will lay the foundation of this thesis by defining trust and reviewing some of the societal changes that have increased industries interest in evaluating trust in business.

THIS PAGE INTENTIONALLY LEFT BLANK

II. TRUST

A. DEFINED

The word, "trust," originates back in the 13th century from the Old Norse word, "traust," which was defined as "help, confidence, support'" (Merriam-Webster 2014). Traust is cognate with the German word "Trost," which means comfort (Dictionary.com 2014). In addition, the word trust was also akin to the Old English word, "trēowe," which means, "faithful" (Merriam-Webster 2014). The origin of trust points directly to the interaction between two or more parties. The synonyms of trust are confidence, expectation, faith, hope, assurance, certainty, conviction, credence, dependence, reliance, stock, and sureness. Figure 1 presents a visual depiction of the word trust (Visual Thesaurus 2014).

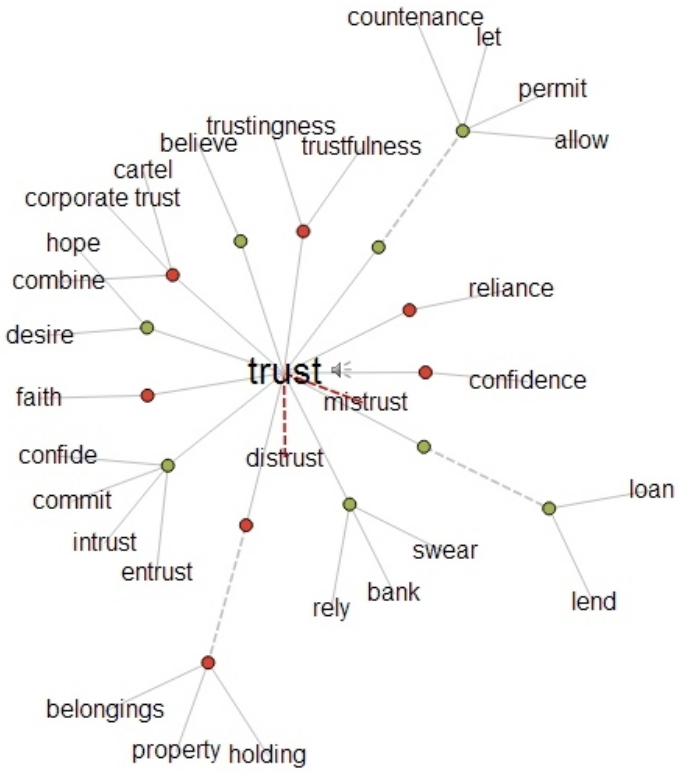

Figure 1. Trust Visual Thesaurus (from Visual Thesaurus 2014)

All of these words have a positive connotation and base their premise on an interaction with another party. To verify the opposite side of the argument, the antonyms of the word "trust" were then analyzed. The most common antonyms were distrust and mistrust, which were both defined as "to have no trust or confidence in (someone or something)" (Merriam-Webster 2014). Other common antonyms are disbelief, doubt, uncertainty, and suspect. As before, each of these terms was based on the premise that there is an interaction between two or more parties.

As a result, one can conclude that trust is the basic element to any cooperative relationship. Therefore, when entering a business contract, it is very important that everyone have the same definition of trust. This is much more complex than it originally seems. If one asks 20 strangers to define trust….after the initial "huh" statement, one will likely get 20 different answers. This simple question is so complicated because there are several variations of trust. Trust has been around for centuries and has evolved based on people's values and personal experiences. The definition of trust can also change based on a person's point of view: economic, behavioral, social, or physiological. Each variation has a different connotation and is used for different purposes. Table 1 lists some of the various definitions of trust as defined by social science experts from their field's point of views.

Table 1. Various Trust Definitions

Theory	Trust Definition	Author
Economics	"Decisions about trust are similar to other forms of risky choice; individuals are presumed to be motivated to make rational, efficient choices (i.e., to maximize expected gains or minimize expected losses from their transactions)."	Oliver E. Williamson (1985)
Psychology	"Trusting behavior occurs when an individual perceives an ambiguous path, the result of which could be good or bad, and the occurrence of the good or bad result is contingent on the actions of another person"	Morton Deutsch (1962)
Subjective	''[T]rust is the mutual confidence that one's vulnerability will not be exploited in an exchange''	Barney and Hansen (1994)
Sociology	"Trust is a bet on the future contingent actions of others"	Piotr Sztompka (1999)
Information	"Trust is that which is essential to a communication channel but cannot be transferred from a source to a destination using that channel."	Ed Gerck (1998)
Common Definition	"Trust is a belief that someone will do some function when asked to do it"	Merriam-Webster (2014)
Social Science	''Trust is an expectancy of positive (or nonnegative) outcomes that one can receive based on the expected action of another party in an interaction characterized by uncertainty''	Bhattacharya, Devinney, and Pillutla (1998)
Risk Related	''[T]rust as a state involving confident positive expectations about another's motives with respect to oneself in situations entailing risk''	Boon and Holmes (1991)
Behavioral	''[T]rust ... is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action''	Gambetta (1988)

This research is only going to focus on the risk management aspect of trust. More precisely, how trust can play a part in a program's risk management process? By analyzing the trust definitions from a risk perspective a few common elements can be pulled out. The three common elements of trust with respect to risk are confidence, vulnerability, and uncertainty. These three elements will be examined further to complete the definition of trust in the area of risk management.

1. Confidence

The first element of trust in risk management is confidence. Confidence in business can be defined as the belief that the partner has the tools and capability to perform the task that is required. Contractors may have the best intentions and really try to perform a task; however, sometimes the technology is above their capability. For example, this author worked on a missile detection program in which the awarded contractor was known for producing missiles and a missile warning protection system that both operated in the one frequency spectrum band. During award selection, the consensus, which should have been deemed invalid, was that a contractor that built missiles and threat detectors in one frequency spectrum band should also be able to develop a missile detection system that operated in the different frequency spectrum band. In the end, the contractor was unable to deliver a missile detection system in the different frequency band. This cost the tax payers millions of dollars and the war-fighter a three-year delay in capability. A contributing factor to the failure of the program was the contractor's lack expertise in the different frequency spectrum. The government bestowed too much confidence in the contractor's experience in the original spectrum when evaluating its capability to develop a system in a different spectrum. This is but one example of how adding trust into the risk management process could lead to better choices. Most people would not trust a stock broker to fix their car. Nor would most people trust a mechanic to invest their money in the stock market. Confidence as related to trust should be domain specific to the task being assigned to performed.

Another example of a poor selection of a prime contractor based on blind confidence is the Affordable HealthCare website release. As reported by the Washington Post, “The lead contractor on the dysfunctional Website for the Affordable Care Act is filled with executives from a company that mishandled at least 20 other government IT projects” (Markon and Crites 2013). So why was this company selected if it had been linked to previous troubled programs? The reason was simple: based on past performance (1970s–1990s), the company had built a reputation as the best company for Health and Human Services IT programs. As a result, CGI Federal was placed on a prescreening list that put them as front runners for any urgent projects. However, due to senior executive and a high employee turnover rate at the end of the 1990s, the company was not the same company and started struggling with the completing programs on time and within budget. “They did not provide us one working piece of software after almost six years,’’ recalled Ed Buelow Jr., the Mississippi state’s former revenue commissioner (Markon and Crites 2013). Confidence in a company to perform a task should not only be based relative past performance but also include a real-time snapshot of a partner’s current program(s) performance and domain specific technical capability. Chapter IV will discuss how to assess confidence levels.

2. Vulnerability

The second element of trust in risk management is vulnerability. The vulnerability side of trust can be taken from Chiles and McMackin (1996, 85) where they define trust as ‘‘the expectation that an exchange partner will not engage in opportunistic behavior, even in the face of countervailing short-term incentives and uncertainty about long-term benefits.’’ In other words, in business a company must determine who they can trust to follow through on an agreement. As Francis Fukuyama (1995, 26) points out, “the most effective organizations are based on communities of shared ethical values.” Industries, such as networking systems, e-commerce, and financial banking, have taken this notion and moved to minimize vulnerability with new global partners companies by looking for companies that share mission statements and/or ethical values. Companies, within these industries, are evaluating potential partner company’s values by assessing with whom they already have business partnerships. For example, Subaru is well known for valuing

safety. Therefore, if Subaru is looking for a business partnership with a windshield company, Subaru will look for a windshield company that works with other companies known for safety, such as Volvo. To assess a business partner's ethical values and integrity, companies are researching common associations of potential partners, such as the charities they support, community involvement, and professional organizations with which they are associated, such as International Council on Systems Engineering (INCOSE). Castelfranchi and Falcone (2000) refer to this notion as relational capital on which trust is built.

Another side of vulnerability is to assess the trustee's intention and willingness to act in the interests of the trustor, otherwise known as goodwill (Das and Teng 2001). Companies must determine the level to which their partner is committed to their relationship. Piotr Sztompka (1999) brings up a similar argument by asserting that if the companies are co-dependent on each other to sustain and/or build up their company's infrastructure then risk is reduced. In addition, if both parties are looking to promote a long term relationship then vulnerability goes down and risk is reduced. Most business relationships will not have equal dependence on one another, but the trustee must take this measurement into account as a risk to the program. If the trusted has little mutual benefit in the success of a program's success, then the trusted company could walk away when provided a better opportunity, or just reprioritize its resources, which could cause delays to its delivery of product to the trustee (i.e., other business partner). Karahannas and Jones (1999, 347) note that trust is "closely related to risk, since without vulnerability there is no need for trust." Therefore, a company must determine their level of vulnerability to determine the level of trust the company is betrothing to the trustor (i.e., business partner). This level of trust will ultimately indicate the companies risk level. Chapter IV will discuss how to determine a company's vulnerability level.

3. Uncertainty

The third element of trust in risk management is uncertainty. The term "risk" is generally used to describe adverse events with a known probability (Adams 1995). Uncertainty stems from the lack of knowledge and therefore has an unknown probability,

also known as epistemic uncertainty (Amendola 2002). This lack of knowledge could stem from a new technology being developed or a new manufacturing process that a company is employing for the first time. International organizations such as INCOSE, International Organization for Standardization (ISO), DOD, and Software Engineering Institute (SEI) have tried to minimize this uncertainty by setting up standard processes for companies to follow. As a result, companies will often require that their contractors to have certain process certifications, such as ISO 9000 or Capability Maturity Model Integration (CMMI), and required that the contractor follow/maintain these processes for the duration of the program under contract. However, a company may have a certification but never employed this certified process in the domain of the current task. For example, a company can be CMMI level 5 for developing missiles, but never have employed the process for sensor development. Therefore, even with these controls in place there is always uncertainty. Companies do not have the time or ability to work out probability expectations for every possible outcome, nor can a company brainstorm every possible problem that may occur. In order to facilitate the process of calculating the probability of the unknown, companies typically set aside additional funding and resources, called "management reserve," to deal with a level of uncertainty. However, the amount of "management reserve" set aside for a program is an estimate and generally based on a high level of confidence that things will go according to plan. The above sediment is supported by Luhmann (1979), "In situations of uncertainty, trust allows short-cutting probability calculations and thus reduces complexity." The problem with this approach is that the management reserve account is typically managed only by the program manager allowing the funding and resources set aside for uncertainty to be used for other tasking. Therefore, risk is elevated by depleting funding and resources intended for uncertainty. Chapter IV will discuss how to assess a program's uncertainty level.

4. Trust Defined in Risk Management

Based on the analysis of the definitions of trust from the various social science fields and the derived trust elements, a definition for trust for the field of risk management can be affirmed. This research defines trust for the purpose of program risk management as the subjective probability of a positive outcome from an agreement

between two or more parties for a domain specific task based on the capability and goodwill of the trustee and predictability of a positive outcome within the defined technical, cost and schedule boundaries.

B. HOW HAS SOCIETY CHANGED TO ELEVATE THE IMPORTANCE OF TRUST?

Niklas Luhmann (1979) stated that trust gains in importance as society becomes more modern. The combination of new technology, system complexity and modernization raises the likelihood of uncertainty and risk. Two distinctive points can be pulled from Luhamm's comment: society modernization and technology. World-wide modernization and communication advances have recently changed the commercial economy from national to global. Communication advancements over the past three decades, such as video teleconferencing and e-mail, have aided this global partnership to develop business partners internationally. Businesses are no longer handcuffed to partnering with local companies and are branching out to partner with foreign companies for three main reasons: cost, component specialist / expertise, and proximity / market share (Marzec 2014). Companies are looking to reduce their overhead costs, facility labor, utilities and real estate taxes, and have found costs cheaper overseas (Hamlett 2014). As products get more complex, they require multiple specialized components to be manufactured. The cost of setting up a manufacturing product line for every component in a complex product (e.g., manufacturing a computer, airplane, or car) would be too burdensome for one company. Outsourcing production to a second company that has expertise in producing the material can decrease production time (Hamlett 2014). Another advantage is if the product line changes or a repair to equipment is required, the responsibility for the cost associated with this process falls on the supplier (Hamlett 2014). Therefore, companies look to outside manufacturers to supply their specialty components. Proximity reflects the global growth of the market place. Companies are always looking to increase their market share, and modernization of other countries has produced new foreign customers. As a result, companies are outsourcing some of their manufacturing to foreign countries in hopes of getting their business. For example, Boeing's Dreamliner program had an unprecedented scale of development outsourcing—

65 percent of the development work was outsourced to more than 100 suppliers from 12 countries (Exostar 2007; Horng and Bozdogan 2007). This program will be analyzed as a case study in Chapter V. While these new partnerships may open companies to profits, they also open the company to the trust elements or risk in confidence, vulnerability, and uncertainty. As part of this global business partnership, companies are relying on both quantitative risk analysis, but also qualitative risk analysis (also known as trust analysis) to determine a company's trustworthiness. For example, the banking industry is updating their small business lending models to use qualitative information along with financial information to forecast small company's creditworthiness (Grunet 2005). Qualitative data that companies may gather include information about the reputation of the company by asking questions such as: how does the company treat its own employees (What is the turnover rate?); how long the company has been in business?, what are the employee skill sets that the company hires? and, who were the company's past business relationships? Companies are also looking into potential partners' past performance to determine qualitative risk using questions such as: does the company meet their obligations? and has the company met deadlines and provided their product on time? Favorable responses to these qualitative risks are the building blocks of trust in a business partnership and should be assessed during contract initiation and throughout the life cycle of a program.

The last main contributor to companies adding qualitative risk assessment into their program management decisions is the influx of business corruption. A man's word was his honor, and when he shook hands on a deal, it was followed through. But now litigation and profit are the dominant players. WorldCom, EnRon, and FreddieMac are just a few examples of how businesses have strayed from the path of trust as a priority to the path of profit as a priority, often compromising trust elements. As a result, companies look to protect themselves with well-crafted contracts by teams of lawyers, which basically state, "We don't trust you." This leads to the last point, most do not like to confront one another and say they do not trust each other. Imagine talking to a stranger in the airport line and after five minutes of meeting that person you tell him that you do not trust him but would like to be friends. That person will immediately be put on the defensive, and you are not likely to develop a friendship. The same holds true in

business; starting off a business relationship by openly stating distrust is not a good way to build cohesion in the relationship. As a result, some companies tend to ignore the qualitative risks to avoid confrontation and lean toward assumed trust.

In this chapter, a definition of trust was derived based on the analysis of the definitions of trust from the various social science fields. The definition of trust was decomposed into three key elements: confidence, vulnerability and uncertainty. Each element of trust was defined to establish a standard definition to support this research paper. In addition, this chapter highlighted some of the factors and past historical events that have caused trust to become more influential to companies when making business decisions. The following chapter will summarize the Risk Management Guide for DOD Acquisition to construct the foundation for incorporating trust into the established risk management process.

III. DOD RISK MANAGEMENT PROCESS

A. DEFINED

Risk management is the overarching process that encompasses risk identification, analysis, mitigation planning, mitigation plan implementation, and tracking (DOD 2006). The purpose of risk management is to identify cost, schedule, and technical risks that may occur in the future of a program so that each risk item can be monitored and/or controlled. The Risk Management Guide for DOD Acquisition breaks risk into three components: 1) it must be a future root cause that can be overcome or avoided, 2) the risk has a likelihood of occurring if not managed, and 3) there is a consequence of cost, schedule and/or technical performance if the risk realized. By addressing program risks early on, the potential for program cost and schedule overruns may be mitigated. In addition, risk management may also forecast technical risks that could be mitigated or overcome by applying additional resources earlier than originally planned.

The first step in the risk management process is to identify the risk items of a program. In order to identify risk, one must know what is the definition of risk, general practices on how risks can be identified, and who should identify risk. The Risk Management Guide for DOD Acquisition summarizes risk as the root cause that can prevent a program from achieving performance goals and objectives within defined performance constraints, cost, and schedule over the life cycle of the program. Best practice to identifying risk is to decompose the program into the work breakdown structure (WBS) elements and allow the system matter experts to identify risk for each WBS based on prior experience, according to the Risk Management Guide for DOD Acquisition (2006). Risk identification should not only occur at the beginning of a program. Risk should continually be identified in all facets of the program to include the ability to assess technical performance, schedule, resource availability, program cost, manufacturing process and contractor earned value management (EVM) data/trends. Since risk affects all areas of the program, risk identification should be the job of the entire program team; this includes the test manager, financial manager, contracting officer, logistician, and every other team member, not just the program manager or

systems engineer. In addition, since the contractor's ability to develop and manufacture the system affects program risks; the contractor should also be considered a valuable partner in risk planning.

The identified risk must then be analyzed to determine how big the risk is. The Risk Management Guide for DOD Acquisition uses a Risk Reporting Matrix, Figure 2, to assess the level of risk for each risk item. The risk is reported as low (green), moderate (yellow), or high (red) based on the assigned values of likelihood and consequence of each risk element.

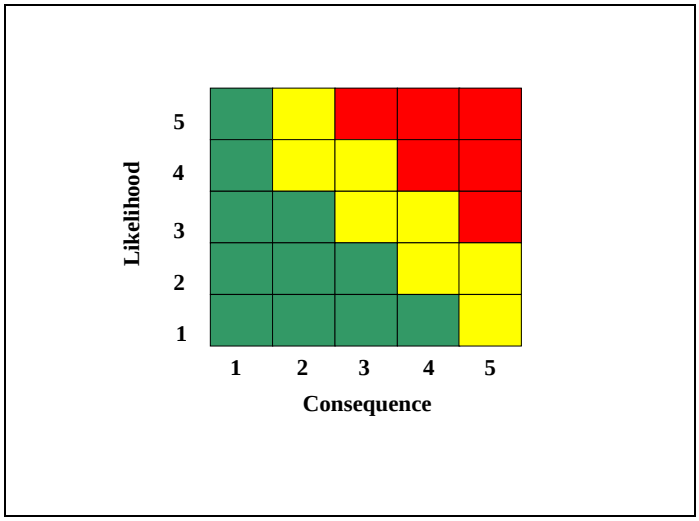

Figure 2. Risk Reporting Matrix (from DOD 2006)

Each risk item is assigned a value for the likelihood of occurrence. The likelihood is the probability that an action could occur based on past experience and current data. A typical likelihood definition is depicted in Figure 3 (DOD 2006). An explanation of how to read and use the likelihood criteria figure is described in the following paragraphs.

Likelihood

Level	Likelihood	Probability of Occurrence
1	Not Likely	~10%
2	Low Likelihood	~30%
3	Likely	~50%
4	Highly Likely	~70%
5	Near Certainty	~90%

Figure 3. Levels of Likelihood Criteria (from DOD 2006)

Each risk element is also assigned a consequence value. Consequence is an assessment of how the risk element will affect technical performance, schedule or cost if realized. A typical DOD Risk Management consequence definition table is shown in Figure 4 (DOD 2006). An explanation of how to read and use the consequence criteria figure is described in the following paragraphs.

Level	Technical Performance	Schedule	Cost
1	Minimal or no consequence to technical performance	Minimal or no impact	Minimal or no impact
2	Minor reduction in technical performance or supportability, can be tolerated with little or no impact on program	Able to meet key dates. Slip < * month(s)	Budget increase or unit production cost increases. < ** (1% of Budget)
3	Moderate reduction in technical performance or supportability with limited impact on program objectives	Minor schedule slip. Able to meet key milestones with no schedule float. Slip < * month(s) Sub-system slip > * month(s) plus available float.	Budget increase or unit production cost increase < ** (5% of Budget)
4	Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success	Program critical path affected. Slip < * months	Budget increase or unit production cost increase < ** (10% of Budget)
5	Severe degradation in technical performance; Cannot meet KPP or key technical/supportability threshold; will jeopardize program success	Cannot meet key program milestones. Slip > * months	Exceeds APB threshold > ** (10% of Budget)

Figure 4. Levels and Types of Consequence Criteria (from DOD 2006)

The risk item is then plotted on the 5X5 Risk Reporting Matrix (Figure 1) based on its likelihood and consequence values and the risk level is reported as low (green), moderate (yellow), or high (red).

After the risk item has been assigned a risk value, the program risk team will attempt to identify mitigation steps that could potentially lower the likelihood or consequence value. For example, if the program is worried about a part not fitting in the aircraft, the program could hire someone to build a non-working prototype to conduct a fit check prior to the final system build.

Once the mitigation steps are identified, the Integrated Program Team (IPT) can start making decisions on the specifics of what needs to be done, when in the schedule it can be accomplished, who is the responsible party, and is whether there is enough funding to implement the risk mitigation plan.

Throughout the life cycle of the program, the program manager will track the progress of the risk items. In addition, the program will hold periodic Program Risk Management Boards to address new risk items and report on the status of the current risk items. Figure 5 shows the basic DOD Risk Management Process. The risk management process is iterative should continually be managed throughout the acquisition life cycle.

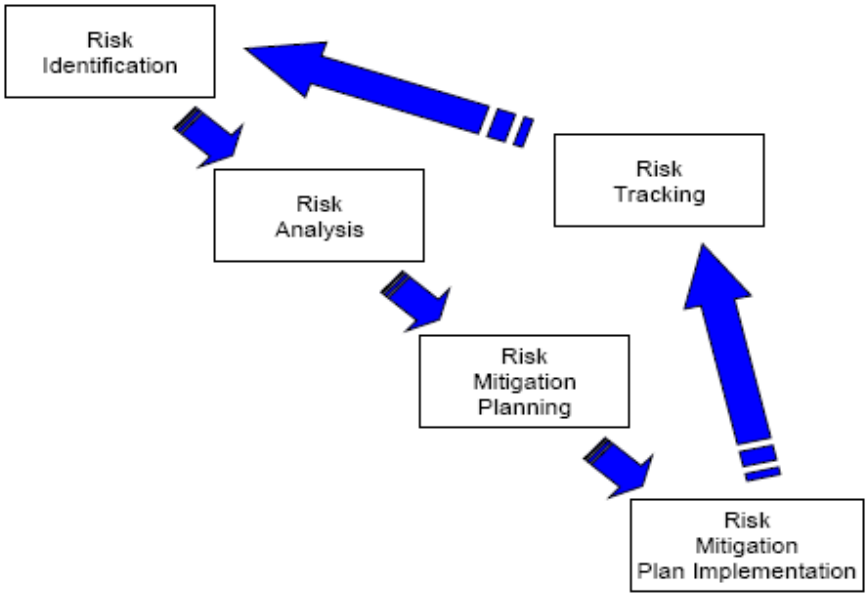

Figure 5. DOD Risk Program Management Process (from DOD 2006)

This chapter summarized the current DOD risk management process as outlined by the Risk Management Guide for DOD Acquisition. The process of risk identification, analysis, mitigation planning, mitigation plan implementation, and tracking was described. Risk was defined by three components: 1) it must be a future root cause that can be overcome or avoided, 2) the risk has a likelihood of occurring if not managed, and 3) there is a consequence of cost, schedule and/or technical performance if the risk realized. The current process of assessing risk on the 5X5 Risk Reporting Matrix based on the definitions of likelihood and consequence was reviewed. The following chapter will evaluate the feasibility and value of incorporating trust, as defined in Chapter II, into the DOD risk management process.

IV. ALIGNMENT OF TRUST INTO THE DOD RISK MANAGEMENT PROCESS

A. THE RELATIONSHIP BETWEEN TRUST AND RISK

The relationship between trust and risk must be defined in order to implement trust into the risk management process. Castelfranchi and Falcone (2000, 4) summarize the difference between risk and trust by stating, "risk is just about the possible outcome of a choice, about an event and a result; trust is about a person or organization: it mainly consists of beliefs, evaluations, and expectations about the other actor, his capabilities, willingness, and general motivations." So, if risk and trust are not the same, how are they related?

To determine the relationship between risk and trust one must answer, "Can risk exist without trust?" The answer is "yes." The following simple example will rationalize this concept. Contrary to James Coleman's (1990) notion that the decision to place trust is analogous to the decision to place a bet, placing a bet has no trust element. If a person goes to a casino and puts money in a slot machine, then the individual is taking a risk. The individual may lose or win money. The amount of risk can be calculated based on the odds of winning money (likelihood) and the total value of money (consequence) placed in the slot machine. The entire scenario revolves around one's own choice. There is no individual to trust and therefore no element of trust in making a bet. Another example of an event that contains risk without an element of trust is a man cliff diving into the ocean. The man is risking his life (consequence) for the adrenaline rush (likelihood) achieved by cliff diving. Though there is a risk being taken by cliff diving, there is not a reliance on another individual and therefore no element of trust. Next, consider the reverse question of whether trust can exist without risk. The answer is "no." As backed up by the various definitions of trust from Table 1, when an individual trusts someone or something to perform a task, he is taking a risk that someone or something will or will not perform the task. For example, if someone asks a friend to pick him up from the airport, then the requestor is taking a risk on that friend showing up on time or at all. If the friend is late to arrive at the designated time, then the requestor will lose

personal time that could have used to perform other tasks. If the friend does not show up at the airport, then the requestor will lose the time it takes me to devise a new plan, the cost (taxi, or rental car), and the additional time that the new plan incurs. Therefore, to capture the likelihood and consequence of an action that requires dependence on other individuals to take action, the element of trust should be assessed.

B. WHY SHOULD TRUST BE PART OF THE DOD PROCESS

A contract is a binding agreement of trust between the government and contractor. The government clearly defines its programmatic and technical requirements in a request for proposal. The contractors reply with their proposal to the contract accepting the stated programmatic and technical requirements and add the boundary conditions of cost and schedule. Then the government accepts a contractor's proposal to make a binding contract between the two parties. Or as Howard Shore (2012, np) defined, "contractual trust is trust that exists only to the extent that things are explicitly agreed upon and one can only trust what people state in formal agreements." The DOD acquisition starting point is a trusting agreement between two parties.

Trust is also essential for a team to be functional. As Patrick Lencioni (2002) points out in his book *The Five Dysfunctions of a Team*, one of the five dysfunctions of a team is "the absence of trust." Team members must be trust one another to be able to share ideas, different opinions and mistakes without fear of ridicule or job security. Ultimately, the IPT should reach a level of trust that the contractor is doing the work required to achieve the final goal. However, as the trust level decreases, people are slower to respond and less likely to divulge all the information. Slow and incomplete communications will lead to delayed and/or bad decisions and ultimately increase programmatic risks to cost and schedule. Therefore, the government and contractor have to maintain a level of trust to minimize the potential risk elements associated from mistrust. This theory is also supported by the work of Eddy Witzel (2014) exploring leader attitudes and behaviors that drive innovation. He found that both trust and risk were critical and were in tension. When a leader is trusted, that leader is allowed to take more risk. When the risk is successfully mitigated, the leader gains additional trust.

However, when the leader fails, trust is reduced and the leader is prevented from taking risk. It is hard to build a trusting business relationship between a particular contractor and government program team due to the following factors. First, the government is a bureaucratic entity in which processes rule the Acquisition Strategy, which does not allow for the flexibility of corporate relations. There can be no side agreements to add/remove capability or to buy more products unless explicitly stated in the contract. Second, the government contract is usually for one product/service with a contractor; it buys one item. There are no guarantees of future work and therefore no future dependency on the relationship with that company for the next project. Therefore, it is very important to monitor the trust level within the IPT by incorporating the element of trust into the risk management process.

C. TRUST EXPRESSED MATHEMATICALLY

This report has defined trust, its relationship with risk, and why it is important. The next task is to determine how to express trust mathematically to incorporate trust into the DOD Risk Management Process. The definition of business trust is the subjective probability of a positive outcome from an agreement between two or more parties for a domain specific task based on the capability and goodwill of the trustee, in the absence of knowledge. To make a probabilistic analysis of a risk item, one must have all the data for that event. However, the element of trust is subjective, and there is not a complete data set to make a probabilistic analysis. Subjective probability analysis can be defined using the Dempster-Shafer theory. The Dempster-Shafer theory is based the idea of obtaining degrees of belief (trust) for one question (risk item) from subjective probabilities (trust factor) (Shafer 1976). The Dempster-Shafer theory is based on belief (confidence) and plausibility (uncertainty) which matches nicely to the trust definition. In addition, the Dempster-Shafter theory also allows the combination of evidence from different sources to arrive at a degree of belief for a related question (risk) as long as there is no major conflict between the sources (Shafer 1976). And since the risk management members are all part of the IPT whose goal is for a successful program, there should be no major conflict between data. Therefore, one can conclude that the trust elements are additive.

Trust is made up of three sub-elements: confidence, vulnerability and uncertainty. To combine these three trust elements into one probability factor, a weight distribution for these factors must be defined. However, each of the trust elements is subjective with no rationale to determine which element is more plausible. Therefore, each trust element should be treated as equally likely to occur. This is supported by John Keynes's principle of indifference. The principle of indifference, states "if there is no known reason for predicating of our subject one rather than another of several alternatives, then relatively to such knowledge the assertions of each of these alternatives have an equal probability" (Keynes 1921, 52–53)

The mathematical relationship between risk and trust will now be defined. Risk has a negative connotation. Only under certain circumstances do companies want to be known for taking larger risk, for instance if the company is looking at competing for market share against a larger established company in a specific product market. However, trust has a positive connotation. Companies and people desire to achieve high trust as a part of their normal operation. So trust and risk are inversely related, generally. This theory is supported by psychometric studies of risk and trust, which often found risk and trust to be inversely related (Siegrist 2010).

$$RISK = C/TRUST \text{ (where C is a constant).}$$

The theory of quantitative risk management was explored to determine whether or not to combine two factors of risk that are independent. Alexander McNeil explains how two risk factors that affect the outcome of an event are considered aggregate risks. Using the axiom of coherence, he demonstrates how aggregate risks are additive "for simple risks" (McNeil 2005). In conclusion, program risk could be equated by the summing the items of trust or items of risk. However, the process is not simple mathematical addition, since trust and risk are inversely related. Gary Langford's method for managing complexity warranted the use of geometric relationships to combine risk and trust into a matrix report (Langford 2007).

1. Geometric Risk and Trust

Based on the taxonomy of confidence, vulnerability and uncertainty: "An element e of a system is associated with a risk, R_e, defined by

$$R_e = X_e U_e V_e = X_e(1-a_e)V_e,$$

where confidence, X_e, is the degree to which harmful events could impact the element; vulnerability, U_e is the probability that element e is degraded or fails in some specific way, if attacked; value, V_e, results from a successful attack on element e; and uncertainty, a_e, is the likelihood that an asset will be found acceptable after a problem is realized. V_e is given by

As in (Langford and Huynh 2007), the system value, V(t), is given by

$$V(t) = \frac{\sum F(t)P(t)Q(t)}{I(t)},$$

where $F(t)$ is a function performed by the system, $P(t)$ is the performance measure of the function $F(t)$, $Q(t)$ is the quality, which is the tolerance assigned to $P(t)$, $I(t)$ is the investment of energy, matter, material wealth (e.g., dollars or other equivalent convenience of at-risk assets), and information. Time, t, is measured relative to the onset of period of interaction for which the system is at risk. If the unit of $Q(t)$ can be converted to the unit of $I(t)$, then the unit of V(t) is that of $P(t)$, since $F(t)$ is dimensionless (Langford 2007). Since an element in a system may be connected to more than one element, the number of interactions of each element is related to the number of elements and the number of links between the elements.

Subscribing to Mannai and Lewis (2007), we obtain the system risk, R, as

$$R = \sum_{i=1}^{2(n+m)} X_i(1-a_i)g_i V_i,$$

in which n denotes the number of elements, m the number of links, and g_i denotes the degree of the i^{th} element" (Langford and Huynh 2007).

To determine the number of elements and links, one must use the geometric theory. The number of elements m is determined by the number of risk or trust elements related to a program risk and the links is calculated by the interfaces. For example, if there were three elements of risk and/or trust, then there are three links between elements. For four elements there are six links between elements. See Figure 6.

Figure 6. Geometric Relationship of Trust and Risk Elements

The result of this process is to end up with a tuple of trust and risk: $T_{n\,(1,2,3,\ldots)}$, $R_{j\,(a,b,c,\ldots)}$. Therefore, the assessment of overall combined risk and trust assessment of program risk is best expressed in a matrix similar to the current Risk Reporting Matrix from the *Risk Management Guide for DOD Acquisition* (DOD 2006).

D. IMPLEMENTATION OF TRUST IN THE DOD RISK MANAGEMENT PROCESS

Chapter III summarizes how the current Risk Management Process for DOD Acquisition works. Risks are identified, evaluated and then each risk is assigned a value on the Risk Reporting Matrix. However, first one must define the values of the rating scale. In the case of the aggregation of risk and trust, the risk matrix must be set up based on the preference for either risk aversion or trust acceptance. Then the program will need to define the meanings of risk levels (high, moderate, and low) and the meanings of trust levels (high, moderate, and low) based on the bias for their acceptance of risk and trust. If the bias toward risk is that of high risk aversion and trust is deemed to be less important than risk (or, alternatively stated as, having an aversion to accepting trust as high except

in the most extreme cases), then the following mappings of risk and trust to their definitions would be used for applying the aggregation of risk and trust in the Risk Matrix, Table 2. One must remember that low trust is equivalent to high risk, since they are inversely related.

Table 2. Risk and Trust Aggregate Matrix

Level	Risk	Trust
High (level 1)	Possible, but not probable	Low
High (level 2 < level 1)	Possible, not modeled	Moderate
High (level 3 < level 2)	Possible, modeled	High
Moderate (level 4 < level 3)	Unconfirmed / Good Estimate	Low
Moderate (level 5 < level 4)	Unconfirmed / Fair Estimate	Moderate
Moderate (level 6 < level 5)	Unconfirmed / Rough Estimate	High
Low (level 7 < level 6)	Confirmed / Sketched	Low
Low (level 8 < level 7)	Confirmed / Modeled	Moderate
Low (level 9 < level 8)	Confirmed /Demonstrated	High

To help demonstrate how to implement trust into the Risk Management Process for DOD Acquisition, an example will be provided for a walk through demonstration of the process. A duplicate figure of the Risk Management Process for DOD Acquisition is added for reader ease, Figure 7.

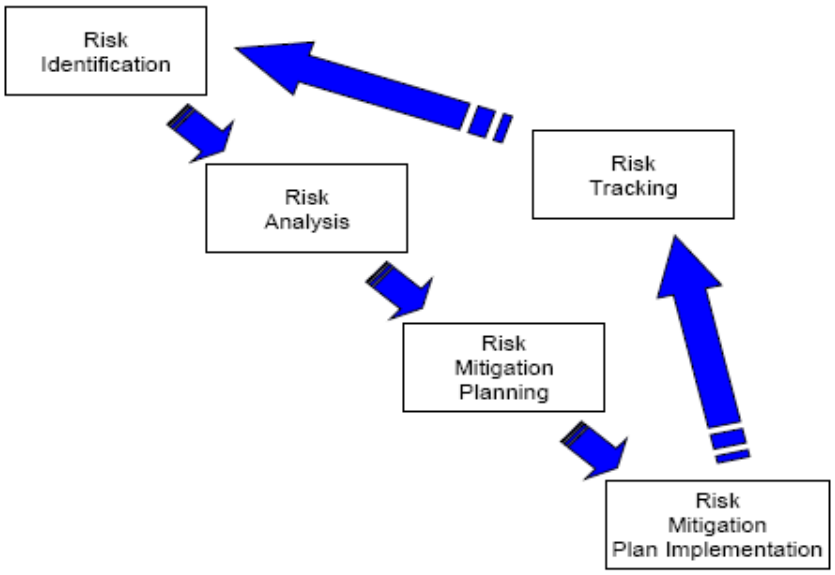

Figure 7. DOD Risk Program Management Process (DOD 2006)

Step one is to identify a risk. For this example, the identified program risk is "Delivery of late s/w." Step two is to analyze the risk. Assume that the IPT risk board members assessed the "Delivery of late s/w" risk as having a likelihood of two and a consequence of three based on the technical information that was available. Using the Risk Reporting Matrix from the *Risk Management Process Guide for DOD Acquisition*, the "Delivery of late s/w" risk item would be rated as a low risk, as presented in Figure 8.

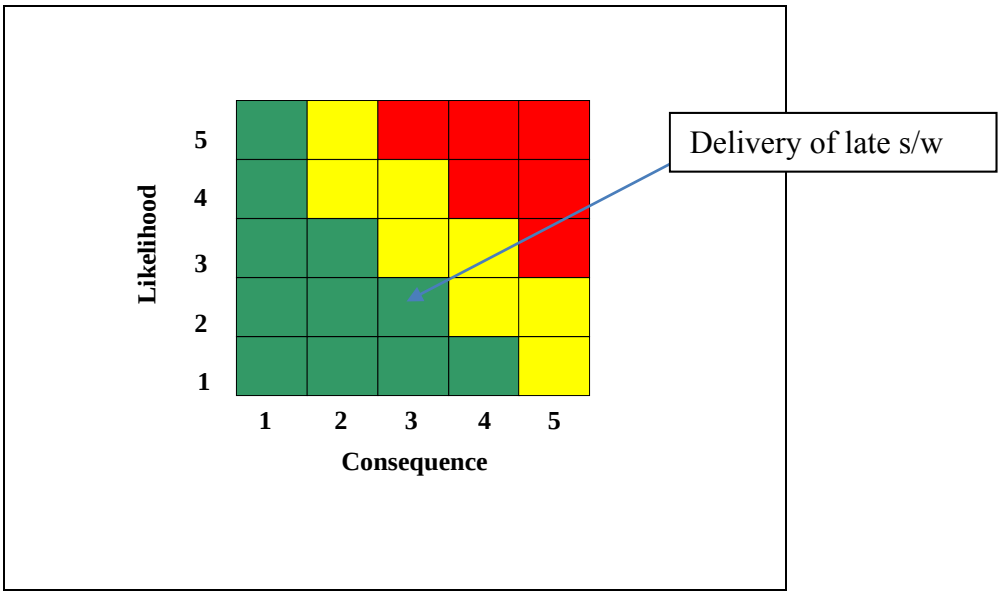

Figure 8. Risk Reporting Example

Following the current risk management process, the program risk board would move on to develop some mitigation steps for this risk item. However, this process would not account for the trust element of risk and not fully define the entire risk item. Therefore, the risk analysis section should be further decomposed by implementing a trust element analysis. The next step is to identify whether trust elements exist, and then analyze each trust element. As part of the trust assessment, the risk board would have to address questions such as: 1) are the programmers capable of completing the task (confidence)? 2) does management think that this program is a high priority to the contractor and has the contractor applied the right resources to get the task completed (vulnerability)? and 3) are the requirements ill defined (uncertainty)? These are just a few examples of questions, which are based on trust that are rarely asked at risk management board reviews. The proposed risk analysis section breakdown of the Risk Management Process for DOD Acquisition is shown in Figure 9.

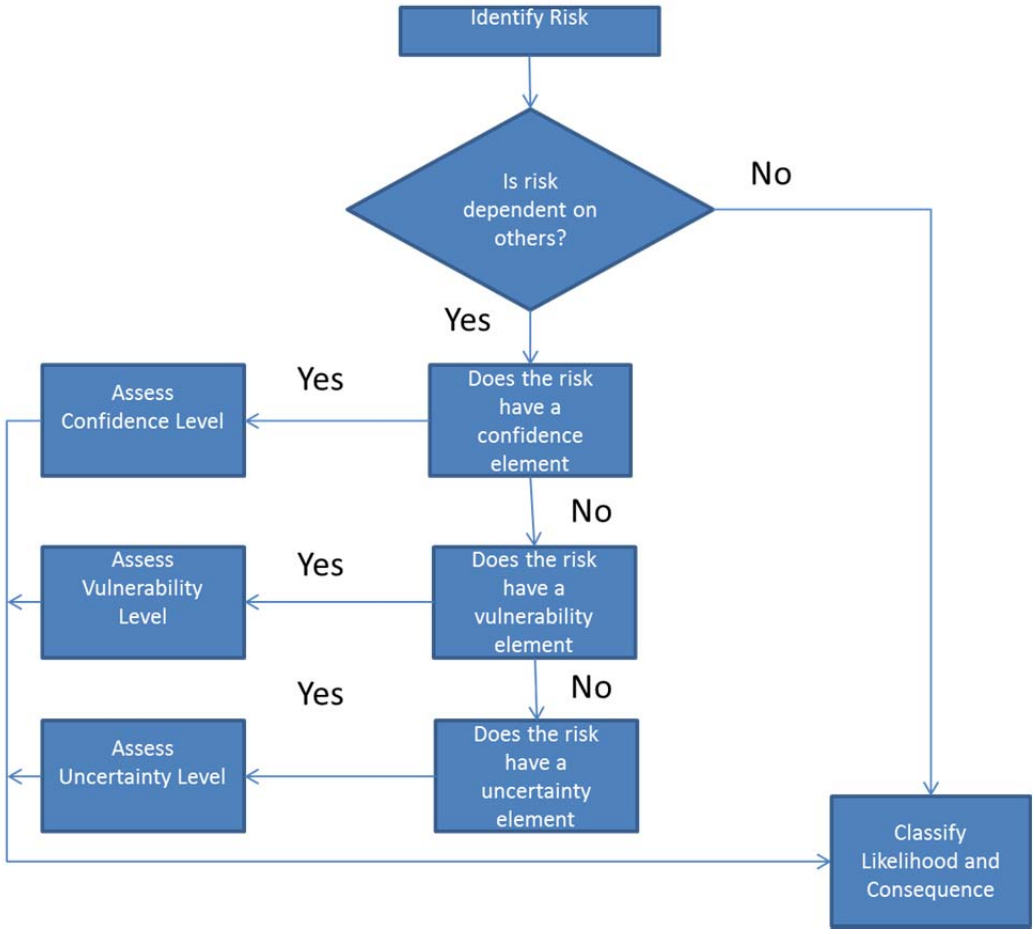

Figure 9. Risk Analysis with Trust Factors

The same example will now be evaluated using the risk and trust aggregate method. The risk identified was "Delivery of late s/w." This risk was initially assigned as a likelihood of two and a consequence of three based on technical data and therefore rated as a low risk. To determine whether the identified risk has a trust element, the risk members must conclude that the risk item is dependent on others. In order to have an element of trust, the risk must rely on a second party to perform a task. In the case of the risk item "late software delivery," the answer is yes. The next step is to analyze the risk element for a confidence element. To reiterate, confidence in business is defined as the belief that the partner has the tools and capability to perform the task that is required. Since delivering s/w is a task reliant upon a business partner, the answer is yes. Potential questions to address could be, are the programmers capable of completing the task

(confidence)? Or does management have a plan to apply the right resources to get the task completed (confidence)? The above two questions relate to the confidence that the stakeholders have in the ability of the contractors in delivering the software on time.

If the stakeholders (all IPT members) were to rate their confidence value on these questions related to the risk item, using the Dempster-Shafter theory, the overall trust rating could increase or decrease the risk. For example, if there were ten members of the IPT and they were all asked to rate their trust value (percentage 0–100) for each question, one would get a confidence value for this risk. Confidence levels of low, medium, and high must be defined prior to performing the confidence level analysis to keep the analysis unbiased. Table 3 provides the confidence level definitions based on the mean value collected from the risk management team confidence ratings.

Table 3. Confidence Level Definitions

Confidence Level	Value
High	0 – 0.30
Medium	>0.30 – 0.70
Low	>0.70 – 100

The confidence level inputs from the risk board members should be evaluated against the programs set confidence level definitions. One must be careful to word the question in a positive way to get the correct percentage. For example, one should ask, "What is your trust level that the s/w programmers can complete the task?" versus "Do you think the s/w programmers can complete the task?" Table 4 presents the synthesized data for this example.

Table 4. Confidence Level Data (Sample Data)

Person	Subjective Trust Value
1	0.4
2	0.3
3	0.6
4	0.5
5	0.8
6	0.3
7	0.4
8	0.5
9	0.6
10	0.5
Total	4.9
Mean	0.49
Result	Medium Confidence

The data does not indicate any conflict and should be considered valid. The resultant trust factor for the confidence element is medium. This process needs to be repeated for the other confidence question. For brevity's sake, assume that the group has a low trust level (0.8) that the program manager has a plan for the s/w development. There are two trust elements from the confidence element that are classified as medium and high.

Next, the stakeholders have to assess whether the risk item has an element of vulnerability. Vulnerability is defined as "the expectation that an exchange partner will not engage in opportunistic behavior, even in the face of countervailing short-term

incentives and uncertainty about long-term benefits" (Chiles and McMackin 1996, 85). Trust is a positive term and vulnerability is more negative so the focus is on the rating of vulnerability toward the working relationship and communication (team cohesion) between the parties. As mentioned before, with respect to the book *5 Dysfunctions of a Team*, a good indication of a partner's vulnerability level is the health of communication between team members. Providing a subjective probability on the working relationship that does not contain conflict data and skew results may be difficult (due to personal friendship bias). Therefore, when assessing the vulnerability of a risk item, it is recommended to use the definitions of high, medium and low vulnerability presented in Table 5.

Table 5. Vulnerability Level Definition

Vulnerability Level (Working Relationship /Team Cohesion)	Definition
High	Worked with this company multiple times on similar scoped efforts, open communication is great
Medium	Work with this company once before on a smaller effort, but they have worked with other agencies, communication is good but not immediate
Low	Never worked with the company before, this is their first effort of this magnitude, communication is bad, employees must always go through supervisor before responding

Examples of vulnerability questions are: 1) Do the s/w programmers personally benefit (i.e., bonuses) from the program's success and/or getting the s/w completed on time? 2) Is the company acting in self-interest, or are they concerned about the success of the program? In addition, this approach to rating vulnerability should also be applied to the relationships between the prime contractor and their sub-contract teams. An example question would be "Are the prime contractor and subcontractor communicating

frequently and well?" For this research example, the program office has never worked with this contractor before, but the contractor has work with other government agencies. During the engineering development phase, the contractor team has identified some s/w problems but hesitates on communicating the problems to the government customer until the manager sets up a formal meeting. Based on this scenario, the IPT risk board members identified two vulnerability risks: lack of experience with contractor and communication slow down. Even though the IPT has not worked with the contractor before, other government agencies have so the risk board members assessed the first vulnerability risk as medium. The delay in communication should start to worry the team, since IPT cannot get direct answers to questions, so the IPT risk board assessed this vulnerability as low.

The risk management team would complete the risk analysis with an assessment of the risk's uncertainties. Uncertainty has a negative connotation, so to keep the ratings consistence with the other ratings, one should rate the level of uncertainty as the predictability level. Uncertainty can be difficult because it is based entirely on the future and what one does not know. Therefore, when assessing the uncertainty of a risk item, it is recommended to use the following default rating scale, see Table 6.

Table 6. Uncertainty Level Definition

Uncertainty Level (Predictability)	Definition
High	Company has multiple experiences with this technology and implementation
Medium	Company has used this technology but not for this application
Low	Company is inexperienced with this technology

For this research example, the program requires converting an old computer language (FORTRAN) to C++. Currently, the software employee staff does not have a FORTRAN software programmer with professional experience. As a result, the risk

management team looks at the uncertainty level definition table and assessed the uncertainty of the contractor to deliver s/w on-time as low because the company has no prior experience with the FORTRAN software language.

The summary of the completed risk analysis of risk item "Delivery of late s/w" is presented in Table 7.

Table 7. Risk and Trust Aggregate Example Summary

Risk Element	
Technical Risk Level	Low
Confidence #1	Medium
Confidence #2	Low
Vulnerability #1	Low
Vulnerability #2	Medium
Uncertainty	Low

Taking all the risk elements and plotting them against the risk reporting matrix, the aggregate would be a medium risk (level 6). For the example, the addition of analyzing trust raised the level of risk. This analysis now gives the program manager more insight into the root cause of the risk and a better ability to manage/mitigate this risk with resources. It is important to note that trust is time dependent, and the level of trust can change rapidly. For example, a troublesome employee could be replaced by someone more competent. This action could improve confidence, vulnerability (working relations) and uncertainty (if the person were a FORTRAN s/w expert). Therefore, risk with trust elements must be monitored on a periodic schedule to manage trends as early as possible.

As a result one can conclude that TRUST must be included as part of the risk management process to accurately identify cost, schedule, and technical risks that may occur in the future of a program.

E. STAKEHOLDER BUY-IN

So this leads into the next consideration, "How will this affect the stakeholders of this process?" All the immediate stakeholders that this process will affect were listed in Table 8. Direct stakeholders are individuals or groups that are engaged in risk management process and the program contract. They include companies, customers, suppliers, government and contractor employees, policy makers, lawyers, and stockholders. Indirect stakeholders were defined as individual or groups who are not engaged in the risk management process and program contract but may be affected by or can affect its actions. They include the general public (tax payers), communities, activist groups, business support groups and the media. After the stakeholders were identified, the stakeholders were ranked based on their impact to the success of the project. The stakeholder requirements, needs and wants, were listed to ensure they were addressed (not necessarily met). Table 8 lists the top three rated stakeholders that this process affects.

Table 8. Stakeholder List

Ranking	Stakeholder	Requirements/Wants/Needs
1	The Integrate Program Team (Gov)	Develop a higher fidelity Risk Management Tool to improve program success Create an unbiased way to measure Risk on program success Deliver a product to the fleet that meets their requirements to complete the mission Deliver a quality product at the lowest cost as quickly as possible Quickly identify high risk tasks that may impede the program to meet cost and schedule Spend less time in meetings
	The Program Executive Office	
	Contractor Business Team	Win the contract to make a profit Deliver a product to the fleet that meets their requirements to complete the mission Deliver a quality product as quickly as possible to build a good company reputation
	Contractor IPT	
2	Tax Payers	Protect my tax dollars with a good investment decision
	Fleet Operators	Provide a quality product quickly at the lowest cost Provide a product that meets my requirements to complete my mission
	DOD Contracts	Ensure all the requirements are being met Ensure the contractor is fulfilling his obligations Quickly identify contract disagreements

Implementing the risk and trust aggregate risk process will likely be met with aversion and skepticism. The proposed change of incorporating trust to the current risk management process for DOD acquisition is an evolution change and therefore can be implemented rather easily with little training or disruption to the work culture of risk management. The addition of the trust element emphasizes the need for good communication and team cohesion. As trust builds, less time is required on monitoring each other, so validating progress and decisions can be made faster. These notions are supported by Naval Air Systems Command leadership of staying focused on the intent of the process and not over burdening the team in an effort to deliver a product to the fleet faster.

This chapter evaluated the feasibility and value of incorporation trust into the DOD risk management process. Through logic and psychometrics studies of risk and trust, it was determined that risk and trust were inversely related. The Dempster-Shafer theory was used to prove that trust elements could be added long as there is no major conflict between the sources. The principle of indifference (Keynes 1921) supported the theory that each element should be weighed equally since we have no idea which element is more plausible. Alexander McNeil's (2005) research on the axiom of coherence was applied to conclude that risk and trust elements were additive. Gary Langford's (2007) method for managing complexity warranted the use of geometric relationships to combine risk and trust into a matrix report. A detailed step-by-step example of how to take a risk item through the proposed risk and trust management process for DOD acquisition was described. Qualitative assessment measurement definitions for all three trust elements; confidence, vulnerability, and uncertainty were created. The risk management example highlighted how a risk item that was assessed quantitatively as a low risk was raised to a medium risk when qualitative measurements (trust) were included in the evaluation. A stakeholder analysis was conducted to assess the impact of incorporating trust and the potential buy-in. The following chapter will examine a case study of the Boeing 787 Dreamliner to support the value of incorporating trust into the risk management process.

THIS PAGE INTENTIONALLY LEFT BLANK

V. BOEING 787 DREAMLINER CASE STUDY

The Boeing 787 Dreamliner case study will be used as a qualitative research tool to evaluate the whether trust is a valuable factor in the risk assessment process in identifying qualitative risk elements. The acceptance of using case studies as a legitimate research technique is still debatable. The following sections will provide a brief history of case study research, define case study and provide rationale for using a case study under certain conditions. The Boeing 787 Dreamliner case study was evaluated against the Robert Yin's research on case study design and methods (Yin 2009) and Gary Langford's research on engineering methods (Langford 2012). Once validated, the Boeing 787 Dreamliner case study was used to evaluate the research question of how the addition of trust could serve to identify qualitative risks to facilitate better management decisions. Figure 10 presents a picture of the Boeing 787 Dreamliner aircraft.

Figure 10. Boeing 787 Dreamliner

A. VALIDATION OF CASE STUDY RESEARCH

1. History of Case Studies

It can be difficult to conduct qualitative research because of its exploratory and subjective nature. There is only so much quantitative research and quantitative data that can be found and analyze in order to validate social theories. That is why case study research has been valuable to the field of qualitative research in social sciences. Case studies allowed social sciences to study human behavior from different aspects and

perspectives. However, the acceptance of using case studies has been debated since the early 1900s as a legitimate research technique (Tellis 1997). The first generation of case studies culminated in the Chicago school of sociology, in which the anthropologist's field study method was practiced (Platt 1992). Chicago was the center for immigration and industry in the 1920s, which allotted it various ethnical backgrounds and poverty levels for the university social researchers to study (Hamel et al. 1993). After the Second World War, social science became dominated by the aspiration for quantitative analysis, called positivism. These positivism advocates called case study research soft science and criticized the methodology for not being scientific because of its qualitative nature. To avoid criticism, a majority of social science researchers went back to taking surveys, opinion polls, and developing quasi-experiments. Case study research was mostly dead until Glaser & Strauss introduced Grounded Theory in 1967 (Johansson 2003). Grounded Theory is a disciplined research method that advocated researchers to combine both quantitative and qualitative data to better appreciate the entire context of the research question being analyzed. The social science community seemed to accept this solution and so no significant advancements in the area of promoting case study research were made until the 1980s. Robert Yin took the next step and developed case study methodology to make it a rigorous and repeatable scientific method. He transferred experimental logic into the field of naturalistic inquiry and combined it with qualitative methods. Since the 1990s, there had been as increase in literature on case study methodology (Johansson 2003). Figure 11 depicts the history of case study methodology.

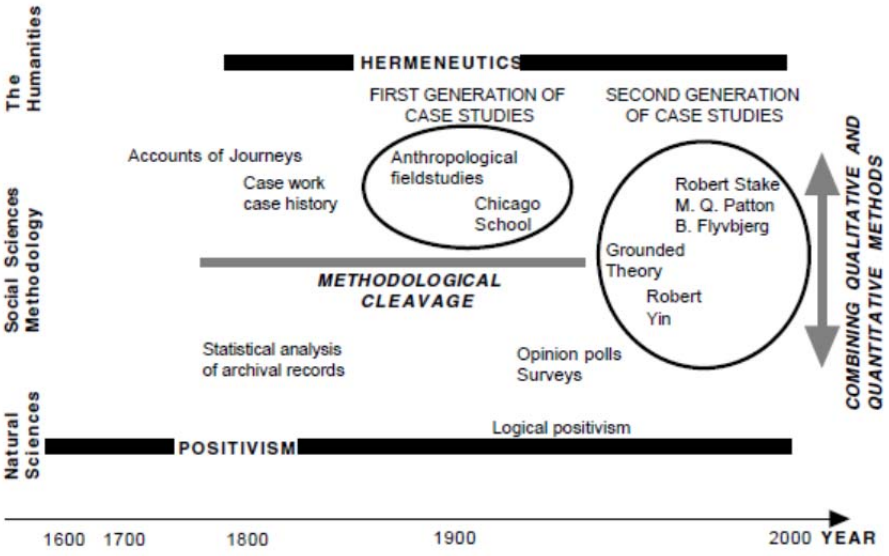

Figure 11. History of Case Study Methodology (from Johansson 2003)

A common criticism of the use of case studies for research is that its dependence on a single case renders it incapable of providing generalizing conclusions because it lacked a sufficient number of relevant examples. Hamel (Hamel et al. 1993) and Yin (1984/1994) forcefully argued that the relative size of the sample whether 2, 10, or 100 cases are used, does not transform a multiple case into a macroscopic study. The goal of the study should establish the parameters, and then should be applied to all research. In this way, even a single case could be considered acceptable, provided it met the established objective (Tellis 1997). Yin is one of the leaders in case study research and has developed rigorous methods with which a case is constructed. His detailed case study methodology fulfills the three tenets of the qualitative method: describing, understanding, and explaining. Yin continues his research on case studies and case study methodology because he understands the benefits. According to Yin (2003a, 2) "the distinctive need for case studies arises out of the desire to understand complex social phenomena" because "the case study method allows investigators to retain the holistic and meaningful characteristics of real-life events," such as organizational and managerial processes. The benefit can be taken from the following heuristic, "Good decisions come from experience, and experience comes from bad decisions" (Author Unknown). Currently,

case studies are used by multiple disciplines such as: psychology, sociology, political science, anthropology, education, medicine, community planning, and systems engineering. But even with all the current research and field expert backing, the merits of case study research are still debated today.

2. Case Study and Case Study Validation

In order to validate the use of a case study, it is important to define a case study. Yin (2003a, 13–14) defines a case study as "an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident." In other words, a case study is an analysis of a past event that looks at all the processes and behavior conditions that led up to the outcome of that particular event. The Boeing 787 Dreamliner case study fits this definition. The Boeing 787 Dreamliner case study conducted by Yao was a comprehensive empirical study of the actual events, process and facts of the design and manufacturing process of the Boeing 787 Dreamliner aircraft. But a case study is not just a historical account about what had happened. The case study must have a problem for the researcher to solve. To address this defined problem, the researcher must design a research strategy that encompassed the required step to conducting a valid case study. A research design is as a "blueprint" for the research, dealing with at least four problems: what questions to study, what data are relevant, what data to collect, and how to analyze the results (Philliber, Schwab, and Samsloss 1980). To start, the researcher should determine whether the case study will be one of three possible types exploratory, descriptive or explanatory. According to Yin, one needs to classify the type of research question being asked. Research questions that ask the "how" and "why" questions are more explanatory and more likely to lead to the use of case studies, histories, and experiments as the preferred research methods (Yin 2009). For case studies, contemporary events are preferred over historical events because access to research material such as personal interviews, current documentation, and artifacts has not been manipulated over time. The Boeing 787 Dreamliner case study is considered explanatory. The researcher, Yao, was trying to solve the problem of "how and why was the Boeing

787 Dreamliner manufacturing delayed?" According to Yin (2009), a case study should contain fives components of research design:

1. a study's questions;

2. its propositions, if any;

3. its units of analysis;

4. the logic linking the data to the propositions; and

5. the criteria for interpreting the findings.

To this list, Langford adds the following comments about the scope of the research. All events cannot be considered. Therefore, the scope of the research needs to be constructed carefully to capture the causal event that links to the problem. Scope outlines the applicability of the tasks to the research. The scope of a research program determines the completeness for a given event's causal relation to the questions of "how" and "why." Since events have assumptions, those assumptions are tested for validity as part of the determination of validity of the case study based on the event selected. Another way of thinking about scope is that scope is the matchup of the boundaries of the event that are relevant over the life cycle of the problem. The scope of the research deals with the problem as that resulting from a systemic issue that is endogenous to the system. But the boundaries of the scope are less than the boundaries of the research. Scope determines the completeness for a given event in terms of its causal effect on the efficacy of the research, and therefore its validity (Langford 2012).

3. The Boeing 787 Dreamliner

The Boeing 787 Dreamliner first flew on December 15, 2009, under the guidance of the Boeing Test and Evaluation team. However, the path to the world's first delivery to All Nippon Airways on September 25, 2011, was marked by a 40-month delay costing an additional $10 billion. The economic realities of benefit for the Dreamliner customers were to replace the 300–400 passenger Boeing 777 as it was believed to have been too expensive and too slow to return its investment to shareholders" (Flightglobal 2014). The Dreamliner was premised on satisfying a business development strategy of delivering the

aircraft faster, building it better, and making it cheaper (Denning 2013). The result was intended to be a three-phased development approach that first pushed the supply chain to deliver faster, then integrating significantly better performance, which precipitates a redesign for lower cost. Piepenbrock's theoretical framework of Enterprise Architecture, Competitive Dynamics, Industrial Evolution, and Firm Performance (Piepenbrock 2004) summarizes the evolution of businesses based on solid product offerings that inspire customers to purchase. With regard to risk, the concatenation within the Piepenbrock framework is ontologically questionable, as there is a conflict of objectives without incorporating the feedback from one stage to the next. Risk is premised on the likelihood of a problem coupled with the consequence of that problem. Without a feedback mechanism, risk within such a framework would only grow as the project progresses. As with the systems engineering process models without feedback, the requirements stated at the onset of the project were not meant to be changed. As is the case with research-inspired development, requirements posed at the beginning of a project as meant to be changed as a consequence of discoveries made during the progression of the work. The Piepenbrock framework is theoretical and perfectly suitable for traditional risk analyses. However, the notion of trust is missing from the Piepenbrock framework.

The Boeing Case study will be analyzed against Yin's (2009 fives components of research design. The first component required for case study research methodology is a clear case study question. The case study question will guide the entire case study process. As discussed earlier, research questions that ask the "how" and "why" questions are more explanatory and more applicable to case study research. The study question for the Boeing 787 Dreamliner case study was, "how and why was the Boeing 787 Dreamliner manufacturing delayed?" The second component of case study methodology is to determine the propositions. Propositions are similar to thesis research questions, in that they direct attention to a certain location or person(s) that should be examined during research. These questions point the researcher in the direction of where to uncover evidence. There is no hard evidence that Yao created propositions when conducting the Boeing 787 Dreamliner case. However, one can conclude Yao must have created a proposition, since he was able to uncover the cause of the problem and obtained enough

empirical evidence to substantiate his claims. The third component of case study methodology is the unit of analysis. The unit of analysis is described as the case that is being solved. The researchers need to identify whether they are investigating a group of people, a single individual, or company. The unit of analysis should be related to the initial study question so it will help focus the researcher's proposition questions on the case being examined. For the Boeing 787 Dreamliner case study, the researcher's unit of analysis was the 100 outsourcing suppliers that Boeing had contracted for aircraft development and manufacturing. The fourth step to case study methodology is linking data to the previous propositions. During this phase, the researcher has taken all the data that is collected and is trying to discover patterns or collaborative details to support the research question. Common methods for linking data found during the case study to propositions are pattern matching, explanation building, time-series analysis, logic models, and cross-case synthesis (Yin 2009). For the Boeing case study, Mr. Zhao used "an integrated empirical-analytical approach where we combine a comprehensive empirical study of the actual events and facts with an economic analysis of financial incentives, gaming and risk in joint development programs" (Zhao 2012, 2). The fifth component for case study methodology is the criteria for interpreting a case study's findings. A major and important alternative strategy is to identify and address rival explanations for the findings (Yin 2009). In other words, the researcher has to be prepared that the same scenario may be interpreted and/or explained opposing ways from multiple sources. As a result, the researcher must decide on which source will have greater weight in a given scenario prior to the data collection and analysis. Yao reconciled the qualitative analysis with practical evidence. He compared the data that was collected to the actions of the suppliers. The "reconciliation clearly shows that the delays occurred not because the suppliers weren't able to do their jobs well but because they just didn't want or care enough to do it well" (Zhao 2012, 12).

The Boeing Case study will be evaluated against the Langford's (2012) scope component of case study research methodology. The scope can be defined as the work that is necessary to complete the project, the case study research. The scope of a research program determines the completeness for a given event's causal relation to the questions

of "how" and "why" (Langford 2012). The Boeing 787 case study covered the 787 development background, the development chain, the management of the supply chain, the delay events, and an economic analysis. The background study of the Boeing case study was used to develop the proposition links by defining all the piece and process that were used to manufacture the test article. The development (supply) chain was analyzed to determine how the outsourcing structure was used and how well it was being managed. Each identified delay event (such as insufficient fasteners) was analyzed to subsidize the supply chain and management process research to develop a complete picture of what really happened. An economic analysis was conducted "to understand the firms' financial incentives and unveil the trap induced by the risk sharing partnership" (Zhao 2012, 2). Since all events cannot be considered, assumptions must be made and tested for validity as part of the determination of validity of the case study (Langford 2012). One of the assumptions made Boeing was confident in their partnerships. There is no direct evidence in the confidence level of Boeing with its suppliers; however, Boeing did delegate all responsibility to the Tier one suppliers for design and integration. The second assumption made was that Boeing and the suppliers were following good business practice of trying to make money. It was determined "that each firm tried to delay behind the schedule or passed its unfinished work to others because by doing so, it can save its direct costs" (Zhao 2012, 13).

In summary, the Boeing 787 Dreamliner case study met all the criteria for being classified as a case study. The case study research followed the rigorous methodology accepted by the field of social science and documented by the leading case study researcher Yin. The case study researcher had no financial ties to any of the stakeholders. The conclusions were based on a triangulated research collection of interview, artifacts, and documentation. Therefore, the Boeing 787 case study can be considered valid for future research studies to use.

B. BACKGROUND OF THE 787 DREAMLINER PROGRAM

The 787 Dreamliner was "Boeing's next generation commercial aircraft targeted at the aviation market segment of rapid, direct and point-to-point connections" (Zhao

2012, 2). The 787 is a mid-sized aircraft that seats between 250–310 people. "The Dreamliner is unique in its extensive use of the lightweight composite materials, which accounted for about 50% of the airplane by weight, and 80% by volume" (Teresko 2007; Zhao 2012, 2). Overall, "the Boeing 787 Dreamliner was designed to cost less to operate and maintain than the current generation aircrafts" (Zhao, 2012, 2). In order to optimize the sales of the 787 Dreamliner, Boeing decided to use a global approach to the design, development, and manufacturing of the 787 Dreamliner commercial aircraft. Boeing had thought that if countries would be more willing to buy an aircraft in which that country had economic ties. As a result, the 787 Dreamliner had an unprecedented scale of development outsourcing— 65 percent of the development work was outsourced to more than 100 suppliers from 12 countries (Exostar 2007; Horng and Bozdogan 2007). The Tier 1 suppliers were responsible for design, fabrication, integration and assembly of the components from the Tier 2 and 3 suppliers. Figure 12 shows a breakout of the Tier 1 suppliers.

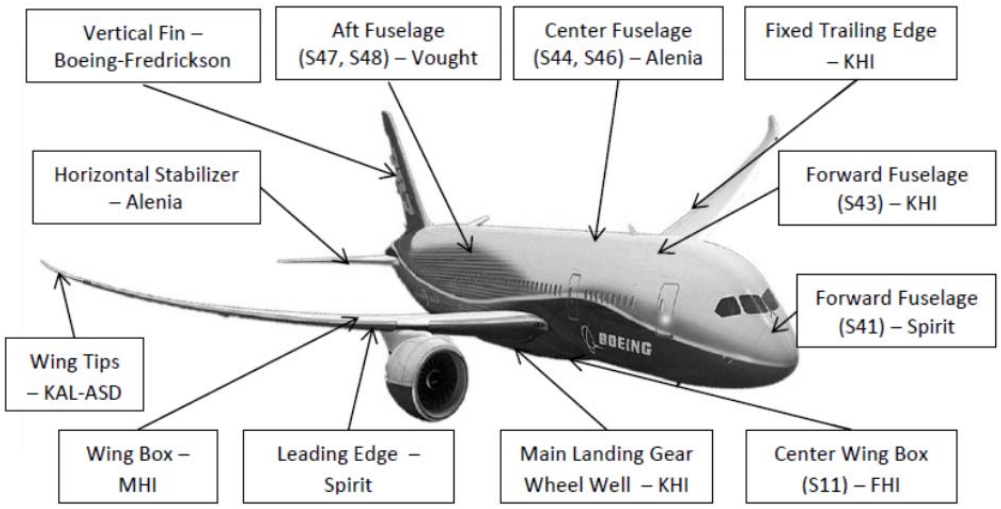

Figure 12. Tier 1 Suppliers for the Boeing 787 Dreamliner (from Zhao 2012)

In addition, Boeing also wanted to share the economic risk of such a big development effort with other countries in the event the 787 Dreamliner was a failure. The concept was that "suppliers share more than half of the upfront non-recurring R&D

investment (Lee and Anupindi 2009), which can be broken down as follows: Alenia ($590 million), Japanese Heavies ($1.6 billion), Global Aeronautica (GA), Spirit, Vought ($3.1 billion), and Boeing ($4.2 billion)" (Zhao 2012, 5). On paper, this seemed like a good plan. So, what could go wrong?

The consequence was that the "first flight was delayed by 26 months and the first delivery was delayed by 40 months with a cost overrun of at least $10 billion" (Zhao 2012, 1.

C. ANALYSIS OF THE CASE STUDY

The major hurdle derived from multiple companies who were jointly dependent on each other to control cost and maintain schedule. Boeing had to trust its suppliers to meet the schedule deadlines which sometimes meant trusting the other companies to put the 787 Dreamliner project's success over their individual company's success. The problem was that Boeing did not have a plan to manage this issue. As a result there were seven major delays that were recorded to explain the 40-month delay and $10 billion cost overrun.

According to the case study, of the seven major delays, three could be attributed to technical issues, such as bad documentation, structural flaw in engineering design, and underestimated task duration. However, the other four major delays can be attributed to bad program risk management.

1. How Could Trust Have Helped the Boeing 787 Dreamliner Program Risk Management?

The trust factor is valuable in that is does not rely on technical risks to highlight risk items. It opens program managements thinking to linkages/codependences rather than individual event. Below are examples of how using the three elements of trust (confidence, vulnerability, and uncertainty) could have save the Boeing 787 Dreamliner cost and schedule.

a. Confidence

Boeing selected the company "Vought to design and manufacture the world's first all-composite aft-fuselage" (Zhao 2012, 8). However, at the time when selected, Vought had no engineering department. This apparent lack of an organizational recognition of an engineering skill may not have shown up on a typical risk matrix because there is not a technical or quantitative value to place on this item. However, if Boeing were to analyze this item from a trust perspective, it would have identified a low confidence level in selecting this company. If the company were already selected, the fact that Vought had no engineering department would have been identified as a high risk.

b. Vulnerability

For example, Vought waited until nearly the last moment (May 2006) to build the plant (job assigned November 2003, due May 2007). If Boeing were to analyze this item from a trust perspective, it would have realized that this company was not fully invested in the success of the overall 787 Dreamliner project. Boeing could have seen that Vought was putting its company first and only looking to do the bare minimum to fulfill its contract obligation.

c. Uncertainty

The production of the Boeing 787 Dreamliner adopted a new outsourcing model. Boeing opted to employ a tiered structure process that assigned the Tier 1 contractors as lead integrators, responsible for the assembly of different parts and subsystems provided from the Tier 2 and Tier 3 suppliers. This would not have shown up on a typical risk matrix because process was new and there were no quantitative technical measures that would highlight this integration process as a risk. However, if Boeing would have analyzed this from a trust perspective, Boeing would have identified that this process was different from their previous process in which Boeing played the traditional role of integrating and assembling different parts and subsystems. This identification of the risk earlier may have encouraged Boeing to take a bigger role in the integration of the 787 Dreamliner program and prevented some of the schedule and cost over runs.

This chapter defined case study and the process to validate a case study for the purposed of using a case study as a research method. The Boeing 787 case study was validated and reinforced the argument that the incorporation of trust can be a valuable tool in assessing risk without the need for metrics and quantitative values. The following chapter will summarize this research paper with conclusion and recommendations supported by the previous chapters. In addition, several topics for future research studies will be described.

VI. CONCLUSIONS RECOMMENDATIONS, AND AREAS OF FURTHER STUDY

A. CONCLUSION

The purpose of this paper was to determine whether it was feasible and advantageous to incorporate "trust" into the risk management process for DOD acquisition. The premise was that there were hidden risk factors attributed to qualitative measures that were not being identified in the current risk management process. These qualitative measures of risk could be directly linked to trust elements. This research paper presented a sound argument on why trust should be incorporated into the risk management process for DOD acquisition programs. Various social, behavioral, theological, and technical expert definitions on the term trust were used to decompose trust into three key elements: confidence, vulnerability, and uncertainty. The three trust elements: confidence, vulnerability and uncertainty, were further defined and correlated with current industry program risk management practices. Based on the analysis of the three trust elements, trust was define for the purpose and use in risk management. Trust for risk management was defined as the subjective probability of a positive outcome from an agreement between two or more parties for a domain specific task based on the capability and goodwill of the trustee and predictability of a positive outcome within the defined technical, cost and schedule boundaries.

Industry is starting to adopt qualitative risk management. Modernization of communication paths (i.e., e-mail and video teleconferencing), and quick technology advancement have opened industry to new partners in a global economy. In addition, there has also been an influx of business corruption that has left people and companies skittish about openly trusting their partners. New business partners lead to possible confidence, vulnerability, and uncertainty concerns. Companies have to weigh these trust elements when entering new partnerships and throughout the contract. To accentuate the point of global business partnership trust based risks, this research paper analyzed a case study on the Boeing 777 Dreamliner program which had an unprecedented scale of development outsourcing— 65 percent of the development work was outsourced to more

than 100 suppliers from 12 countries (Exostar 2007; Horng and Bozdogan 2007). A validation of the case study was conducted against Robert Yin's research on case study design and methods (Yin 2009) and Gary Langford's research on engineering methods (Langford 2012). The case study was concluded as valid and appropriate for analysis for the topic of this research on trust in risk management. The analysis of the case study determined there was risk items associated with each trust element (confidence, vulnerability, and uncertainty) that could have been identified earlier if trust had been incorporated into Boeing's risk management process.

Research was also conducted on the feasibility of incorporating the trust elements of risk into the risk management process for DOD acquisition. The relationship between trust and risk was defined from social science research and scientific methods. By examining social science research, it was determined that to capture the likelihood and consequence of an action that requires dependence on other individuals to take action, the element of trust should be assessed. Through logic and psychometrics studies of risk and trust, it was determined that risk and trust were inversely related. The Dempster-Shafer theory was used to prove that trust elements could be added long as there is no major conflict between the sources. The principle of indifference (Keynes 1921) supported the theory that each element should be weighed equally since we have no idea which element is more plausible. Alexander McNeil's (2005) research on the axiom of coherence was applied to conclude that risk and trust elements were additive. However, the process is not simple mathematical addition, since trust and risk are inversely related. Gary Langford's (2007) method for managing complexity warranted the use of geometric relationships to combine risk and trust into a matrix report.

The current Risk Management Guide for DOD Acquisition (DOD 2006) was studied and the process was decomposed to determine how and where the qualitative measures (trust factors) of risk could be addressed. The most practical place for the trust elements of risk to be analyzed was during the analysis of the quantitative measurement of risk. A detailed step by step example of how to take a risk item through the proposed risk and trust management process for DOD acquisition was described. Qualitative assessment measurement definitions for all three trust elements; confidence,

vulnerability, and uncertainty were created. Example questions were also provided to assist in identifying trust risks. The risk management example highlighted how a risk item that was assessed quantitatively as a low risk was raised to a medium risk when qualitative measurements (trust) were included in the evaluation.

In conclusion, this research paper posits that the incorporation of trust into the risk management process for DOD acquisition is feasible and advantageous. The proposed risk and trust management process will provide the program manager more insight into the root cause of the risk. Clearer insight into the root cause will aid in management of risk and resource allocation for mitigating risk.

B. RECOMMENDATIONS

Based on the research and case study analysis it is recommend that trust be incorporated into the risk management process for DOD acquisition. The process as outlined in Chapter IV should be added to the Risk Management Guide for DOD Acquisition. This process will only enhance a program manager's ability to understand the root cause of a risk item and properly mitigate the risk.

C. AREAS OF FURTHER STUDY

There is a vast amount of data and research that has been completed on the topic of trust. Due to time constraints and the abundance of information, all the topics related to this research could not be explored. Identified topics related to trust that may be worthy of future studies or analysis are provided below.

1. The Risk of Firm Fixed Price vs. Cost Plus Incentive Fee Contracts

There is an element of trust and risk involved in the decision of going with a Firm Fixed Price or Cost Plus Incentive Fee DOD acquisition contract. Generally, for a cost plus incentive fee DOD acquisition contract, the government assumes risk because the contractor can get more money if the program falls behind schedule or runs over cost. However, for a firm fixed price DOD contract, the contractor assumes most of the risk because there is no money to be gained if a program falls behind schedule or runs over

budget. However, a contractor may decide to terminate the contract if the company loses too much money on the program. In both cases, the government must trust the contractor.

2. Analysis Qualitative + Quantitative Risk Management Results in the Commercial Business World

It would be valuable to research companies that have included both qualitative and quantitative risk management practices into their business decision making process to determine whether it had a positive outcome. Asian companies appear to have the most experience with qualitative risk assessment. It would also be valuable to highlight some lessons learned using trust and risk factor based decision making.

3. Analysis of Whether a Program That Places More Emphasis on Trust than Risk is More Efficient

Most experts claim that a high level of trust allows for good communication and faster decision making. But blind trust can be equally damaging if unchecked. It would be interesting to determine if there is an optimum level of trust that will allow a program to be more efficient and how that level can be achieved.

APPENDIX. BOEING 787 DREAMLINER CASE STUDY

The 2012 Boeing 787 Dreamliner case study, by Yao Zhao, PhD, Associate Professor in Supply Chain and Project Management Rutgers, the State University of New Jersey, may be read in its entirety on the web using the following link:

http://zhao.rutgers.edu/787-paper-12-02-2013.pdf

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, John. 1995. *Risk*. London England: UCL Press, 1995.

Amendola, Aniello. 2002. "Recent paradigms for risk informed decision making." *Safety Science* 40, no. 1–4 : 17–30. Accessed January 20, 2014. http://dx.doi.org/10.1016/S0925-7535(01)00039-X.

Barney, Jay B., and Mark H. Hansen. 1994. "Trustworthiness as a Source of Competitive Advantage." *Strategic Management Journal* 15.S1: 175–190.

Bhattacharya, Rajeev, Timothy M. Devinney, and Madan M. Pillutla. 1998. "A Formal Model of Trust Based on Outcomes." *The Academy of Management Review* 23, no. 3, 459–472.

Boon, Susan D., and John G. Holmes. 1991. "The Dynamics of Interpersonal Trust: Resolving Uncertainty in Face of Risk." In *Cooperation and Prosocial Behavior.* Cambridge, UK: Cambridge University Press.

Castelfranchi, Cristiano, and Rino Falcone. 2000. "Trust is Much More than Subjective Probability: Mental Components and Sources of Trust." *In 32nd Hawaii International Conference on System Sciences - Mini-Track on Software Agents* (1–10). www.eecis.udel.edu/~decker/courses/886f04/pubs/castelfranchi00.pdf.

Chiles, Todd H., and John F. McMackin. 1996. "Integrating Variable Risk Preferences, Trust and Transaction Cost Economics." *The Academy of Management Review* 21, no. 1, 73–99.

Coleman, James Samuel. 1990. *Foundations of Social Theory*. Cambridge, MA: Harvard University Press.

Das, T. K., and Bing-Sheng Teng. 2001. "Relational Risk and its Personal Correlates in Strategic Alliances." *Journal of Business and Psychology*, 15, 445–461.

——— 2004. "The Risk-Based View of Trust: A Conceptual Framework." *Journal of Business and Psychology* 19, no. 1: 85–116.

Denning, Steve. 2013. "What Went Wrong At Boeing?." *Forbes*. Accessed August 14, 2014. http://www.forbes.com/sites/stevedenning/2013/01/21/what-went-wrong-at-boeing/.

Department of Defense (DOD). 2006. *Risk Management Guide for Department of Defense Acquisition*, v 1.0. http://www.acq.osd.mil/se/docs/2006-RM-Guide-4Aug06-final-version.pdf.

Deutsch, Morton. 1962. In *Nebraska Symposium on Motivation,* edited by Jones, Marshall Red. 275-320. Oxford, England: University of Nebraska Press.

Dictionary.com. 2014. s.v. "Trust." Accessed August 1, 2014. http://dictionary.reference.com/etymology.

Exostar, LLC. 2007. "Boeing 787: Global Supply Chain Management Takes Flight." http://www.exostar.com/WorkArea/DownloadAsset.aspx?id=684.

Flightglobal. 2014. "The Boeing 787 Dreamliner Debut - The Story So Far". Accessed August 14, 2014. http://www.flightglobal.com/features/787-handover/story-so-far.

Fukuyama, Francis. 1995. *Trust: The Social Virtues and the Creation of Prosperity*. New York Free Press. 26.

Gambetta, Diego. 1988. *Trust: Making and Breaking Cooperative Relations*. New York: Basil Blackwell. 213–237.

Gerck, Ed. 1998. "Trust Points." In *Digital Certificates: Applied Internet Security*, edited by Jalal Feghhi, Jalil Feghhi and Peter Williams 194–195. Reading, MA: Addison-Wesley.

Grunert, Jens, Lars Norden, and Martin Weber. 2005. "The Role of Non-financial Factors in Internal Credit Ratings." J*ournal of Banking & Finance* 29, no. 2: 509–531.

Hamel, Jacques, Stéphane Dufour, and Dominic Fortin. 1993. *Case Study Methods.* Newbury Park: Sage Publications.

Hamlett, Kenneth. 2014. "Reasons for Outsourcing in a Manufacturing Industry." *Chron*. Accessed July 21, 2014. http://smallbusiness.chron.com/reasons-outsourcing-manufacturing-industry-1292.html.

Horng, Tzu-Ching, and Kirk Bozdogan 2007. "Comparative Analysis of Supply Chain Management Practices by Boeing and Airbus: Long-term Strategic Implications." Presentation at the MIT Lean Aerospace Initiative, Monterey, CA, April 18.

Johansson, Rolf. 2003. "Case Study Methodology." Keynote speech. International Conference on Methodologies in Housing Research. Stockholm, Sweden. September 22–24.

Karahannas, Marios, and Matthew Jones. 1999. "Interorganizational Systems and Trust in Strategic Alliances." *ICIS 1999 Proceedings*. Paper 32. http://aisel.aisnet.org/icis1999/32.

Keynes, John Maynard. 1921. *A Treatise on Probability*. London: Macmillan and Co., Limited.

Langford, Gary. 2012. *Engineering Systems Integration Theory, Metrics, and Methods*. Boca Raton: CRC Press.

Langford, Gary, and Thomas Huynh. 2007. "A Methodology for Managing Complexity," Systems Engineering Test and Evaluation SETE Conference, Complex Systems and Sustainability, 24–27 September, Sydney, Australia. Paper published and archived, SETE Conference Proceedings.

Lee, Moses, and Ravi Anupindi. 2009. "Boeing: the Fight for Fasteners." Tauber Institute Case 1–428–787, November 17.

Lencioni, Patrick. 2002. *The Five Dysfunctions of a Team, a Leadership Fable.* San Francisco. Jossey-Bass.

Luhmann, Niklas. 1979. *Trust and Power: Two Works*. Chichester: John Wiley.

Mannai, Al, Waleed Al Mannai, and Ted Lewis. 2007. "Minimizing Network Risk with Application to Critical Infrastructure Protection." *Journal of Information Warfare* 6, 2, 52–68.

Markon, Jerry, and Alice Crites. 2013. "Health-care Website's Lead Contractor Employs Executives from Troubled IT Company." *The Washington Post*. Accessed November 15, 2013. http://www.washingtonpost.com/politics/health-care-web-sites-lead-contractor-employs-executives-from-troubled-it-company/2013/11/15/6e107e2e-487a-11e3-a196–3544a03c2351_story.html.

Marzec, Evangeline. 2014. "Why Do Companies Outsource Manufacturing?." *eHow*. Accessed June 5, 2014. http://www.ehow.com/facts_5876212_do-companies-outsource-manufacturing_.html.

Massie, Suzanne. 2013. *Trust but Verify: Reagan, Russia and Me: A Personal Memoir*. Rockland, Maine: Maine Authors Publishing.

McNeil, Alexander J., Rüdiger Frey, and Paul Embrechts. 2005. *Quantitative Risk Management: Concepts, Techniques and Tools*. Princeton, N.J.: Princeton University Press. Print.

Merriam-Webster, 2014. s.v. "Distrust." Accessed June 27, 2014. http://www.merriam-webster.com/dictionary/distrust.

Merriam-Webster, 2014. s.v. "Trust." Accessed June 27, 2014. http://www.merriam-webster.com/dictionary/trust.

Ojala, Mika, and J Hallikas. 2006. "Investment Decision-Making in Supplier Networks: Management of Risk." *International Journal of Production Economics* 104, 201–213.

Phillibber, Susan Gustavus, Mary R. Schwab, and G. Sam Sloss. 1980. *Social research*. Itasca, Illinois: F. E. Peacock Publishers.

Piepenbrock, Ted. 2004. "Enterprise Design for Dynamic Complexity: Architecting & Engineering Organizations using System & Structural Dynamics," Master's thesis, Massachusetts Institute of Technology. http://dspace.mit.edu/handle/1721.1/34777.

———. 2009. "The Architecture and Evolution of World-Class Enterprises," Second International Engineering Systems Symposium, 15–17 June. Massachusetts Institute of Technology, INCOSE.

Platt, Jennifer. 1992. "Case Study" in American Methodological Thought." *Current Sociology*. 40, no. 1: 17–48.

Riege, Andreas M. 2003. "Validity and Reliability Tests in Case Study Research: A Literature Review with "Hands-on" Applications for Each Research Phase." *Qualitative Market Research*: *An International Journal.* 6.2. 75–86.

Sentz, Kari, and Scott Ferson 2002. "Combination of Evidence in Dempster-Shafer Theory." Master's thesis, Binghamton University.

Shafer, Glenn. 1976. *A Mathematical Theory of Evidence*. Princeton, N.J.: Princeton University Press.

Shore, Howard. 2012. "Understanding the Levels of Trust," Activate Group Inc. http://www.activategroupinc.com/2012/10/understanding-the-levels-of-trust/.

Siegrist, Michael, Timothy C. Earle, and Heinz Gutscher. 2010. *Trust in Risk Management Uncertainty and Scepticism in the Public Mind*. London [u.a.] Earthscan.

Sztompka, Piotr. 1999. *Trust a Sociological Theory*. Cambridge, UK [u.a.] Cambridge University Press.

Tellis, Winston. 1997. "Application of a Case Study Methodology." *The Qualitative Report*. 3. No 2. July 1997. http://www.nova.edu/ssss/QR/QR3–2/tellis1.html.

Teresko, John. 2007. "The Boeing 787: A Matter of Materials -- Special Report: Anatomy of a Supply Chain." *Industry Week*. http://www.industryweek.com/articles/boeing_787_a_matter_of_materials_--_special_report_anatomy_of_a_supply_chain_15339.aspx.

Visual Thesaurus. 2014. s.v. "Trust." Accessed July 11, 2014. http://www.visualthesaurus.com/browse/en/trust.

Williamson, Oliver. 1985. *The Economic Institutions of Capitalism*. The Free Press. New York.

Witzel, Eddy. 2014. "Wheel of Innovation: How leaders Attitudes and Behaviors Drive Disruptive Technology in the U.S. Navy." PhD diss., Andrews University.

Yin, Robert. 1984/1994. *Case Study Research: Design and Methods*. Thousand Oaks, London, New Delhi: Sage.

Yin, Robert K. 2003a. *Case study research, design and methods*. Thousand Oaks: Sage Publications. 3. 5.

———. 2009. *Case Study Research: Design and Methods*. Thousand Oaks, Calif.: Sage Publications. 4.

Zhao, Yao. 2012. "Why 787 Slips Were Inevitable?" http://zhao.rutgers.edu/787-paper-12–02–2013.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California