NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPROVING SPAWAR PEO C4I ORGANIZATIONAL ALIGNMENT TO BETTER ENABLE ENTERPRISE TECHNICAL RISK MANAGEMENT

by

Steven C. Crosson

March 2017

Thesis Advisor: Mark Rhoades
Co-Advisor: Deborah Gibbons

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE IMPROVING SPAWAR PEO C4I ORGANIZATIONAL ALIGNMENT TO BETTER ENABLE ENTERPRISE TECHNICAL RISK MANAGEMENT			**5. FUNDING NUMBERS**
6. AUTHOR(S) Steven C. Crosson			
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 is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This thesis examined how the Navy's Program Executive Office Command, Control, Communications, Computers and Intelligence (PEO C4I) has performed enterprise risk management (ERM). Based on ERM literature, the study developed an analytical framework to assess PEO C4I's ERM practices against documented ERM best practices, including evaluating a new risk in terms of its impact on existing risks and ensuring risks are managed at the most detailed level possible. The thesis also utilized organizational alignment literature to include organizational alignment principles in the evaluation. Key principles include 1) every employee has the responsibility to manage risk and 2) multiple teams are able to manage a single risk. The resultant analytical framework was applied to PEO C4I and documented for application to other organizations. PEO C4I performed well in the areas of 1) evaluating risks in areas other than the originating program office and 2) providing the framework to elevate risks to leadership. PEO C4I could use improvement in cross-team risk coordination and development of enterprise models to provide context for enterprise risks. Recommended interventions focus on having more functional areas involved in risk mitigation and developing a common enterprise architecture to improve understanding of potential areas of risk.

14. SUBJECT TERMS organizational alignment, enterprise risk management, DOD risk management			**15. NUMBER OF PAGES** 113
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** 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 is unlimited.

IMPROVING SPAWAR PEO C4I ORGANIZATIONAL ALIGNMENT TO BETTER ENABLE ENTERPRISE TECHNICAL RISK MANAGEMENT

Steven C. Crosson
Civilian, Department of the Navy
B.C.E., University of Delaware, 2004
M.S., Monmouth University, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2017

Approved by: Mark Rhoades
Thesis Advisor

Deborah Gibbons
Co-Advisor

Ronald Giachetti
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examined how the Navy's Program Executive Office Command, Control, Communications, Computers and Intelligence (PEO C4I) has performed enterprise risk management (ERM). Based on ERM literature, the study developed an analytical framework to assess PEO C4I's ERM practices against documented ERM best practices, including evaluating a new risk in terms of its impact on existing risks and ensuring risks are managed at the most detailed level possible. The thesis also utilized organizational alignment literature to include organizational alignment principles in the evaluation. Key principles include 1) every employee has the responsibility to manage risk and 2) multiple teams are able to manage a single risk. The resultant analytical framework was applied to PEO C4I and documented for application to other organizations. PEO C4I performed well in the areas of 1) evaluating risks in areas other than the originating program office and 2) providing the framework to elevate risks to leadership. PEO C4I could use improvement in cross-team risk coordination and development of enterprise models to provide context for enterprise risks. Recommended interventions focus on having more functional areas involved in risk mitigation and developing a common enterprise architecture to improve understanding of potential areas of risk.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. IMPORTANCE OF ENTERPRISE RISK MANAGEMENT—PROBLEM STATEMENT....1
B. ALIGNING ORGANIZATIONAL STRUCTURES IN DOD....2
C. OVERVIEW OF PEO C4I ETRB....4
D. ANALYSIS STRATEGY....6
E. LITERATURE REVIEW....9
1. Organizational Alignment....9
2. Risk Management....11
F. OVERVIEW OF CHAPTERS....13

II. ORGANIZATIONAL STRUCTURES....15
A. COMMON STRUCTURES....16
1. Functional Organizations....16
2. Product Organizations....19
3. Considerations for the PEO C4I ETRB....21
B. RISK MANAGEMENT EMPHASIS IN ORGANIZATIONAL STRUCTURES....23
1. Employee Responsibility and Accountability....23
2. Cross-team Coordination....24
3. Multiple Team Risk Ownership....25
4. Enterprise Definition of Risk Management Practices and Risk Areas....26
5. Evaluating Risks in Areas Other Than Your Own....27
C. ANALYSIS OF POSITIONS ASSOCIATED WITH PEO C4I ETRB....28
1. Employee Responsibility and Accountability....28
2. Cross-team Coordination....31
3. Multiple Team Risk Ownership....32
4. Enterprise Definition of Risk Management Practices and Risk Areas....33
5. Evaluating Risks in Areas Other Than Your Own....35
D. CHAPTER SUMMARY....36

III. ENTERPRISE RISK MANAGEMENT....39
A. CORE PRINCIPLES....39
B. RELATIONSHIP OF CORE PRINCIPLES TO ENTERPRISE IMPLEMENTATION....41

1. Ability to Consider Short-Term and Long-Term Impacts of Risks 41
2. Evaluating a New Risk with Regard to its Impact on Existing Risks 42
3. Risks Managed at the Most Detailed Level Possible 43
4. Presence of Enterprise Engineering Models or Architectures to Provide Objective Context for Technical Risk 45
5. Risks Evaluated with Context of System Position in Acquisition Life-Cycle 45
6. Assessment of Ability to Mitigate Risk in Current Enterprise Architecture 47

C. ANALYSIS OF RISK MANAGEMENT PRINCIPLES APPLIED IN PEO C4I ETRB 48
1. Ability to Consider Short-Term and Long-Term Impacts of Risks 48
2. Evaluating a New Risk with Regard to its Impact on Existing Risks 50
3. Risks Managed at the Most Detailed Level Possible 52
4. Presence of Enterprise Engineering Models or Architectures to Provide Objective Context for Technical Risk 53
5. Risks Evaluated with Context of System Position in Acquisition Life-Cycle 55
6. Assessment of Ability to Mitigate Risk in Current Enterprise Architecture 56

D. CHAPTER SUMMARY 58

IV. RECOMMENDATIONS FOR PEO C4I ETRB 61

A. ORGANIZATIONAL STRENGTHS, WEAKNESSES AND RECOMMENDATIONS 61
1. Strengths 61
2. Weaknesses 63
3. Neutral 65
4. Recommendations 66

B. ENTERPRISE RISK MANAGEMENT STRENGTHS, WEAKNESSES AND RECOMMENDATIONS 70
1. Strengths 70
2. Weaknesses 71
3. Neutral 72
4. Recommendations 75

C. LIMITATIONS OF ANALYSIS 77

D. CHAPTER SUMMARY 78

V. CONCLUSIONS AND FUTURE RESEARCH 81
A. CONCLUSIONS 81
B. POTENTIAL FUTURE RESEARCH 83

APPENDIX. ENTERPRISE RISK MANAGEMENT EVALUATION MATRIX 85

LIST OF REFERENCES 87

INITIAL DISTRIBUTION LIST 89

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. DOD Organizational Structure. Source: DCMO (2015).....3

Figure 2. PEO C4I Organizational Structure. Source: PEO C4I (2014). 5

Figure 3. Core Functional and Product-Aligned Portions of PEO C4I Organization. Adapted from PEO C4I (2014). 22

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Key Attributes of Organizational Positions. Adapted from Kerzner (2013). 15

Table 2. PEO C4I ETRB Evaluation—Organizational Alignment Criterion #1 30

Table 3. PEO C4I ETRB Evaluation—Organizational Alignment Criterion #2 31

Table 4. PEO C4I ETRB Evaluation—Organizational Alignment Criterion #3 33

Table 5. PEO C4I ETRB Evaluation—Organizational Alignment Criterion #4 34

Table 6. PEO C4I ETRB Evaluation—Organizational Alignment Criterion #5 36

Table 7. PEO C4I ETRB Evaluation—Enterprise Risk Management Criterion #1 49

Table 8. PEO C4I ETRB Evaluation—Enterprise Risk Management Criterion #2 51

Table 9. PEO C4I ETRB Evaluation—Enterprise Risk Management Criterion #3 52

Table 10. PEO C4I ETRB Evaluation—Enterprise Risk Management Criterion #4 54

Table 11. PEO C4I ETRB Evaluation—Enterprise Risk Management Criterion #5 55

Table 12. PEO C4I ETRB Evaluation—Enterprise Risk Management Criterion #6 57

Table 13. Summary of Organizational and Risk Management Alignment Recommendations 82

Table 14. Organizational Alignment and Risk Management Evaluation Criteria 85

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APEO-E	assistant program executive officer—engineering
APM-E	assistant program manager—engineering
ATL	acquisition, technology and logistics
C4I	command, control, communication, computers and intelligence
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CRO	chief risk officer
DAU	Defense Acquisition University
DOD	Department of Defense
ERM	enterprise risk management
ETR	enterprise technical risk
ETRB	Enterprise Technical Risk Board
JCIDS	Joint Capabilities Integration and Development System
OSD	Office of the Secretary of Defense
PEO	program executive office
PGB	Portfolio Governance Board
PM	program manager
PMW	program manager warfare
SEB	Systems Engineering Board
SOP	standard operating procedure

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Risk management is a critical aspect of managing any program. This is especially true in the Department of Defense (DOD); there is an official DOD publication specifically aimed at providing guidance for managing risks within acquisition programs. As defense systems become less stove-piped and require greater system-of-systems interoperability, risk management must also expand to consider potential risks beyond any single system boundary. These risks could be technical, schedule, or cost driven, but any cross-system dependency requires cross-system risk management.

To this end, DOD, as well as businesses in many other industries, are turning toward enterprise risk management. Enterprise risk management includes a broader and more strategic set of specific risk management principles and best practices; also it is dependent on a foundational shift in organizational alignment to ensure that best practices may be implemented to their fullest. This is true regardless of whether the organization is functionally or product-aligned, or a hybrid of both.

In order to implement an enterprise risk management strategy, an organization must first understand its current strengths and weaknesses. Viewed strictly from the perspective of more fully managing risk, both functional- and product-aligned organizations have strengths and weaknesses. There is much historical and current research on what organizational structures best support meeting specific performance goals, and some of the aspects that are focused on maximizing a risk management strategy may not directly align with maximizing other organizational functions.

For this study, the focus was on how to set up an evaluation framework to determine how well aligned an organization was to implement enterprise risk management best practices. The Navy's program executive office (PEO) for command, control, communications, computers and intelligence (C4I) was chosen as a case study for utilizing the proposed criteria. The PEO has a decidedly hybrid organizational structure, which includes several product-aligned program offices as well as a set of functionally aligned specialty organizations both at the PEO level as well as embedded in

the program offices. The enterprise risk management effort is strongly aligned to the PEO engineering functional organization, an alignment that provides many benefits for analyzing technical risks but also many limitations for non-technical risk identification and mitigation efforts.

Managing risks at an enterprise level also requires alignment across the enterprise, or all portions of an organization, with regard to how risks are defined, assigned, managed, tracked and mitigated. If there are multiple definitions of what constitutes a risk across different parts of the organization, then risks will not be defined in like terms or evaluated with equivalent criticality. The PEO C4I Enterprise Technical Risk Board (ETRB) does an effective job of having technical staff from all aspects of the organization nominate and review risks; however, the ability to identify or manage risks beyond the technical domain is severely limited by the lack of non-engineering staff involved in the ETRB. Also, there is not a clear set of standard operating procedures or common risk definitions that could be used to normalize risks originating from different parts of the PEO. This leads to risks being assessed as more or less critical than they really are as the criticality assessment is made by whoever initially nominates the risk.

Utilizing evaluation criteria from authoritative research in both organizational alignment and enterprise risk management best practices, the study of PEO C4I's ETRB results in several recommendations. In terms of organizational alignment, it is recommended that every employee or functional area within the PEO should be directly assigned risk management responsibilities. This increases the likelihood of risks being discovered and nominated to the ETRB. It also expands the membership of the ETRB beyond the current engineering staff. It is recommended that there be regular guidance from PEO leadership on their core areas of focus and potential risks at a strategic level to ensure the ETRB is focusing risk management efforts in areas viewed as strategically critical to the PEO. Finally, it would be beneficial for the ETRB to have a documented regular and recurring path to notify PEO leadership of enterprise level risks that are in need of leadership engagement to help mitigate. This ensures risks shared by multiple portions of the PEO can be better mitigated across program lines.

There are also several recommendations to improve the PEO's implementation of enterprise risk management best practices. The first is defining an enterprise risk template to ensure all risks nominated for enterprise management are defined in common terms and with consistent criticality metrics. This avoids unintentional bias of under or over assessing criticality, or describing the risk in insufficient detail for an effective mitigation strategy to be developed. Also, to aid in commonly defining enterprise risks, it is necessary for there to be an over-arching enterprise architecture for the entire system-of-systems within the control of the PEO. A common enterprise architecture will aid in defining enterprise risks as all ETRB participants would then have a shared understanding of the end state technical, and associated programmatic, goals of the various programs within PEO C4I. Having this common understanding gives a consistent reference point for risk definition, whether a function that is missing from the enterprise architecture, a poorly-defined interface, or some other gap or inconsistency requiring action.

Implementing these recommendations will provide an improved foundation both in regards to organizational alignment and adherence to enterprise risk management best practices. The result is a PEO organization more adept at identifying and managing risks beyond the scope of any single portfolio or functional area. The key evaluation criteria identified in this review also provide a framework that could be re-used to identify organizational and enterprise risk management strengths and weaknesses in any organization, whether within DOD or otherwise. Future expansion of the criteria as more research is done and more case studies executed would be an excellent topic for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

My sincere thanks to my advisors, Professor Mark Rhoades and Dr. Deborah Gibbons. Their advice and edits made a huge difference in the quality of this thesis, and their continuous willingness to review draft after draft made all the difference in me completing this effort. I will also always appreciate their schedule flexibility as I endeavored to get this done months in advance of the standard thesis schedule.

I am also thankful to Professor Barbara Berlitz for her patience with my grammar and citation questions, which I often thought were obscure but which she always answered promptly and clearly. My thanks to Professor Wally Owen, whose advice as I was putting together the proposal for this thesis got me on the right track from the start.

I could not have completed this thesis on my desired schedule without the endless support of Heather Hahn. She laid out the routing process for each step of this effort clearly, and multiple times thanks to my need for constant reminders.

Thanks to my colleagues at SPAWAR, specifically Nic Bergeron, Jim Ciocco and Alyssa Mroczek. Nic for letting me take a critical eye at our internal risk management processes, and Jim and Alyssa for teaching me more about the history of the PEO C4I ETRB than I thought was possible.

Finally, my thanks to my family. First to my yet-to-be-born son, William, for timing his arrival into the world for after I completed this thesis. Also, and most especially, to my wife, Becky. Her endless support and understanding through this whole program, but especially during my writing of this thesis, is something I am not sure I could ever adequately thank her for.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. IMPORTANCE OF ENTERPRISE RISK MANAGEMENT—PROBLEM STATEMENT

Risk management is one of the central tenets of program management, both in industry and in the Department of Defense (DOD). Risk management receives such emphasis that there is an entire DOD publication dedicated to defining how acquisition programs should handle risk, the *Risk Management Guide for DoD Acquisition*, most recently released in 2015. This guide describes the steps of risk management: Risk Identification, Risk Analysis, Risk Mitigation Planning, and Risk Tracking. It also addresses risk management roles at different levels of the organization. What it does not do, however, is discuss how to handle risks beyond the boundaries of a single program. It does not address enterprise risk management.

Enterprise risk management is not a new concept, originating in the mid-1990s in private industry (Dickinson 2001). The principles of risk management do not necessarily change when implemented at the enterprise level, but the involved participants and scope of risks being considered both broaden, potentially quite substantially. This indicates that to implement fully the principles of enterprise risk management, an organization must have both an implementable risk management strategy, as well as orient their organization and key participants' duties to focus on risk management as a priority across all areas. Therefore, risk management best practices and key concepts of organizational alignment are proposed to be equally critical to successful enterprise risk management.

The concept of enterprise risk management is taking on such emphasis that there are even graduate programs offering master's degrees in enterprise risk management showing up at American universities such as St. John's University and Columbia University in New York and Johns Hopkins University in Maryland.

While each of these programs is part of its respective university's business school, the concept of managing risk at an enterprise, or system-of-systems level is also taking hold in the DOD. To this end, the Space and Naval Warfare Systems Command

(SPAWAR) Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I) has established at the PEO front office level, an Enterprise Technical Risk Board (ETRB) run by the PEO's engineering functional area lead.

The ETRB Charter states that the scope of the board is to assess and manage, "Any risk that affects system dependencies which requires coordination/cooperation and technical performance between two or more programs or projects from different [offices] or other external systems" (PEO C4I 2015, 3). Given this goal, this thesis reviewed both the implementation of risk management best practices employed by the ETRB as well as the alignment of PEO C4I's organization to enable risk management, while addressing the question as to whether that organizational alignment could be improved to better provide for enterprise risk management. Later in this chapter is a description of an analysis method that could be applied to any organization to evaluate alignment to organizational optimization and employment of risk management principles for effective enterprise risk management. Later in this thesis, that evaluation method is applied to assess the PEO C4I ETRB in particular.

B. ALIGNING ORGANIZATIONAL STRUCTURES IN DOD

Chapter II will briefly discuss general principles of common organizational structures, but the emphasis is in relation to those structures commonly employed by the Department of Defense and the goals of each organization with regard to risk management. It should be noted that the top-level organizational chart of the DOD, shown in Figure 1, includes allusions to both functionally aligned and project-aligned organizations.

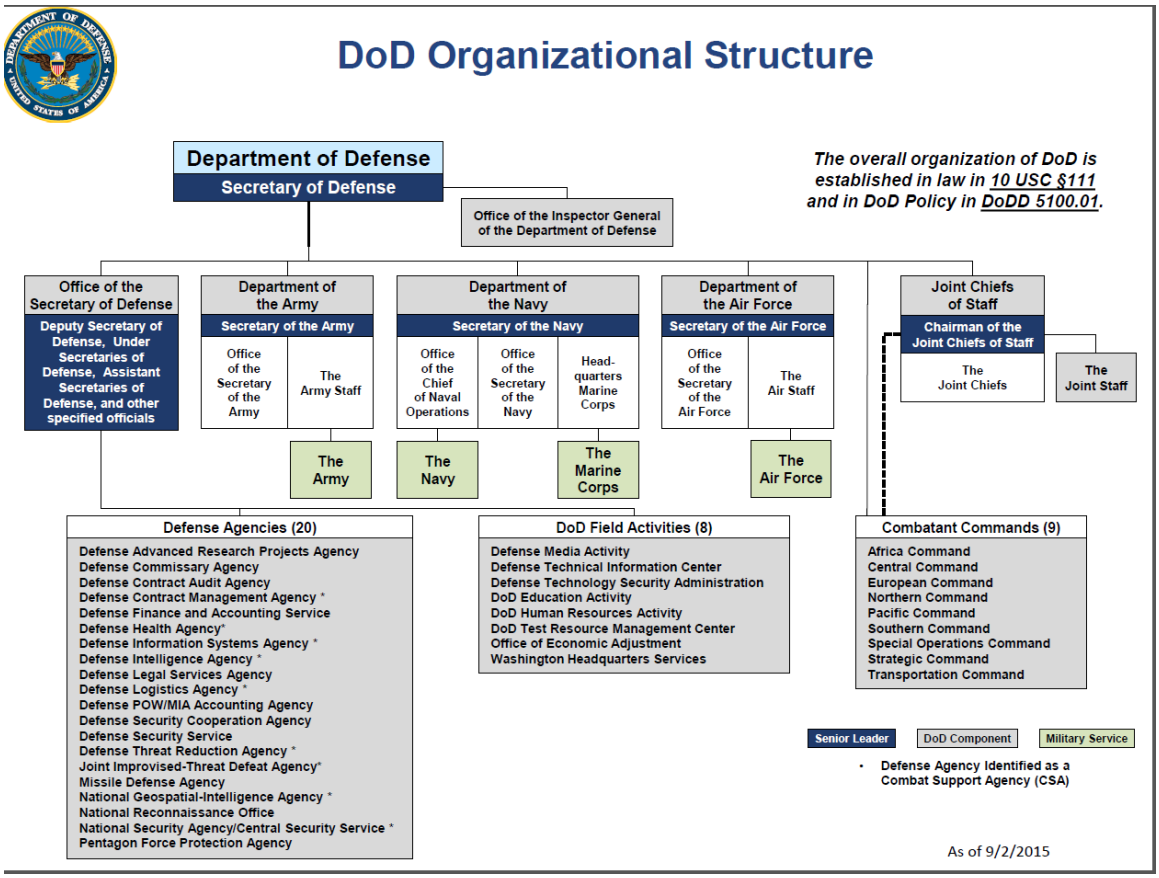

Figure 1. DOD Organizational Structure. Source: DCMO (2015).

As can be seen in Figure 1, the acquisition organizations under the individual military services are essentially project-aligned organizations. They have specific mission sets they are assigned to carry out and have functional experts in various fields aligned to support them. On the same organizational chart, however, the 20 Defense Agencies in the lower left are more functionally organized. They have specific and well-defined areas of expertise, and while there may be some personnel with other functional expertise in their organizations, they are nonetheless focused on one specific function, whether that be in the area of intelligence, security, or information systems, among others.

This review is focused on the management of enterprise risks at the level of a program executive office, which is specifically charged with the development, integration, fielding, sustainment, and overall acquisition of Navy systems in the domain of command, control, communications, computers and intelligence. A specific, but still

very far-reaching set of capabilities. This context of a collection of product-aligned organizations will serve as the framework for defining the boundaries of the "enterprise" for the PEO C4I ETRB, but will also provide a basis for comparing how enterprise risk management would operate in other variations of DOD organizational structures.

It should also be noted that DOD organizations are continuously evolving; in fact, a Defense Acquisition University (DAU) study in 2007 of overall defense acquisition structures found that change was one of the few constants in regards to DOD organizational structures. Despite the finding of continuous changes within DOD organizational structures, that same study surprisingly concluded that many of the organizational adjustments within acquisition organizations were not to help maximize their acquisition efforts. In fact, the study concluded that these reorganizations were often intended to improve office productivity, but were also "based on overly optimistic budget, schedule and technology readiness forecasts" (DAU 2007, viii), perhaps an indictment of their use, or lack of use, of enterprise risk management principles in framing the respective reorganizations. This underscores a key tenet of this thesis' research effort: ensuring that organizational alignment is being maximized for the purposes of enterprise risk management, specifically with regards to the PEO C4I ETRB.

C. OVERVIEW OF PEO C4I ETRB

Each of the subsequent chapters in this thesis will examine the degree to which the PEO C4I ETRB aligns with core principles of organizational alignment and risk management for the purposes of enterprise risk management. To provide context to that analysis, this section will provide a brief overview of PEO C4I and its Enterprise Technical Risk Board.

Figure 2 provides a high-level view of the PEO C4I organizational structure. Note that the PEO contains both product and functionally aligned organizations. The product-aligned organizations are the program offices, or Program Manager Warfare offices (PMWs) in PEO C4I terms. Each program office is run by a program manager and is charged with a specific grouping of products, such as Command and Control. The functionally aligned organizations are run by the individuals noted in the box to the left

of the PEO in Figure 2. These include functional organizations for installations, logistics, engineering, and science and technology. It is the PEO functional lead for engineering, the Assistant Program Executive Officer for Engineering (APEO-E) who chairs the PEO C4I ETRB. The benefits and drawbacks of having the functionally aligned engineering organization manage enterprise risks on behalf of both the functional and product-centered portions of the PEO are examined in Chapter II.

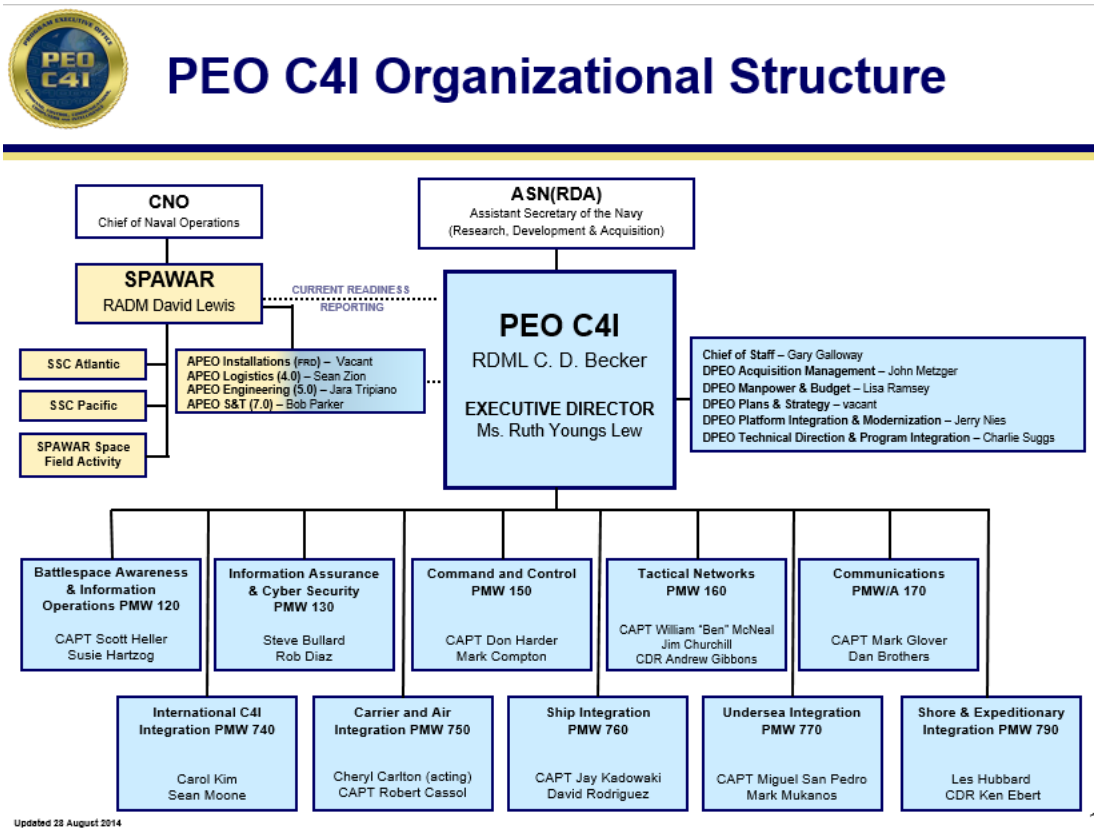

Figure 2. PEO C4I Organizational Structure. Source: PEO C4I (2014).

The ETRB was charted in March 2015 and was tasked with the following objectives:

- Determine whether a submitted risk/issue should be designated as an Enterprise Technical Risk (ETR).
- Identify a lead (ETR owner) responsible for ensuring that the ETR is kept up to date, with mature language describing the ETR and associated mitigation plans.
- Evaluate the adequacy of mitigation plans developed for ETRs.
- Provide a disposition on whether an ETR has been successfully mitigated (PEO C4I 2015, 3).

As with many other organizational risk management plans, the charter also stipulates that risks can be raised by any member or from other parallel organizational boards. The charter also lists the required membership which consists of the chair and required membership. The Assistant Program Executive Officer for Engineering, the engineering functional lead for the PEO as shown in Figure 2, is established as the chair of the board. The other required members are the engineering supervisors and engineering staff embedded in each program office. All other members are listed purely in an advisory capacity and attend only as necessary or desired on their part.

The core responsibility for the chair and required members is to "Provide *technical feedback*, analysis and recommendations on submitted ETRs" (PEO C4I 2015, 5; emphasis added). The board is scheduled to meet at least monthly, with sessions more frequently if events dictate. The key facets of this board are further discussed in Chapters II, III and IV, but this section shall be referenced throughout that analysis.

D. ANALYSIS STRATEGY

With the assertion that successful enterprise risk management is dependent on both an organization's ability to adopt and follow risk management best practices as well as align the organizational roles to achieve a holistic focus on risk in each position, the analysis of the PEO C4I ETRB will need to be evaluated in both contexts. This will involve identifying enterprise risk management best practices and organizational alignment key tenets as evaluation criteria to be utilized in the analysis.

Chapter II will review organizational constructs and strategies to ensure organizational focus on risk management. Chapter III will discuss enterprise risk management best practices. Within each of those chapters, evaluation criteria are discussed and used to determine to what extent the PEO C4I ETRB adopts those tenets. These criteria were gathered from authoritative, published research in both the organizational alignment and enterprise risk management fields.

To perform the analysis, each evaluation criterion will have an ideal case as derived from the source research. It is not expected that any enterprise risk management strategy would meet the ideal case in each organizational alignment or risk best practices area, but rather the criteria are established to provide context to evaluate the enterprise risk management strategy in both domains. If an enterprise risk management strategy is designed to focus only on risks in a certain functional area, or only in a certain part of the product life-cycle, then some aspects of the organizational alignment may be intentionally ignored and some features of enterprise risk management given minimal attention so as to make best use of resources and energy on the organizational priorities.

Since the goal is to provide a framework for an objective analysis in both the organizational alignment and risk management best practices domains, a repeatable analysis framework should be established. As mentioned previously, a conclusion that an enterprise risk management effort is weak in a certain area does not mean that the strategy is ill-formed if the lack of focus in that area is intentional. The results would provide feedback on strengths and weaknesses of a risk management approach with regard to organizational and risk management best practices. Any conclusions or changes driven by the evaluation would be at the discretion of the organization. To capture the summary of each evaluation, a comparison matrix is utilized; a blank version of this matrix for use in the analysis of the any organization is included in the Appendix. The analysis includes a description of core principles, both in regards to organizational alignment and risk management. This set of core principles is paired with a definition of what an ideal implementation entails, and then a description of how the PEO C4I ETRB aligns to that ideal case. The final column of the matrix is a top-level analysis of the

quality of alignment between the PEO C4I ETRB and the core principle in question. The core principles to be used as evaluation criteria are:

Organizational Alignment

- Employee's Responsibility / Accountability for Managing Risk (Liu 2011)
- Cross-Team Coordination for Purpose of Managing Risk (Hardy 2015)
- Allowance for Multiple Teams to Co-Own Risk Mitigation (Liu 2011)
- Enterprise-Level Definition of Risk Management Practices (Galliano 2011) and Risk Areas for Each Organizational Component (Roberts 1991)
- Evaluating Risk in Terms of Impact to Efforts Other Than Your Own (Tonello 2007)

Risk Management Best Practices

- Ability to Consider Short-Term and Long-Term Impacts to Risk (Tonello 2007)
- Evaluating a New Risk with Regard to its Impact on Existing Risks (Liu 2011)
- Risks Managed at the Most Detailed Level Possible (Liu 2011)
- Presence of Enterprise Engineering Models or Architectures to Provide Objective Context for Technical Risks (Brunson et al. 2009)
- Risks Evaluated with Context of System Position in Acquisition Life-Cycle (Stevens et al. 2009)
- Assessment of Ability to Mitigate Risk in Current Enterprise Architecture (Langford et al. 2008)

E. LITERATURE REVIEW

Authoritative research was utilized to determine which evaluation criteria were most relevant in assessing organizational efforts to enable enterprise risk management. These criteria fell into the broad categories of organizational alignment and risk management best principles, and the research approach included review of publications emphasizing those areas in general but also within the context of DOD in particular.

1. Organizational Alignment

Organizational focus on enterprise risk management in particular has significantly increased in recent years. The concept that risk is not something to be managed only at the level of individual business units or functional areas is discussed in depth by Matteo Tonello (2007) in *Emerging Governance Practices in Enterprise Risk Management*. This includes a discussion of the benefits, as well as drawbacks of elevating risk management to an executive board level. This is so risks can be managed by senior executives with a vision that includes not just resolving risks impacting a particular unit in their organization, but also take into account the potential strategic impacts of various approaches to mitigating those risks. Also among the benefits is the ability of senior leaders to take something seen as a risk through the eyes of a functional manager and potentially to turn it into a future opportunity when viewed at a strategic level.

A view of enterprise risk management as it is being organizationally adopted in the federal government is presented by Karen Hardy in *Enterprise Risk Management: A Guide for Government Professionals*, published in 2015. This examines not only the risk management techniques that are key to enterprise risk management, but it examines the concept of enterprise risk management in a federal government as potentially being nearly on a world-altering scale. Methods for coordinating across federal agencies to try to mitigate the risks that result from the occurrence of a natural disaster is one such example. Similar to Tonello's (2007) assertions, Hardy (2015) emphasizes the need for agency executive-level involvement. This higher-level engagement helps ensure that organizational perspectives beyond the individual department, or even individual agency, are considered when it comes to risk management. Having services unavailable in one

agency, while not only a risk to it, could also become a much broader risk in the event of a natural emergency when other agencies are counting on that same service.

A common definition of where the organization considers its risks to be, and what it defines as the minimum threshold for a potential problem to be considered a risk are reviewed at a high-level by Carlos Galliano (2011) in his presentation entitled *Implementation of an Enterprise Level Risk Management Process at the Naval Undersea Warfare Center*. This is also addressed in other sources to a similar point, indicating that no level of organizational dedication to managing risk as an enterprise can be effective without a commonly expressed vision of an organization's key risk areas and threshold definitions of risk.

A much more organizational-centric focus is presented by Xin Liu in *A Holistic Perspective of Enterprise Risk Management* (2011), where he posits that enterprise risk management techniques could be made more effective if the organization focuses less on the identification and resolution of risk, but instead emphasizes that each member of the organization "owns" a portion of any risk. This gives each employee an added investment in managing risk and sense of responsibility always to be aware of potential risks and working to resolve them. This includes working to resolve risks through working across departmental boundaries.

While not always overtly stated, the key principle of enterprise risk management that calls for the inclusion of executive level personnel in the risk management process is discussed in most literature researched for this thesis. The inclusion of executives as stakeholders in risk management automatically adds a more overall enterprise viewpoint to the risk management approach, by adding their strategic outlook to the risk discussion. Also included and seemingly as critical, however, is the emphasis that all risks must have ownership by all portions of an organization to enable the most effective and efficient methods of enterprise risk management. Without that holistic ownership of risk, and each employee having a sense of responsibility to identify and resolve risks regardless of their origin or impact, any enterprise risk management strategy will be ineffective. Here the term enterprise is not just a descriptor of the scope of the risk, but also represents that the enterprise is responsible for dealing with that risk.

2. Risk Management

There is much research available in the area of risk management, addressing all aspects of the practice. In fact, DOD publishes its own guide to risk management, with the latest iteration released in 2015. This guide has the greatest focus on risks within the context of a single program, with no mention of enterprise risk management appearing in the document. Hardy (2015) has an extensive discussion on viewing risks in relation to organizational strategic goals, rather than just a single project's execution. This is a concept that appears to still just be starting to take hold in DOD, despite having been a topic discussed in the commercial business world for many years.

Viewing or considering risks from an enterprise level is not equivalent to managing those risks at an enterprise level. To manage risks at an enterprise level, the context of those risks must also be considered. There are several sources that address this in a more abstract way, such as a few papers presented as part of Naval Postgraduate School Annual Research Symposia. One was Renee Stevens et al.'s (2009) presentation which included a discussion regarding risk evaluation that emphasized viewing potential risks in the context of the system's position in the acquisition life-cycle. Another was from the 2008 symposium where Gary Langford et al. described that some risks for a given system are best resolved not by modifying that system, but instead through identifying the risk as a gap in the overall set of service capabilities, thus being better resolved as a capability gap to be considered in the acquisition process. Given the DOD requirements definition process, this latter concept would inherently force the involvement of senior DOD leadership to turn the risk-driven-gap into a new capability requirement.

Xin Liu (2011) has an interesting discussion about risk management that expands on his review of organizational alignment strategies to maximize risk management. This includes the assertion that through organizational alignment, ensuring that all members of the team feel that they own a portion of the risk management effort, improves a group's ability to manage risks at a more detailed level. This concept is founded on the idea that if all internalize that they own a part of risk management, then they will strive to have a more detailed understanding of the risks facing the organization. Through this increased

"ownership" a more in-depth understanding of risks, their root causes, and their potential mitigations will result. Essentially, extending ownership of enterprise risks to all members of an organization drives a desire for more detailed descriptions and analyses of enterprise risks.

Extending that organizational investment concept, Liu (2011) also posits that a by-product of the more engaged risk management efforts of the whole team will allow for a greater understanding of the impacts of one risk on other risks already being tracked. For example, a product running into development delays having an impact on the schedule for rolling out a new marketing strategy. Without a whole-team engagement on risk management, these risks would be managed separately and with potentially orthogonal mitigation approaches. Such as the development risk being managed by the engineering team while the marketing schedule risk was being managed independently by the marketing team. Instead, a combined risk management effort allows the mitigation of the first risk to inform the mitigation strategy on the second risk. This whole concept represents an example of the end-game desired when an organization increases focus on moving from standard product or project-centered risk management to enterprise risk management.

Enterprise risk management is also most effective when the overall technical effort on a project is performed from an enterprise perspective. This means overarching enterprise, or system-of-systems engineering artifacts used both to start the project development and design efforts, as well as used as references to validate lower-level component design efforts. Karl Brunson et al., in their 2009 *A Framework for Systems Engineering Development of Complex Systems*, state that without those enterprise engineering artifacts, it is not possible to have enterprise risk management. The assertion is that without an enterprise context for the system, there is no authoritative way to measure enterprise risk, or at least enterprise technical risk. Otherwise, some degree of measuring the risk at the enterprise level is based on conjecture, since the system is being managed at a lower level and that lower level is the only place where there is technical certainty in system architecture and design. This idea is critical for enterprise risk

management efficacy. It implies the whole system must be managed at the enterprise level as a precursor for enterprise risk management.

While not frequently acknowledged directly, co-dependence is demonstrated between enterprise risk management and organizational alignment in the literature on both topics. In the majority of the enterprise risk management principles it is implicit that there is organizational buy-in for an enterprise approach not solely to risk management but also to system development writ large. This alignment in concepts is a core driver of the analysis of the PEO C4I ETRB in the subsequent chapters.

F. OVERVIEW OF CHAPTERS

The introductory chapter, Chapter I, provided background on the evolution of risk management from an individual project level, to an enterprise level. It also discussed variations in how organizations in DOD align in product- or function-oriented ways. A description of the PEO C4I ETRB is provided, as well as the central research question as to whether improvements could be made to the structure and conduct of the ETRB to better align it to key organizational alignment and risk management best practices. Chapter I also includes a discussion of the analysis methodology that is used to answer that research question.

An overview of high-level organizational structures is covered at the beginning of Chapter II. The chapter discusses key principles in aligning organizations for specific focus areas, such as risk management. The discussion of these key principles also includes a review of how those principles form the criteria that are used to assess the ETRB for an effective organizational alignment to enable enterprise risk management. Those criteria are then each applied to the ETRB model, and an assessment of the ETRB's compliance is discussed.

Chapter III performs a similar study as Chapter II, but is on the best practices of risk management, with an emphasis specifically on enterprise risk management. The chapter includes a discussion on the relatively recent evolution to focus on managing risk at the enterprise level, and the benefits that provides to an organization. This involves a discussion of those core enterprise risk management tenets, and a review of which of

those tenets are chosen as criteria against which the ETRB is evaluated. As in Chapter II, Chapter III ends with a review of the ETRB's adherence to the best practices, and the potential impacts to the ETRB's efficacy that the associated levels of compliance indicate.

From these analyses of individual organizational alignment and risk management best practices, an overall review of the ETRB utilization of those best practices is the focus of Chapter IV. This review includes a discussion on the impacts of areas of alignment or misalignment as well as a discussion on how organizational goals and priorities could be driving some of those misalignments. The discussion of organizational misalignments is addressed from a holistic level as some potential misalignments may have been undertaken with specific intent by the founders of the PEO C4I ETRB. This chapter also includes recommendations on steps the ETRB could undertake to move into better alignment with both the organizational alignment and enterprise risk management best practices. Finally, there is a discussion on the limitations of the analysis and recommendations with regard to the ETRB.

Chapter V provides a summary of the analysis, and describe the conclusions that were drawn with regard to the structure and focus of the PEO C4I ETRB. This chapter also discusses areas not addressed in this thesis that could serve as potential areas for future research.

II. ORGANIZATIONAL STRUCTURES

The focus of any organizational structure is to maximize the ability of that organization to complete its mission, whether that mission is product development, consulting, or the national defense. At a high level, there are two standard structures that organizations can adopt: a functional structure or a product-centered structure. Within each structure there are different allocations of the three key aspects of each organizational position: authority, responsibility, and accountability (Kerzner 2013).

Briefly, each of these aspects is defined in Table 1, as quoted from Kerzner (2013).

Table 1. Key Attributes of Organizational Positions. Adapted from Kerzner (2013).

Position Attribute	Description
Authority	The power granted to individuals so that they can make final decisions
Responsibility	The obligation incurred by individuals in their roles in the formal organization to effectively perform assignments
Accountability	Being answerable for the satisfactory completion of a specific assignment

It should also be known that in the descriptions, accountability is equated to being the combination of authority and responsibility (Kerzner 2013). These attributes are important in comparing common organizational structures and how authority, responsibility, and accountability are allocated in the various structures.

A. COMMON STRUCTURES

This section examines two standard organizational structures, a functionally centered structure and a product-centered structure. It should be emphasized that many organizations employ some manner of a hybrid between these two organizational types. Referring back to Figure 2, the PEO C4I overall structure is certainly a hybrid, with individual program offices that are product-centered but also PEO-level staff that are functionally aligned in areas such as engineering, logistics and contracts. The attributes of a hybrid organizational structure are a consideration when evaluating the organizational structure of the PEO as it relates to the ETRB. The context of the strictly aligned organizations discussed in the next section is also important with regard to interpreting the potential benefits and drawbacks of the hybrid alignment implemented within the PEO as it impacts the scope and set of viewpoints available within the ETRB.

1. Functional Organizations

When describing a functional organization the key characteristic is that, "The organizational links are primarily among those who perform similar functions" (Ulrich and Eppinger 2012). In DOD this is often thought of in very general terms, such as technical versus programmatic functions, it can actually be broken down even further. Consider a private industry organization and the departments it might have, such as finance, marketing, human resources, engineering, test, production and the like. Each of these would be considered a separate functional area and in a functional organization would be managed by a leadership team within that same functional area. The personnel may be assigned to work on individual projects, but their alignment is to their functional leadership, not to any project they are working on. They would be loosely coupled, if at all, to any project lead (Ulrich and Eppinger 2012).

a. Strengths

There are several fundamental strengths associated with functional organizational structures. These include:

- They develop deep specialization and expertise (Ulrich and Eppinger 2012).
- They provide better flexibility in utilization of staff (Kerzner 2013).
- They provide continuity in departmental policies, procedures and reporting chains (Kerzner 2013).
- The have well established and vertical communication channels (Kerzner 2013).
- They allow easier budgeting and cost control are possible (Kerzner 2013).

The common thread in each of these strengths ties back to consistency. By employing a functionally aligned organizational structure, leadership is also defining an organization that looks the same regardless of the projects being undertaken. Personnel are aligned by their expertise, not any specific project utilizing that expertise. Due to the organizational alignment being more consistent, it is much easier to budget as the organizational costs do not fluctuate drastically with changing projects, but rather the same personnel are just assigned different project priorities as the project life-cycles carry out. With this strong functional alignment, employees report to their single functional organization management regardless of how many projects they are assisting with. This makes for a much clearer chain of command then if those employees reported to all of their disparate project managers.

Finally, through the strong functional alignment, consistent reporting, and record keeping, department policies can be established and utilized by employees for all efforts. This is far easier to manage at the individual employee level than if they have different policies for each of several projects to which they are contributing, which would result in more overhead by doing the same work in a different manner depending on the project.

b. Weaknesses

There are also drawbacks to a functional organization alignment, which include:

- coordination across functional groups can be difficult and/or slow (Ulrich and Eppinger 2012)
- slower response to changing customer needs (Kerzner 2013)
- weakly-defined responsibility for overall project execution (Kerzner 2013)
- ideas for improvement are functionally focused and more difficult to apply to individual projects (Kerzner 2013)

Since personnel alignment and thus presumably internal priorities are aligned to a functional area and not to any specific project, efforts to coordinate across departments within the context of a project are hindered. The idea of project execution is in many ways secondary to functional area priorities, resulting in far less emphasis on cross-functional communication on any single project effort. As a by-product of this, any new or changing needs from the customer are addressed more slowly because the changes would frequently need the contributions of multiple organizational functions to be implemented.

Also, benefits that result from process improvement efforts would have a slower impact on individual projects, as the improvements would be focused on benefitting a functional organization as a whole, with benefit to the project as a secondary focus at best. This also means that improvement efforts in any one functional area may not match with current execution processes in another functional area, resulting in lessened if any benefits at the project level.

Finally, since any project ownership responsibility would be shared across multiple functional areas in this organizational alignment, there would be a very weak project leadership organization, if any formal project ownership was defined. This may not be a major issue for organizations whose products are stable, but for any organization looking to evolve existing products, or develop entirely new ones, this weak project ownership factor may prove critical.

2. Product Organizations

As the title indicates, product or project organizations are focused on executing the full life-cycle of a project to produce a particular product or system. As a result, personnel from each necessary functional area are assigned to a product and report directly to a product manager. This product manager has full control of all aspects of product execution and also full authority to direct all personnel assigned to the product (Ulrich and Eppinger 2012). "The major advantage…is that one individual, the program manager, maintains complete line authority over the entire project" (Kerzner 2013). In many ways this is the converse structure to a functionally aligned organization.

a. Strengths

Product centered organizational structures have several advantages, including:

- It provides for complete control and authority over all aspects of the project (Kerzner 2013).
- Staff maintains expertise on a single project rather than dispersed knowledge over several efforts (Kerzner 2013).
- Cross-functional trade-off analyses can be done more rapidly (Ulrich and Eppinger 2012).
- There is a single focal point for external and customer relations (Kerzner 2013).

Having a single point of responsibility, and equally designated authority, to execute a product is the key tenet of a project-aligned organization. As discussed earlier in this chapter, this results in accountability of product leadership for executing all aspects of the product development and delivering the needed product at the conclusion of the effort.

The centralization of accountability at the management level is the first step, but to provide the necessary alignment to then execute the product development, a centrally-aligned staff is necessary. This second aspect of the product manager's authority is to be the direct manager of functional experts assigned to this specific product. This results not only in centralized accountability but centralized responsibility for every employee in the product organization.

Finally, as this product is every team members' complete focal point, a natural relationship between the product organization and external entities is created. This is especially crucial in establishing a small set of entry points for the customer base to interact with the project organization, resulting in a product that more closely aligns with the customer's needs and vision.

b. Weaknesses

There are of course also weaknesses to a product-aligned organization. These are:

- the ability to keep up with evolution of technology is hindered as technical personnel are focused on executing an existing system design (Ulrich and Eppinger 2012)
- the potential limiting factor on long-term career opportunities (Kerzner 2013)
- the tendency to be slow to change personnel as the project moves through the life-cycle (Kerzner 2013)

The tight association with personnel to a specific product is a definite strength when their function is providing key input and expertise to a product. As products evolve, however, it can be hard to change personnel due to the tight team identity that has already been established. This, for example, could result in design engineers being kept on a product even once it is in full production and different engineering skillsets could be more valuable.

Relatedly, since personnel become synonymous with the product on which they are working, it can be difficult for product staff to take advantage of advancement opportunities. They become identified only in terms of their product affiliation, not for their functional skillsets, and so hiring managers may have difficulty imagining them contributing functional knowledge to a product with a different end goal.

Finally, as staff focus on a specific product, and on executing a vision defined early in the life-cycle, it can be difficult for them to incorporate technical advances or other industry changes. The product team has a vision that was created largely from their inputs, and it can become an issue of personal pride if significant changes are proposed due to industry evolution.

3. Considerations for the PEO C4I ETRB

As discussed in the overview of the PEO C4I organization in Chapter I, the ETRB is chaired by the APEO-Engineering, who leads the PEO C4I functionally aligned engineering organization. Included in this organization are Assistant Program Managers-Engineering (APM-E) that are engineering core staff but are embedded in the PEO C4I program management organizations. A similar construct is followed for the PEO logistics staff.

The result of this is a functionally aligned organization running the ETRB, but utilizing personnel that are embedded in the program management product-aligned organizations is an interesting hybrid organizational structure that influences the ETRB. The APEO-E provides engineering oversight for all PEO C4I activities. This authority is also delegated to the APM-E staff, but that group spends their day-to-day efforts embedded in the product-aligned program offices, giving them a very different view on technical risks in particular than may be available at the PEO level. A depiction of the key functional and product-aligned portions of the PEO C4I organization are displayed in Figure 3.

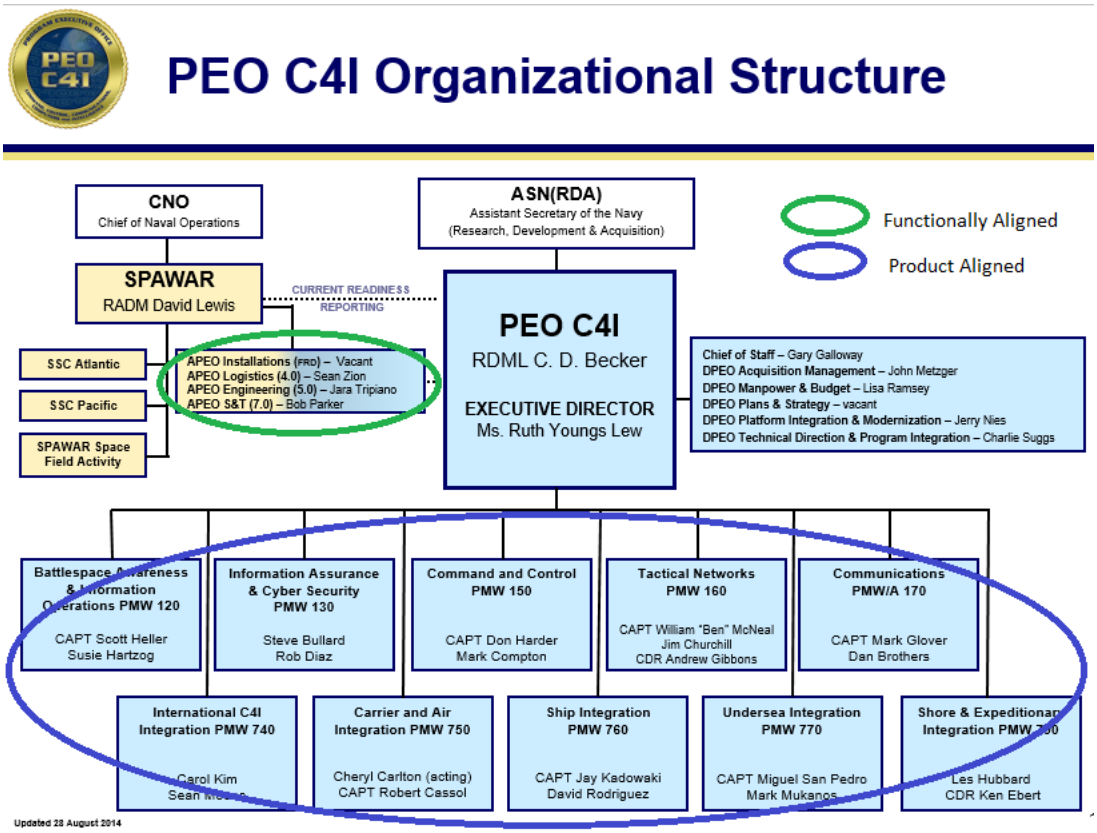

Figure 3. Core Functional and Product-Aligned Portions of PEO C4I Organization. Adapted from PEO C4I (2014).

The impacts of this hybrid organizational alignment also needs to be a consideration as the ETRB is evaluated against the organizational alignment principles that are discussed in the next section. This organizational structure could be placing limitations on the ETRB, or it could be providing needed and desired focus on the engineering aspects of risk management. Limitations of this construct for the ETRB should be considered, but it should also be determined if those limitations were implemented intentionally by leadership.

B. RISK MANAGEMENT EMPHASIS IN ORGANIZATIONAL STRUCTURES

The overarching organizational constructs defined in the previous section and the strengths and weaknesses associated with each, as well as how those organizational constructs relate to the structure of the PEO C4I ETRB were used as context for the evaluation in this thesis. Given those considerations, an examination of key organizational alignment principles related to enterprise risk management was performed. They were compared against the key concepts of authority, responsibility and accountability as described in functional and project centered organizations.

1. Employee Responsibility and Accountability

As defined earlier in this chapter, accountability is composed of authority and responsibility, "Being answerable for the satisfactory completion of a specific assignment" (Kerzner 2013). Based on that definition, accountability is in context of the employee's assignment. If this were an employee in a functionally aligned organization, that function could be a specific engineering, or marketing, or other task that the employee repeated with regularity though potentially on many disparate projects. Were the employee in a product-aligned organization, the assignment could be any number of tasks focused on a particular aspect of a product, or a particular function within the product life-cycle. This may include engineering analysis on any number of tradeoff studies, or marketing for different versions of a product produced by the organization.

Liu (2011) postulated that enterprise risk management would be more effective if an organization imbued each employee with the responsibility to manage risks, and not just risks in their own area but in all areas of a company or product. This responsibility to manage all potential risks, and the authority to help develop mitigations, would make each employee more accountable for risk management as a whole. With that accountability would come an increased dedication to risk management and therefore greater success at managing risk at an enterprise level. In fact, that increased authority may be considered a pre-requisite for implementing enterprise risk management (ERM), "ERM requires risk owners at the operational level to have considerable knowledge,

communication, control, and authority which are reserved for managers in a traditional risk management system" (Liu 2011).

This principle was selected as an evaluation criteria since it was the most fundamental organizational concept to enable enterprise risk management. It would be impossible for an organization to profess an effort to manage risks at an enterprise level yet have only a subset of its employees charged with managing risks as part of their responsibilities. To truly infuse an organization with the goal of managing risks at the enterprise level each employee must inherently understand that such an effort includes every employee at every level. Without that stipulation, any enterprise risk management effort is not encompassing the entire organization.

2. Cross-team Coordination

Providing employees with the responsibility to manage enterprise risks could have other organizational benefits as well. "Coordination and interactions…among risk owners or co-owners are important for a successful ERM program. For example, coordination of risk discussions across the entire entity may reduce risk owners' tendency to refuse to share information and hide its negative impact" (Liu 2011, 14). From earlier in this chapter, the benefit of increased cross-team interactions is also a foundational benefit of operating in a project-aligned organization. It would be an interesting study to research how effective this aspect of enterprise risk management would be in a functionally aligned organization, where cross-team interaction is an assumed weakness.

"ERM challenges the status quo and requires managers and leaders to step out of their organizational comfort zones and into a collaborative environment to not only discuss common risks but uncover latent risks as well" (Hardy 2015, 29). This principle of enterprise risk management leverages the concept of imbuing each employee with the responsibility of enterprise risk management. By issuing that priority, employees need to better understand the enterprise within which they are operating, and thus it results in more cross-team communication. That is the first step toward coordination; making that transition into cross-team coordination includes having enterprise level definitions of risk

management methods. The methods and overall enterprise risks are discussed later in this chapter.

Assuming the implementation of the first criteria is complete, the next step in managing risks as an enterprise involves communication among all the entities in an organization that constitute that enterprise. Therefore, assessing an organization's construct and how it enables or even encourages cross-team coordination on not only risk but any other core area of the organization is a crucial indicator as to whether the organizational construct is set up to enable enterprise risk management.

3. Multiple Team Risk Ownership

Continuing the evolution of having employees take responsibility for the enterprise level management of risks to then coordinating across teams to manage risks is the principle that enterprise risks should actually be owned by multiple teams. This evolution is beyond just managing or mitigating a risk as a team, but having employee and managerial ownership for resolving the risk. This is the ultimate in responsibility and accountability, and drives the next level of individual investment in enterprise risk management as it is not just your singular responsibility but that of your whole team and that team's management.

"Strategic risk is not likely to have a single risk owner because it crosses multiple units, including manufacturing, marketing, and finance" (Liu 2011, 22). Risks at an organizationally strategic level are something rarely emphasized in standard project-level risk management, especially as outlined in the DOD Risk Management Guide in 2015. If a risk is at a strategic level, it requires actions from multiple functional areas to fully address, thus requiring that it be owned by multiple teams and given equal priority by each of those teams. To be able to understand what an organization views as strategic risks, managerial definition of areas of strategic importance is necessary.

The progression of organizationally enabling multiple teams to own responsibility for mitigating risks builds upon the previous two organizational alignment principles. This progression is not possible without the foundation of assigning each employee the responsibility of managing enterprise risks, and setting up a communication structure that

enables cross-team coordination on risk activities. The ability to have multiple teams co-manage a risk indicates an optimized organization in regards both to individual risk management responsibilities and to a common methodology for identifying and defining risks in general. These enterprise risk management principles are discussed in the next chapter. Only with complimentary organizational alignment principles and well-defined risk management methods could multiple teams own the same risk without any concern for attempting to mitigate it in significantly different manners.

4. Enterprise Definition of Risk Management Practices and Risk Areas

If multiple parts of an organization are going to own and mitigate enterprise risks collaboratively, it is imperative that the organization have a global set of criteria to evaluate potential risks against. This is often an issue organizations face when trying to implement enterprise risk management. Barriers such as these were discovered when the Naval Undersea Warfare Center at Newport attempted such an effort. “Risk management was found to be inconsistently applied from department to department and from project to project within a department” (Galliano 2011, 6). If risks are managed across departments but each department has a different definition of what qualifies as a risk, or how to prioritize those risks, the ability to manage the diverse set of risks in any consistent manner is significantly hampered.

Relatedly, defining organization-wide areas of potential risk is critical to keeping all entities within the organization focused on the same varieties of risk. “The danger is that lower-level management choices are more of a reflection of their parochial interests than they are a reflection of what is best for the whole” (Roberts 1991, 23). To align organizationally for enterprise risk management, this issue of departmental silos must be addressed at a more fundamental level, such as by ensuring each employee has individual responsibility for managing enterprise risk as described earlier in this chapter. Beyond that allocation of responsibility is a managerial definition of strategic risks of which all departments must be aware. To that end, it also encourages departments to look beyond their own organizational boundaries to examine what risks exist in other areas that may have enterprise impact.

While personal responsibility and team alignment to risk mitigation responsibilities are key enablers to enterprise risk management, a true enterprise approach can only succeed if there are common risk management processes followed by all portions of the organization. This portion of the criterion is an emphasis on risk mitigation strategies, which can include common procedures as well as ancillary functions such as communications plans or a regular schedule of risk review boards.

The second part of the criterion is an emphasis that enterprise risk management can also benefit from organizational leadership identifying key areas of potential risk for all portions of the enterprise to consider as part of their risk mitigation efforts. While this research discusses approaches that mostly focus on bottom-up risk identification and enterprise management, it is just as beneficial for the highest echelons of the organization to identify all-encompassing potential risk areas for which functional and product teams must be aware.

5. Evaluating Risks in Areas Other Than Your Own

Presuming that an overall organizational definition of risk management practices and key sources of risk have been identified, implementing enterprise risk management allows lessons learned from mitigating risks in one functional area or on one project to be utilized in other areas of the organization. “Internal communication is essential to the success of ERM, senior management should pay extra attention to the establishment of reporting lines…so that any information on risk management provided by a business unit leader can be analyzed and compared with what was learned from other divisions” (Tonello 2007, 42).

This ability to capture past, successful risk management strategies from across the organization provides a foundation for allowing certain types of risks to be managed as a committee with various managers bringing their own risk mitigation expertise to bear. This also allows those managers to utilize the strategies that have provided the greatest past impact for risk mitigation from other departments in the organization. Some private companies actually employ an enterprise risk management executive committee, “A specialized executive committee funnels the diverse intellectual contributions of

functional managers to the [Chief Risk Officer]…functional managers work directly with business unit managers; by means of the committee they should be able to voice at the executive level any concerns expressed by lower organizational levels" (Tonello 2007, 39).

This criterion is the culmination of the previous four criteria in many ways. Leveraging individual responsibility to consider risks in the enterprise context, organizing teams to share ownership of risks, and having leadership identify both methods for risk management as well as potential enterprise risks requiring attention build to enable the concept that through this shift in mindset and sudden awareness of other areas of focus, individuals or teams could start to notice risk in areas outside of their organization. This cross-organization ability to recognize and manage risks should be the ultimate goal of any enterprise risk management effort because this is the full integration of all of the prior criteria.

C. ANALYSIS OF POSITIONS ASSOCIATED WITH PEO C4I ETRB

Utilizing the key organizational principles associated with successful enterprise risk management implementation, the alignment of the PEO C4I ETRB was assessed. The degree to which the ETRB implements the core organizational foci to enable enterprise risk management are reviewed in this section.

1. Employee Responsibility and Accountability

The ETRB charter assigns responsibilities to several groups, including the Chair, Members, Advisors, Submitters, Risk Owners, Board Secretariat, and ETRB Working Group (PEO C4I 2015). From that list alone, it is simple to conclude that the responsibility and accountability for risk management is assigned to the Risk Owner. The charter does not specify who can be assigned as a risk owner, so the assumption is it could be anyone in the PEO.

A closer reading of the role descriptions, however, indicates some other participants who have risk mitigation responsibilities. For all the following entries, an ETR is an Enterprise Technical Risk. These functions include:

- ETRB Chair—"Assign an owner for each ETR to manage all details pertaining to that ETR" (PEO C4I 2015, 4).
- ETRB Members—"Provide technical feedback, analysis and recommendations on submitted ETRs" (PEO C4I 2015, 5).
- ETRB Advisors—"Provide technical feedback, analysis, and recommendation on proposed ETRs, disposition, mitigation strategy, and mitigation status" (PEO C4I 2015, 5).
- ETR Owner—"Maintain the description and/or mitigation plan, to ensure accuracy, completeness, and currency, providing updates to ETR records as changes happen" (PEO C4I 2015, 5).
- ETRB Working Group—"The ETRB Working Group convenes weekly or as needed to preview ETR submission and conduct detailed review of open ETRs" (PEO C4I 2015, 5).

Given all those various participants that have a direct or indirect role in risk ownership in the ETRB, the assessment of compliance to organizational principles for enterprise risk management is less straight-forward. Table 2 provides a summary comparison of the PEO C4I ETRB alignment to assigning employees responsibility for enterprise risk management.

Table 2. PEO C4I ETRB Evaluation—Organizational Alignment Criterion #1

Evaluation Criterion	**Ideal Case**	**PEO C4I ETRB Comparison**	**Conclusion**
Employee's Responsibility / Accountability for Managing Risk (Liu 2011)	Employee provided authority and responsibility to manage and mitigate enterprise risks.	Responsibility distributed among several ETRB roles. Includes risk owner, ETRB membership, ETRB Working Group and others. Managerial responsibility clearly designated and mitigation responsibility distributed across whole board.	As description of responsibility is not explicit, potential for multiple groups to presume they have risk ownership, or that groups assume another member has taken mitigation responsibility. Possibly resulting in no one or multiple people assuming managerial or mitigation responsibility.

The ETRB description of roles indicates several groups, all listed earlier in this section, as having some degree of responsibility for risk ownership and risk management. This is a potential area of confusion as there is a possibility of multiple groups within the ETRB assuming ownership of a given ETR. Conversely, there is an equal possibility of multiple groups assuming one of the other constituencies is taking responsibility for a risk which may result in none of the roles taking ownership. This approach does provide benefits in terms of involving multiple roles and multiple areas of expertise in mitigating enterprise risks, but it should be clear how overall risk mitigation is being managed to ensure effective risk mitigation,. How this risk mitigation management is accomplished is discussed later in this section with regard to the Multiple Team Risk Ownership criterion.

2. Cross-team Coordination

Reviewing the PEO C4I ETRB membership list includes mandatory members within the PEO C4I engineering functional organization, including the APEO-E, the two Deputy APEO-Es and the APM-Es that are embedded within each of the product-aligned program offices within the PEO. Beyond the engineering functional area, ETRB advisory members include acquisition staff from the program offices, ship baseline managers from the ship integration staff as well as members of the PEO test, evaluation and certification staff.

While all of these roles are listed as members, they are not necessarily mandated to attend each ETRB, nor is there any description of the process for determining which members are assigned to own and manage risks. Having expertise from multiple areas is desired for enterprise risk management, but a consistent definition of responsibilities is also needed to ensure consistent management of risks. Examining the expertise of the roles associated with the ETRB, an assessment of the board's ability to enable cross-team coordination is possible. Table 3 provides a summary of this assessment.

Table 3. PEO C4I ETRB Evaluation—Organizational Alignment Criterion #2

Evaluation Criterion	**Ideal Case**	**PEO C4I ETRB Comparison**	**Conclusion**
Cross-Team Coordination for Purpose of Managing Risk (Hardy 2015)	Multiple groups with varying functional expertise combine knowledge for the purposes of enterprise risk management.	Multiple groups with varying functional expertise are members of the ETRB. Unclear from charter how the involvement of those groups is managed or what criteria is used to assign cross-functional risk owners.	Wide range of functional members, however to ensure effective cross-team coordination, more clear guidelines on the organizational responsibilities and risk management battle rhythms should be identified.

Similar to the evaluation of the first organizational alignment criterion, the PEO C4I ETRB charter defines the involvement of personnel with engineering, acquisition, installation, and test/certification expertise, so the framework for cross-team management of risks is present. What is less clear is how the assignment of responsibility among individuals and teams is performed to help ensure the clear definition of risk management responsibility and the associated teams involved. A few minor changes, or a new process definition section within the ETRB charter would be a good way to address this question.

3. Multiple Team Risk Ownership

The next step beyond cross-team coordination for the purposes of providing the most comprehensive knowledge base for managing risks is the concept of multiple teams or functional areas actually owning enterprise risks and being fully responsible for their management and mitigation. This is an area where the ETRB charter is largely silent. Defining a risk owner is mentioned as an overall goal of the ETRB, and the ETRB chair has the specific responsibility to assign an ETR owner (PEO C4I 2015). However, a review of the responsibilities of the ETR Owner reveals that they:

- [are] designated by the ETRB Chair
- ensure that ETR is captured in Risk Exchange
- maintain the description and/or mitigation plan, to ensure accuracy, completeness, and currency, providing updates to ETR records as changes happen. (PEO C4I 2015)

These are important responsibilities, but none ensures actual mitigation of the risk or management of it other than ensuring it is being tracked and updates are provided. Table 4 compares this against the organizational alignment principle for multiple-team risk ownership.

Table 4. PEO C4I ETRB Evaluation—Organizational Alignment Criterion #3

Evaluation Criterion	**Ideal Case**	**PEO C4I ETRB Comparison**	**Conclusion**
Allowance for Multiple Teams to Co-own Risk Mitigation (Liu 2011)	Multiple teams, each with a stake in a positive risk mitigation outcome, are assigned responsibility for mitigation of designated enterprise risks.	The assignment of a risk owner through a multi-team board is described, but actual multi-team ownership is only implied, and not a clear principle of the ETRB.	It is unclear if the ETRB construct is organized to allow for multi-team ownership of a given enterprise technical risk. This needs to be clarified.

It may be intentional that the ETRB desires only a single team to have ownership of any given ETR, or it may be assumed that multi-team ownership is implied. To ensure cross-team buy in and support for either ownership structure, it should be made explicit in the ETRB charter so that organizations can be prepared to engage at the proper level.

4. Enterprise Definition of Risk Management Practices and Risk Areas

For cross-team discussion of risks, and multiple team ownership of risks, the organization as a whole must have a common set of risk practices that all teams and functional areas follow. Without this common set of practices, it would be increasingly difficult to manage risks as more parts of the organization become involved. Each part of the organization would have its own ways of defining risks, its own hierarchy of mitigation strategies, and its own definitions of what amounted to mitigation in terms of risks. Additionally, to aid the various parts of an organization in considering risks at an enterprise level, it would be beneficial to have the upper levels of organizational management define areas they are most focused on in terms of tracking risk. This gives each segment of the organization a starting point for considering potential enterprise risk areas.

In the context of the ETRB charter, the only mention of more senior groups in the organization is the ability of the ETRB to elevate risks if needed. The ETRB Chair shall, "Escalate ETRs to the SEB [Systems Engineering Board] and/or PGB [Portfolio Governance Board] when appropriate" (PEO C4I 2015, 4). Within PEO C4I, the SEB is the most senior technical adjudication board, and the PGB the most senior acquisition and programmatic board. The presence of these more senior boards indicates the potential for more senior involvement in ETRs is available, though there is not an expectation it be regularly used. The reverse appears to also be true from the ETRB charter, in that there is no mention of more senior-level guidance of risk areas the ETRB should be particularly focused on, instead leaving it to whatever risks the ETRB members and advisors choose to nominate. Table 5 provides a summary evaluation of the ETRB against this organizational criterion.

Table 5. PEO C4I ETRB Evaluation—Organizational Alignment Criterion #4

Evaluation Criterion	**Ideal Case**	**PEO C4I ETRB Comparison**	**Conclusion**
Enterprise-Level Definition of Risk Management Practices (Galliano 2011) and Risk Areas for Each Organizational Component (Roberts 1991)	Organization level risk management guide is published and kept current. Senior organizational leadership identifies key areas for potential enterprise risk monitoring	Mechanism for elevating risks to senior leadership exists, but no specific guidelines in place for triggering its use. No process described for receiving leadership input on potential enterprise risk areas of emphasis.	The framework exists for risk elevation, but a more formal set of guidelines for risk management and areas of leadership focus for enterprise risks should be established and linked to the ETRB.

This particular evaluation criterion has the most room for interpretation in regards to implementation strategy. The scope of the ETRB has an emphasis on technical risk management at an enterprise level, so the lack of continuing involvement by more senior boards may not actually be an issue, but a result of intentional design.

5. Evaluating Risks in Areas Other Than Your Own

This organizational alignment principle for enterprise risk management is a natural extension of the first principle of having each employee instilled with the responsibility to manage enterprise risks. To manage enterprise risks, the risks must not only be viewed for their impacts beyond a single area, but in a more enterprise context. Beyond this, risks from other areas should also be reviewed both for potential impact to a functional area, and for the betterment of the enterprise writ large.

The meeting business rules of the ETRB indicate that all members have a role in evaluating every risk that comes before the ETRB. “All members are expected to review, assess, and provide comments on ETRs prior to the meeting” (PEO C4I 2015, 6). By definition, this means all ETRB members, the functionally aligned engineering staff, are evaluating all risks that come to the ETRB regardless of their origin. If this is paired with those ETRB members feeling that they have the responsibility to evaluate and manage risks at an enterprise level, as defined in organizational principle #1, then this mechanism for having the engineering staff review every nominated ETR is very effective at implementing principle #5. Table 6 provides a summary of the alignment of the ETRB to this principle.

Table 6. PEO C4I ETRB Evaluation—Organizational Alignment Criterion #5

Evaluation Criterion	**Ideal Case**	**PEO C4I ETRB Comparison**	**Conclusion**
Evaluating Risk in Terms of Impact to Efforts Other Than Your Own (Liu 2011)	Every employee evaluates all candidate risks for enterprise impacts	The meeting business rules of the ETRB dictate that every member review every nominated ETR	This implementation totally aligns with the ideal case, the only question being how regularly the ETRB sees inputs on ETRs from every member of the ETRB

This is the criterion with which the ETRB seems most aligned. The meeting rules indicate every member shall review every ETR and provide input. The main potential issue with this set up within the ETRB is whether every member truly does review every ETR, and what variation in perspectives is available during that review since the only mandated members are from the engineering functional area. The impacts of the potential membership limitation are discussed further in Chapter IV.

D. CHAPTER SUMMARY

This chapter included an overview of the two fundamental styles of organizational alignment, specifically functionally aligned organizations and product-aligned organizations. This also involved a review of benefits and drawbacks to each style of alignment and a discussion on how PEO C4I is a hybrid of both styles. The program offices are product focused, with an emphasis on acquiring or producing specific product lines within the context of a certain set of warfighting tasks, such as Intelligence, Surveillance and Reconnaissance, or Command and Control. To complement these product-aligned program offices, the PEO also includes a set of front office staff who are functionally aligned, each reporting to a functional lead with either a Deputy PEO or Assistant PEO title.

There was also an overview of the PEO C4I ETRB as it related to this hybrid organizational structure within the PEO, to include considerations for alignment of functionally focused engineering staff as the core members of the ETRB, with personnel with other functional expertise utilized either from other PEO staff offices, or the product-centered program offices to support the ETRB as desired. The impacts of this organizational alignment are revisited in the context of the compliance of the ETRB with core organizational alignment principles to enable enterprise risk management in Chapter IV.

The chapter included a review of key organizational alignment principles that would support implementation of enterprise risk management, first introduced in Chapter 1 and expanded upon in this chapter. A further discussion of the origin of the principles was provided, including the research that surrounded their selection as evaluation criteria in this thesis.

These criteria were there applied to the PEO C4I ETRB. The key point for evaluation was a comparison of the main tenet of the organizational alignment principle with the content of the ETRB charter. Some effort was made to understand items not explicitly in the charter, but implied, as well as to account for activities that were spelled out as possible actions in the charter but without specified standard operating procedures. Each of the five criteria was repeated, with an ideal case for implementation, then a description of how the ETRB did or did not implement that principle, and a conclusion on level of implementation by the ETRB.

A degree of evaluation was performed in terms of considerations for how the ETRB might more fully implement a given organizational alignment principle, as well as some discussion on the potential limitations placed on the ETRB based on its chosen implementation strategy. Several of the criteria directly related to the ETRB receiving more senior level guidance on organizational priorities for enterprise risk management.

Further evaluation on the impacts of the ETRB's level of implementation of the key principles is covered in Chapter IV. This includes not only potential consequences with regards to the ETRB's effectiveness, but also discussions on how to adjust the

ETRB to be more complaint with the organizational alignment principles. Chapter IV also takes some of the conclusions drawn here in this chapter and discusses why those limitations may have been implemented with intent, to specifically limit the potential scope of the ETRB.

III. ENTERPRISE RISK MANAGEMENT

While Chapter II focused on how organizational principles could be adjusted to better support enterprise risk management, it is equally important for an organization to employ the proper enterprise risk management principles. Many discussions of risk management focus on risk mitigation efforts within the bounds of a single product. Even if the product team has members from multiple functional areas, the considerations of risk end at the boundaries of the product team's area of responsibility, or at the boundary of the product itself. Expanding those areas of consideration for risk management requires changing the team perspective on risk, which is achieved through increased attention to and implementation of the principles of enterprise risk management.

A. CORE PRINCIPLES

While it would be overly simplistic to say the only difference between standard risk management and enterprise risk management is the word enterprise, that comparison may do a better job of demonstrating the contrast than anticipated. Somewhat appropriately, Merriam Webster's Dictionary definition of the word enterprise is, "A project or undertaking that is especially difficult, complicated, or risky." An alternate definition is, "A unit of economic organization or activity; especially: a business organization." Combining these two definitions yields an undertaking that is complicated and risky and related to a business organization. Extrapolating slightly beyond that definition would yield a description of enterprise risk management as an effort to examine risks for the entirety of a business organization, and likely a business organization existing in an arena that is inherently risky.

Fundamentally, Tonello (2007) expresses enterprise risk management as the effort of elevating risk discussions to a strategic level. As is discussed later in this chapter, elevating the risk discussion in that manner can help not only with managing risks in an enterprise context, but with that leadership perspective, one also views risks for their potential to serve as opportunities. While much of Tonello's (2007) research was in the domain of private industry, several of his observations are just as applicable to the

government. It was asserted that in most businesses the majority of risk management was handled at the individual business unit level, thus resulting in a bottoms-up risk management approach. “This means it is often left to the discretion of the single business unit to assess the relevance of a risk issue and decide if it requires an immediate mitigation response and if it should be raised to higher ranks in the chain of command or should simply be disregarded as immaterial” (Tonello 2007, 16).

While this approach also has its merits, it can be subject to the blind spots of an individual business unit, or an individual project team within an overall organization. Risks that seem immaterial to one group could indeed be critical to another if risk management extended beyond team boundaries. “With ERM, this approach is inverted and managing risk becomes a cohesive on-going activity led by senior management and overseen by the corporate board” (Tonello 2007, 16). While government entities may not have a corporate board, as previously discussed in Figure 2, the ETRB is managed at the PEO staff level which is comparable to a corporate board. Therefore, this is a seemingly good foundation for the group under review.

Beyond the enterprise approach to risk management, one must consider the cascading impacts of risks, such as the more components that are involved in developing a system, both organizational and physical, the more likely it is that risks in one area of the system will impact or cause risks in another area of the system. “Developing and delivering complex systems requires the management of complex risks” (Brunson et al. 2009, 7). The more complex the risks, the more likely they are to cross organizational boundaries and require management and mitigation strategies from an enterprise perspective. Said another way, “Managing risk within one’s own work scope without thinking of other departments or the whole company may increase total risk for the whole company” (Liu 2011, 21).

Finally, even by accepting the idea that by elevating the risk management conversation to the enterprise level, an item that may have been considered a risk by one business unit may actually be considered an opportunity by the enterprise. There are broader implications in the area of DOD acquisition. These include the idea that most modern DOD systems acquisition is based on the foundation of gaps in current

warfighting capability, or more simply, capability risks that need to be mitigated. Framed another way, risks in an existing system could instead be viewed as enterprise capability gaps for consideration of new system development via the Joint Capabilities Integration Development System (JCIDS) process. As described in the JCIDS instruction, "Validated capability requirement documents then drive the development, procurement and fielding of materiel and non-materiel solutions that satisfy the validated capability requirements and close or mitigate associated capability gaps" (CJCSI 2015, A-1).

Examination of a warfighting capability gap is one of the first steps in the development of a new military system. "The metrics of Gap Analysis are defined on the basis of system value and assessed risks" (Langford et al. 2008, 11). Therefore, from a DOD perspective, a risk to one program may be an opportunity to create another program, one tailored to address just that risk. Examining risks at the enterprise level within DOD could help enable the more effective use of acquisition resources. Do not address that risk in the program that discovered it, benefiting only the user base of that discovering system. Instead develop a specialized solution to address that risk for all warfighters.

B. RELATIONSHIP OF CORE PRINCIPLES TO ENTERPRISE IMPLEMENTATION

Utilizing the overarching principles discussed in the previous section, six criteria were derived to be used in evaluating how a risk management organization adheres to the core principles of enterprise risk management. These six criteria are discussed over the next several sections.

1. Ability to Consider Short-Term and Long-Term Impacts of Risks

In a risk management strategy that is limited to a single product, or even to a single effort within a product, risks are assessed for impact solely on that product. Thus the impact assessment is typically just considered in the short term, relatively speaking. One of the fundamentals of approaching risk from an enterprise perspective is that the company, or departments, that comprise the enterprise will continue to exist beyond any

given individual product. Therefore, all risks considered at the enterprise level must be considered in both short and long term contexts.

Therefore, a risk discovered today, should be evaluated for potential impact for current products as is standard in any risk management environment, but it must also be evaluated for its potential impact on the enterprise as a whole both for other on-going projects as well as for future investment opportunities. “Given its emphasis on strategy, ERM can help the corporation find a better balance between loss-prevention, risk mitigation efforts and risk-taking, entrepreneurial endeavors” (Tonello 2007, 7).

Later in this section there is a wider discussion on the use of risks for potential future investment, or in DOD context, for examining risks as inputs to gap analysis activities for future projects. From a general enterprise risk management approach, however, this evaluation metric is representative of one of the most fundamental tenets of managing risks at an enterprise level. This criterion evaluates an organization’s ability to look at risks beyond just current efforts, but rather for broader impacts not only to other projects, but to the organizational body as a whole.

2. Evaluating a New Risk with Regard to its Impact on Existing Risks

It sounds intuitive to say that a newly discovered risk could have impacts on risks already in the risk management system. Despite that, this is not something specified in the *Risk Management Guide for DoD Acquisition*. This is also discussed as a potential limitation in organizational alignment research, “Managing risk within one’s own work scope without thinking of other departments or the whole company may increase total risk for the whole company” (Liu 2011, 21).

As Liu (2011) says more directly, “A given risk influences other risks.” This concept appears to be very straightforward and foundational, and yet it again is not something covered in any depth in DOD risk management guidelines. Also, as was discussed in the previous section, if an organization is only examining risks within the context of a specific project or a specific timeline, then consideration of other enterprise risks that fall outside of either of those parameters would not be considered in relation to any newly nominated risks.

Building from the first criterion to consider risks in both short and long term phases of a project or enterprise, this is a logical second criterion. If risks are being considered beyond the boundaries of a single project, then comparing them to risks on other enterprise efforts should be the next level of implementation for an enterprise risk management structure. In this context, risk management efforts on projects from all aspects of the enterprise should be utilizing risk registries or other risk tracking systems from all other projects or efforts within the same enterprise. This provides the necessary information to compare new risks in one area against existing risks in any other area, presuming both an enterprise risk management mindset as well as the ability to share risk information across the enterprise in a common context.

3. Risks Managed at the Most Detailed Level Possible

In order to truly understand impacts of risks on the enterprise as a whole, it is critical to be able to understand all potential risks at the greatest level of detail available. Liu (2011) performed a significant amount of psychologically-centric research within the context of enterprise risk management and found that many people look at vague events as having vague impacts. Put another way, the less detail there is associated with a risk, the less detail will likely be associated with the consequences of that risk, and thus dependencies on or from other aspects of the enterprise will be abstracted away and the risk will not receive the focus it needs for proper mitigation strategies to be developed.

This would be especially true of risks where specific mitigation steps require cooperation from other aspects of the enterprise. Without defining these mitigation efforts in detail, the enterprise dependencies or implications would not be detected. “In the ERM context, a high-level construal of paying taxes might be [described as] complying with IRS regulations and avoiding regulation risk, whereas a low-level construal of this activity might focus on details such as the tax deductions, the tax payments and the filing deadlines” (Liu 2011, 24). Using this example, if the risk statement was focused on avoiding a tax audit, then the high-level risk mitigation would simply be to pay the required taxes. This reads as a very simple activity and would be classified as having a high consequence but low likelihood in most standard risk models. Examining the

specific steps needed to pay the required taxes includes the low-level detailed activities that must be completed. These detailed mitigations include 1) calculating the deductions, which in an enterprise context could result in new risks ensuring there were staff on hand with knowledge of tax law; or 2) making the tax payments on time, which might yield another risk as to whether there was an existing communications mechanism between the department that calculated the tax payment and the department that actually submitted the payment.

For this criterion to effectively manage risks at an enterprise level, one must define risks and the associated mitigation efforts at a very detailed level. Without this specific description of the risk and mitigation steps, the execution of the previous two criteria will be very difficult. A risk manager cannot evaluate short and long term impacts of a given risk if the efforts that will be undertaken to mitigate the risk cannot be expressed in a context that associates temporal impacts with the mitigation efforts. Additionally, the impact of a risk in one area of the enterprise on risks in other areas of the enterprise cannot be assessed if all the risks are at a very abstracted level. Using the tax example from earlier in this section, just describing the risk as being a negative impact if taxes were not paid on time would not be nearly enough detail for an enterprise to examine the communication paths between the financial department determining the tax burden and the department making the tax payments. Having detailed risk definitions and detailed risk mitigation efforts are a mandatory precursor to being able to employ enterprise risk management techniques.

4. Presence of Enterprise Engineering Models or Architectures to Provide Objective Context for Technical Risk

To provide the necessary detail described with the previous criterion, an overall context of the system or organizational construct is a key artifact that must already be defined. To put risks in context of an overall system, system-of-systems, enterprise, or other larger construct, that large construct must have a definition that is common for all participants. In the case of enterprise risk, this could be an enterprise engineering model to provide reference for technical risks, or more generically, an enterprise architecture.

Enterprise architecture is often described in a technical, system architecture focus, specifically with regard to Information Technology systems. Enterprise architecture, however, can also be a vital tool for determining system dependencies, whether through system-to-system interfaces or system-to-stakeholder interfaces. One of the chief sources of technical risks for newly developed systems is the failure to adhere to industry standards or specifications in defining interfaces and data exchange models (Tse 2016).

Having a defined overall system enterprise-level architecture is required to be able to define technical risks in adequate detail to analyze them for enterprise impacts. “Acquisition life-cycle decisions can be potentially flawed if the systems engineering development model isn’t appropriately matched to the complex system being developed” (Brunson et al. 2009, 7). It is very difficult to determine impacts across an enterprise of systems, and therefore difficult to employ enterprise risk management efforts if that enterprise is not commonly defined.

5. Risks Evaluated with Context of System Position in Acquisition Life-Cycle

The methods that would be used to mitigate a risk vary depending on where the subject system is in its development life-cycle. A system still in the planning and design stages that has a dependency risk related to an interface with an external system has several paths available for mitigating that risk. If that same interface risk is not discovered until final system testing though, the available mitigation options are far more limited and almost certainly more expensive. Given recent DOD emphasis on rapid

prototyping and fielding of capabilities (Pomerleau 2016), the chances of risks being discovered for the first time late in the life-cycle increase substantially. Mitigating the impacts of discovering risks late in the life-cycle could be aided through the employment of enterprise risk management techniques. “These systems [information technology systems] are often intended to operate in highly volatile environments and, thus, are subject to changing user needs and expectations” (Stevens et al. 2009, 75). Examining risks in both the short- and long-term contexts, evaluating those risks in the context of other existing risks, and ensuring that risks and mitigations are described in sufficient detail, from the time a risk is first raised, should all be done within awareness of the system’s current phase within the development life-cycle.

Given this, it is not sufficient only to evaluate risks with regards to their potential enterprise impact. The ability for a system to mitigate a risk, given the system’s position in the development life-cycle, should also be a consideration. “For these systems [systems where change is inevitable], there is a risk that requirements are locked in too early and may not be responsive to legitimately changing user needs and that technologies become outdated while the system is still in development” (Stevens et al. 2009, 75). The mitigation for a risk discovered in one system may actually be executed by a different system within the enterprise to lower the life-cycle impact on the original system, where the risk was discovered.

While the previous enterprise risk management evaluation criteria focused on the ability to define and mitigate risks outside the boundaries of one specific project yet within the enterprise, this criterion instead is focused on ensuring a consideration of how to best mitigate a given risk includes the context of the system’s stage in its overall life-cycle. Just as defining a new risk’s impacts on other risks could yield a mitigation in System B for a risk found by System A, a similar impact could be driven by life-cycle considerations. An interface risk between Systems A and B, found by System A as it is going through final test, could be mitigated more effectively and efficiently for the whole enterprise if System B is earlier in its development life-cycle. A key component for being able to make such an evaluation is an overall enterprise architecture, which could be used for helping to identify these interfaces and dependencies between systems. This is

another example of these enterprise risk management principles being closely related. The ability of a risk management approach to consider these other facets of a risk beyond just the risk statement is critical to effective enterprise risk management.

6. Assessment of Ability to Mitigate Risk in Current Enterprise Architecture

A final consideration in enterprise risk management is that the most appropriate or effective way to mitigate a risk within the enterprise could be to expand the enterprise itself. One of the foundations for determining the scope of new DOD programs is identifying capabilities not already provided by existing systems, "The metrics of Gap Analysis are defined on the basis of system value and assessed risks" (Langford et al. 2008, 11). In this case, the assessed risk could be from a predecessor system that was unable to meet all of its capabilities, or perhaps in fulfilling its requirements exposed a new gap in capability that was not considered previously.

Frequently, these gaps in capability are defined in terms of risks to a core DOD mission set. Whether it be an actual system vulnerability or a potential threat from an adversary, the capability gaps are often defined in terms of risk to the overall force, a fundamental enterprise risk. "The risks are a function of the threats and vulnerabilities, where threats are typed by magnitudes and frequencies, and vulnerabilities are determined by the likelihoods of success" (Langford et al. 2008, 20).

Therefore, the final criterion for evaluating an organization's enterprise risk management implementation is to determine if it is capable of evaluating enterprise risks as risks that should not be addressed by the current enterprise, but rather a risk that should require a change or expansion of the enterprise. This is the capstone of determining either enterprise system or organizational limitations, and indicates that all the prior enterprise risk management criteria have already been employed. If risks are:

- evaluated for near and long term impacts,
- evaluated in context of other risks,
- mitigated at a detailed enough level to determine impacts across the enterprise,

- based on a common definition of the enterprise architecture, and
- account for limitations to mitigations based on the system's place in the development life-cycle.

Yet the risk still cannot be adequately mitigated, then that may indicate a limitation of the enterprise itself, requiring mitigation by changing the enterprise as a whole.

C. ANALYSIS OF RISK MANAGEMENT PRINCIPLES APPLIED IN PEO C4I ETRB

Utilizing the principles of implementing an enterprise risk management framework just described, this section now examines how the PEO C4I ETRB implements those principles.

1. Ability to Consider Short-Term and Long-Term Impacts of Risks

To implement this principle, both the risk owner and the overarching risk management framework would need to mandate a time consideration for risk impacts and risk mitigations. While this may also imply a consideration of scope impact, that is covered more by the next criterion. The ETRB charter, however, is largely silent on definitions of the temporal impacts of Enterprise Technical Risks (ETRs) that are brought to the ETRB. Table 7 provides a summary of how the ETRB addresses this enterprise risk management principle.

Table 7. PEO C4I ETRB Evaluation—Enterprise Risk Management Criterion #1

Evaluation Criterion	**Ideal Case**	**PEO C4I ETRB Comparison**	**Conclusion**
Ability to Consider Short-Term and Long-Term Impacts to Risk (Tonello 2007)	Risk framework includes adequate definition to account for evaluation of near term single-project impacts and long-term multi-project or enterprise impacts.	The ETRB charter is largely silent on the content of any given enterprise technical risk (ETR) with regards to scope or temporal considerations. This definition is left up to the assigned ETR owner.	The ETRB does not provide any specific guidelines that indicate either alignment or misalignment with this principle. Further definition on the content of a risk description would be useful with regards to this criterion.

As the ETRB charter is silent on this facet of risk management, it would be left to the individual ETR owners to determine impact dates for a given risk, which would almost certainly lead to inconsistent definitions of impact timelines for risks with different owners. Having variations in the mechanisms utilized to define and manage risks depending on the risk owner is counter to the core concepts of enterprise risk management, indicating that all risks from all aspects of the enterprise should be managed in the same fashion and utilizing common criteria.

While potential impacts of this lack of definition of risk impact timelines within the ETRB is further discussed in Chapter IV, it should also be noted that the ETRB charter does indicate that ETRB members should "Identify additional impacted areas when reviewing a submitted ETR" (PEO C4I 2015, 5). While this appears to be more aligned with discussions on how a risk impacts parts of the enterprise other than the segment nominating the risk, it could also be used as a method for discussing the timeline for risk resolution so as to determine time constraints on mitigating the risk. This should

be made clearer in the ETRB's governing charter to ensure consistency amongst all nominated ETRs while enabling more direct comparisons between ETRs.

2. Evaluating a New Risk with Regard to its Impact on Existing Risks

This criterion is likely the most fundamental principle of implementing an enterprise risk management framework. To manage risks in an enterprise context, all risks must be viewed through their impact to the enterprise as a whole, not solely a certain subset. To accomplish this, the risk management structure must enable risks to be defined in common terminology, reviewed in common forums, and enforce upon the risk management membership the requirement to view risks beyond the boundaries of just their individual assignments and especially with regard to impacts on existing risks being managed by the enterprise. On this criterion, the ETRB charter does specifically address the review of risks for impacts beyond those stated in the ETR. The mechanism for this evaluation is described in Table 8.

Table 8. PEO C4I ETRB Evaluation—Enterprise Risk Management Criterion #2

Evaluation Criterion	**Ideal Case**	**PEO C4I ETRB Comparison**	**Conclusion**
Evaluating a New Risk with Regard to its Impact on Existing Risks (Liu 2011)	Risk framework provides individual risk owners access to all other risks within the enterprise, to include common risk definitions and levels of detail to allow for cross-referencing of risks.	ETRB charter states that the core members shall identify any other areas that could be impacted by a given ETR when it is defined or updated or otherwise discussed in the ETRB.	While the charter does not specify a common method to be used to determine this impact, it does indicate that the members have the responsibility to look at individual risks in the context of other, existing risks, or for the potential of a new risk to generate further risks in other parts of the enterprise.

On this item, the ETRB charter is very specific in assigning the responsibility to evaluate the impacts of risks beyond the area they are nominated from. For the ETRB Members roles and responsibilities, one of the enumerated tasks is to review each ETR and identify other impacted areas beyond those named in the initial ETR.

The charter is silent on how these other impacts are captured with regard to the ETR, nor does it address how these new, presumably enterprise-level, impacts are to be tracked over the life of the ETR. It also does not cover how mitigation strategies for the enterprise impacts will be developed nor does it describe how responsibility for implementing those mitigations will be tracked. The consideration of enterprise impacts is important, but also important is how those impacts will be tracked and dealt with.

3. Risks Managed at the Most Detailed Level Possible

Related to the examination of the first criterion, the ETRB Charter is also silent on the level of detail necessary to define ETR descriptions or associated mitigation strategies. It does indicate that the ETR owner needs to keep the risk current based on all inputs. Without specific guidance or a reference to indicate to a risk owner the level of detail necessary in the risk definition or mitigation steps, however, it is likely that each owner will take their own definition of what constitutes sufficient detail. A summary of the ETRB implementation of these best practices is in Table 9.

Table 9. PEO C4I ETRB Evaluation—Enterprise Risk Management Criterion #3

Evaluation Criterion	**Ideal Case**	**PEO C4I ETRB Comparison**	**Conclusion**
Risks Managed at the Most Detailed Level Possible (Liu 2011)	Risk structure includes sufficiently detailed risk statement and mitigation tasks to determine where either risk or mitigation impacts or interfaces with other systems in the enterprise.	The ETRB charter does not specify a level of detail in capturing the risk or any associated mitigations, only identifying that the risk owner must keep the risk current.	While there is a template for entering ETR descriptions, mitigations, and impact dates, there does not appear to be any set guidance on the level of detail that must be captured for each of those ETR elements. This likely results in varying levels of detail depending on the ETR owner.

There is some degree of compliance with this principle as the ETRB has assigned risk ownership responsibility for each ETR, thus there is a person or group responsible for defining the risk and associated mitigations. The lack of a reference or other guidance to indicate the proper level of detail that could be held consistent for all risks that come to the ETRB is a limiting factor with regard to fulfilling this criterion. If all risks receive a different level of analysis, and are expressed in differing levels of detail, it will be of little consequence that the ETRB members are responsible for identifying all impacted areas related to new ETRs, as there will not be enough information in the ETRs for the members to make those connections for other impacts.

Given the current lack of specificity in risk and mitigation definitions, any efforts at enterprise risk management centered on this criterion would mostly be the result of dedicated individual efforts. This still provides value to the enterprise as a whole but is nonetheless inconsistent. Some methods that could improve the implementation of this enterprise risk management principle are further discussed in Chapter IV.

4. Presence of Enterprise Engineering Models or Architectures to Provide Objective Context for Technical Risk

To aid risk reviewers in determining impacts to other systems or organizations within the enterprise, a common definition of the enterprise is a critical foundational item. To provide detailed risk descriptions, especially impact statements, for risks that impact other portions of the enterprise it is necessary to have a common context for describing those impacts. Thus an overarching architecture either for the technical system-of-systems, or enterprise in any other construct, would provide that common context for risk identification or risk management. The enterprise reference artifacts and context available to the ETRB are summarized in Table 10.

Table 10. PEO C4I ETRB Evaluation—Enterprise Risk Management Criterion #4

Evaluation Criterion	**Ideal Case**	**PEO C4I ETRB Comparison**	**Conclusion**
Presence of Enterprise Engineering Models or Architectures to Provide Objective Context for Technical Risks (Brunson et al. 2009)	Enterprise system design models or enterprise architectures (whether technical or organization) are defined and baselined such as to provide objective artifacts to evaluate risks against so as to determine enterprise-level impacts.	While system-of-systems or other representations of the enterprise are in work at SPAWAR, none are specifically referenced by the ETRB charter for comparison.	If there are no common artifacts used to define the role of a system in the scope of the whole enterprise, then even risks described in great detail are still subject to not capturing all the enterprise impacts of a risk as there is no core definition of the enterprise.

The ability to fulfill this criterion does not exist entirely within the scope of the ETRB. Any common definition of the enterprise, whether architectural or just organizational, must be agreed upon by the entirety of the enterprise to be effective. Not having an agreed to definition of the enterprise is an enterprise risk in and of itself, and something that the ETRB should pursue to benefit the organization's ability to truly perform enterprise risk management.

As was mentioned in Chapter II, the ETRB charter provides a mechanism to raise risks to the PEO's top level engineering forum, the Systems Engineering Board (SEB), or top level program-management board, the Portfolio Governance Board (PGB). A potential use case for this process would be nominating the risks associated with attempting enterprise risk management without an agreed to set of enterprise system architecture artifacts to serve as a common reference for risk identification.

5. Risks Evaluated with Context of System Position in Acquisition Life-Cycle

The fifth evaluation criterion for organizational alignment to support enterprise risk management in Chapter II addressed the concept of ensuring members from all aspects of the organization were reviewing risks in areas, whether project or functional, outside of their own area of focus. While the ETRB does have all core members review all risks, one of the limitations of the board is that it only mandates the core engineering staff to be consistent members of the ETRB. While members from other functional areas within the PEO are considered as advisors, they are only asked to participate as is applicable. Therefore, contributions from the acquisition portions of the organization would be inconsistent at best. A summary of the ETRB compliance with this criterion is discussed in Table 11.

Table 11. PEO C4I ETRB Evaluation—Enterprise Risk Management Criterion #5

Evaluation Criterion	**Ideal Case**	**PEO C4I ETRB Comparison**	**Conclusion**
Risks Evaluated with Context of System Position in Acquisition Life-Cycle (Stevens et al. 2009)	Risk structure includes identification of system development status to provide context for impact of mitigating a risk within the subject system or another system in the enterprise.	The ETRB allows for members of the acquisition community to also join the ETRB to augment any technical risk analysis with acquisition impacts. Their participation is not mandatory though, while the technical staffs' participation is mandated.	To account for different approaches in mitigating risks based on potential acquisition impacts, more regular participation by the acquisition experts within the PEO would be beneficial.

In many ways, the ability of the ETRB to fulfill this risk management principle is directly related to the fulfillment of Criterion #5 in Chapter II, specifically with regard to the regular participation of acquisition experts in the ETRB. As currently constructed, and utilizing only the mandatory members of the ETRB, it would be left to the engineering staff to evaluate risks in the context not only of technical impacts, but also with consideration for alternate mitigation approaches given potential acquisition impacts to the systems in question. This approach would imply very extensive expertise within the technical competencies of the organization, and while not necessarily impossible, is nonetheless very unlikely. Therefore, it would be prudent for the ETRB to expand its mandated membership, or otherwise incorporate other functional areas in the review of potential enterprise risks to ensure all aspects of a risk are considered when mitigation strategies are being decided on.

6. Assessment of Ability to Mitigate Risk in Current Enterprise Architecture

Much like the previous enterprise risk management evaluation criterion was linked to an organizational alignment criterion from Chapter II, this criterion is linked to criterion #4 earlier in this chapter. There is always the potential that a new risk is best mitigated not through any existing aspect of the enterprise, but rather by expanding the enterprise through a new system or other method of expanding available capabilities. The summary of the ETRB's fulfillment of this criterion is provided in Table 12.

Table 12. PEO C4I ETRB Evaluation—Enterprise Risk Management Criterion #6

Evaluation Criterion	**Ideal Case**	**PEO C4I ETRB Comparison**	**Conclusion**
Assessment of Ability to Mitigate Risk in Current Enterprise Architecture (Langford et al. 2008)	Risk context is provided to determine if mitigation of a risk fits within the scope of an existing system or if it requires a new system to expand the enterprise boundaries.	Other than mentioning that ETRs can be transferred to another group to mitigate, there is no specific mention within the ETRB Charter of a process to evaluate whether the risk *should* be mitigated within the boundaries of the current definition of the enterprise.	This is a criterion that would be a natural extension of an enterprise risk management process that was already fully mature and fulfilling the previous five criteria identified in this chapter. Therefore, it is not a major limitation of the ETRB that it does not address this concept, but is still something that should be considered in any revisions to the ETRB scope or charter.

In order for the team performing an evaluation of a risk to determine if it is best mitigated through existing components of the enterprise, or if it instead defines a new function of the enterprise, the team must have an agreed to representation of the enterprise to use as a baseline. This was discussed in regards to enterprise risk management principle #4 earlier in this chapter and included the analysis that PEO C4I did not have a common definition or representation of the enterprise available as a resource for the ETRB.

Therefore, it will not be possible for the ETRB to consider methods to fulfill this criterion without first implementing or developing an enterprise baseline definition to

meet criterion #4. As an approach is defined to be able to provide a common representation of the enterprise, however, there should also be consideration on how to expand the ETRB scope to utilize that enterprise baseline not only for mitigation of risks within the enterprise, but for evaluating when the best mitigation option involves expansion of the enterprise.

D. CHAPTER SUMMARY

This chapter provided a brief review of risk management principles, both within industry in general and within the DOD in particular. It discussed some of the basic aspects of DOD risk management guidance and contrasted that with some of the fundamental concepts of enterprise risk management. This included the idea of elevating risk management to a strategic level through the regular involvement of senior leadership in risk management discussions.

The chapter then utilized core concepts from existing enterprise risk management research to define six core principles for successfully implementing enterprise risk management techniques within an organization. These principles began with very fundamental concepts, such as regarding risks beyond their impacts in the immediate term. The principles also include those that would be implemented via a mature organizational approach to enterprise risk management, such as having a common definition of the enterprise, whether architectural or in some other form. This common definition is necessary for any risks to truly be evaluated in an enterprise context, otherwise every risk owner's view of the enterprise would almost certainly be different. The final enterprise risk management principle was to examine risk mitigations not only for mitigation options within the existing enterprise, but also to examine risk mitigations that involved expanding the enterprise itself. This aligns closely with the concepts utilized by DOD in threat and gap assessments when defining the capabilities to be fulfilled by new acquisition efforts.

These six enterprise risk management principles were then applied to the PEO C4I ETRB. An initial analysis of the ETRB's level of compliance was performed, including discussion of what was potentially implied by language in the ETRB charter

even if it was not mentioned specifically. This high-level evaluation also considered areas where other aspects of the organization needed to provide reference or baseline material, such as an overall enterprise architecture, to the ETRB to enable full enterprise risk management.

More comprehensive analysis of the ETRB's level of implementation of these six principles are provided in Chapter IV. This analysis includes a discussion on the limitations of the PEO C4I ETRB based on any gaps found in the board's implementation of these core enterprise risk management principles, as well as any other enabling activities that must take place to aid the ETRB in truly serving as an enterprise-level risk board.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RECOMMENDATIONS FOR PEO C4I ETRB

Using the evaluation criteria established in Chapters II and III based on core principles for organizational alignment and enterprise risk management, this chapter provides a more in depth review of how the PEO C4I ETRB implementation strategy fulfills those criteria. This review covers the level of alignment between the ETRB and the core principles, but also the impacts of that alignment or misalignment.

This chapter also reviews potential adjustments that could be made either to the ETRB's structure or its implementation to improve its alignment with the core principles described in the prior chapters. This review includes a discussion of the benefits to be seen both at the level of the ETRB and for the organization as a whole if the suggested adjustments are made.

A. ORGANIZATIONAL STRENGTHS, WEAKNESSES AND RECOMMENDATIONS

The comparison of the PEO C4I ETRB structure and participants found several areas that reflected excellent alignment with the organizational principles discussed in Chapter II for how best to enable enterprise consideration of risks. There were also several areas that demonstrated poor alignment and one that was largely undefined. This last category is described as neutral in the following discussion. It should be noted that the assessment of one criterion resulted in a strength for the ETRB in one context and a weakness for the ETRB in another context. While the categories are labeled as strengths and weaknesses, this is solely in regards to the level of alignment with the core organizational principles defined for maximum enabling of enterprise risk management. The actual impacts of these strengths and weaknesses are discussed in the Recommendations section.

1. Strengths

Within the organizational alignment criteria, there were two areas where the PEO C4I ETRB strongly aligned with the core organizational principles. These are: 1)

Enterprise-Level Definition of Risk Management Practices and 2) Evaluating Risk in Terms of Impact to Efforts Other Than Your Own.

a. Enterprise-Level Definition of Risk Management Practices

While there may not be an enterprise standard for how to define or mitigate each new ETR brought before the ETRB, the fact that there is an ETRB indicates that leadership acknowledges that there are risks that have enterprise level impacts. It is also a reflection of the desire of leadership to manage and mitigate those risks as an enterprise organization.

This does not necessarily speak to the efficacy of this enterprise board, and that is addressed later in this section. Acknowledging the presence of risks at an enterprise level and establishing a working-level framework with representatives from across the enterprise are necessary actions to implement effective enterprise risk management. The chartering of the ETRB demonstrates that PEO C4I has an understanding that risks can have impacts beyond a single project, and an appreciation that those types of risks must be managed in an enterprise context.

The existence of the ETRB within the context of the PEO organization also provides a mechanism for the ETRB to get leadership attention on key or highly impactful risks. This defined path to take an enterprise risk and utilize the PEO's top systems engineering board (SEB) or programmatic board (PGB) to assist in mitigating the risk demonstrates a commitment to enterprise risk management at the highest levels of the organization. That is why the ETRB is considered to demonstrate a strength in the ability to coordinate enterprise level definition of risk management practices.

b. Evaluating Risk In Terms of Impact to Efforts Other Than Your Own

The ETRB charter dictates that one of the core responsibilities of the members of the ETRB is to evaluate all newly raised candidate enterprise technical risks for potential impacts beyond those stated in the draft risk. This is the definition of enterprise thinking and a key enabler to enterprise risk management. The breadth of the enterprise considerations is dependent on which areas of an organization are considered members of

the board, which is discussed later, but the mandate that all members consider *any* potential impact of the risk immediately brings the risk to an enterprise level of review and potential mitigation.

For those employees that are members of the ETRB, this also emphasizes the organizational concept that each employee must consider risk ownership as part of their core responsibilities; also, that risk management must not just be for areas of the enterprise that they work in every day but rather in all aspects of the enterprise. Through feeling that responsibility, and then participating in a forum such as the ETRB that mandates they consider all potential impacts of a risk and not just impacts within their project or their focus area, the organizational foundation for defining risks in terms of the enterprise and managing risks in terms of the enterprise is established.

2. Weaknesses

The analysis also showed that for three of the organizational alignment criteria, the ETRB had weak alignment. These are: 1) Employee's Responsibility / Accountability for Managing Risk, 2) Cross-Team Coordination for Purpose of Managing Risk, and 3) Enterprise-Level Definition of Risk Areas for Each Organizational Component

a. Employee's Responsibility / Accountability for Managing Risk

This organizational criterion provided an interesting contrast to one of the areas that was evaluated as a strength for the ETRB, the requirement of members of the ETRB to evaluate risks for impacts to areas other than their own. While that edict in the ETRB charter is indeed a strength with regard to close alignment to that enterprise-view of risks within an organization, it is also in many ways a strength with a weak foundation.

The ETRB charter does dictate that all ETRB members consider risks in an enterprise context by considering impacts outside of their own area of responsibility. The ETRB directed membership, however, consists only of participants from the engineering competency within PEO C4I. Therefore, to a large extent the strength of an enterprise viewpoint on risks at the ETRB is restricted by the fact that such a limited scope of expertise within PEO C4I is required to participate in the ETRB.

If only the employees with engineering backgrounds or areas of focus are mandated to consider risk in an enterprise context, or to have the responsibility to manage risks at an enterprise risk board, then the ability for the organization as a whole to assert that all employees feel the responsibility to manage risk at an enterprise level seems severely limited. Therefore, this assessment has concluded the ETRB has very weak alignment to this particular criterion. Furthermore, this weak alignment also impacts the next organizational criterion under consideration.

b. Cross-Team Coordination for Purpose of Managing Risk

It is very difficult for this to be seen as anything other than a weakness for the ETRB. As the only mandatory members are the engineering staff, there is only one team with the responsibility to participate in managing enterprise risks. Cross-team coordination is not possible as there are no other teams participating in an enterprise sense.

There is a caveat to this assessment. The ETRB is by its very name focused on Enterprise Technical Risks, so the core membership is focused on the engineering staff which is a logical path for the board to take. For PEO C4I as a whole, however, this is the only group specifically charged with enterprise risk management; so even if the ETRB is viewed to be effectively managing technical risk at an enterprise level, the PEO as a whole would still face the same limitation with regard to cross-team coordination.

Therefore, while it is possible to view the ability of the engineering staff to coordinate on risks across multiple projects as a strength of the ETRB, the overall ability to have cross-team risk management is significantly limited. If the PEO viewed the technical domain as the primary source of enterprise risk then this might be the right approach toward enterprise risk management. The path for leadership to identify key areas of potential enterprise risk, however, is also considered a weakness in this analysis.

c. Enterprise-Level Definition of Risk Areas for Each Organizational Component

One of the strengths of the ETRB is that it has two paths to elevate critical enterprise risks to the higher echelons of the PEO organization. In fact, it has defined

paths for elevating risks to the top engineering body in the PEO, the Systems Engineering Board (SEB) as well as the top programmatic body, the Portfolio Governance Board (PGB). That these two paths are both defined indicates the idea that the ETRB could have risks with both technical and programmatic impacts and thus could require assistance, prioritization, or adjudication in both the technical and programmatic domains.

The reverse is not documented as part of the ETRB though. There is no directed or specified path by which the PEO leadership, whether technical or programmatic, could provide inputs on areas of enterprise risk that leadership desires an increased focus or awareness. While in theory any member of the PEO organization could nominate a new risk for consideration from the ETRB, and therefore leadership could identify those risks, there is no specifically defined mechanism to solicit this leadership insight.

If the path to elevate working-level risks for leadership consideration is defined, any path to provide leadership guidance down to the ETRB should be equally defined. This may be accomplished by simply amending the ETRB charter to reflect the reality if this guidance is already being provided today. Given the evidence available via this research effort though, this is evaluated as a weakness of the ETRB with regard to alignment to organizational evaluation criteria.

3. Neutral

One of the organizational alignment criterion was implied or otherwise indirectly indicated in this research, but not explicitly defined within the ETRB, which is Allowance for Multiple Teams to Co-Own Risk Mitigation. This criterion is therefore evaluated as neither a strength nor a weakness, but rather as neutral.

Similar to the concept of cross-team coordination for risk management, the ETRB does not specify any particular allowances for multiple teams to own a risk. While the ETRB membership can identify other impacts beyond the team that submits the risk, the ETR owner is described as a single person or team.

Again, this is not explicit in the charter which is why the alignment is considered neutral; as multiple team ownership of an enterprise risk is neither defined as a potential

mitigation mechanism, nor prohibited by any of the other tenets of the ETRB. To better manage enterprise risk, a revision of the charter could more clearly define processes to allow for multiple groups to manage and own a risk.

While allowing for a multiple-team risk ownership construct would assist in implementing this organizational alignment principle, some of the other weaknesses identified earlier in this chapter would also need to be addressed to make multiple-team ownership more productive. Recommendations to improve the alignment of the ETRB to the organizational principles that enable enterprise risk management as described in Chapter II is covered in the next section.

4. Recommendations

The recommendations provided in this section are from the perspective of ensuring the PEO C4I ETRB has the greatest possible alignment with the organizational principles that are most important for enabling full enterprise risk management.

a. Assign Risk Management Responsibilities to Every Employee

For any other recommendation to be implementable, there must first be a clear definition of responsibility for all members of the organization to manage risk. A foundational way of accomplishing this could include adding performance objectives for each employee related to managing risk. Some employees already have such an entry, in whole or in part, in their yearly performance plan. Therefore, expanding this practice would provide not only a mechanism but also motivation for employees to analyze organizational activities for risks and take a role in managing and mitigating those risks. Additionally, it would be beneficial for PEO leadership to present cases of successful risk management at regular intervals, perhaps at all hands meetings or via the regular internal PEO newsletter. This would not only demonstrate the benefits of an organizational focus on risk management, but would also reinforce to all employees that they too should be focused on risk management as it is a leadership priority.

b. Expanding Membership of the ETRB

It is possible that the ETRB was solely intended to manage technical risks. Given that there are no other enterprise risk boards in PEO C4I, however, this recommendation examines methods to increase the scope and expertise of the ETRB to be truly representative of the enterprise. In order to become a truly enterprise risk board, even if it maintains its focus on technical risks, expertise from other functional areas should be included as mandated members of the board. While the risks discussed could still be technical in nature, the mitigations for the risks do not necessarily need to be in purely the technical domain.

Even if the board members follow the organizational principles from Chapter II, through taking personal ownership of all risks across the enterprise, coordinating with representatives from other teams or projects to address risks, and even sharing risk ownership responsibility with other members, if all of those members are still engineers the potential risk mitigations that will be considered will be technical in nature by default. For true enterprise risk management, other avenues for risk mitigation must be considered, and to understand potential mitigation options in non-technical domains, the board would greatly benefit from having mandatory members outside of the engineering functional area.

The rest of the board policies could remain intact and could provide even greater benefit through the more varied expertise of the audience. For example, the policy that all ETRB members should examine every candidate risk for impacts beyond those stated by the member identifying the risk would result in a more comprehensive view of the potential impacts, extending beyond the technical domain. This is an artificial limitation of the board as it stands now given the narrow scope of mandatory members, even if the desire is to focus exclusively on technical risks.

c. Requesting Regular Enterprise Risk Focus Area Inputs from Leadership

While the ETRB does have a path to utilize at the chair's discretion to raise risks to higher echelon boards for assistance or prioritization, there is no identified mechanism for those higher boards to identify areas of enterprise risk of particular concern that the

ETRB should place increased focus. As stated earlier, it is possible given the existing ETRB charter that any member of leadership could raise their own risk to the ETRB. It would seem that the concept of enterprise risk management would be better encouraged if a regular interaction with PEO leadership was scheduled specifically to gather insight on areas of risk they see and about those on which they are expanding effort.

Beyond the knowledge of where leadership sees potential areas of enterprise risk would be the added benefit of learning if any additional efforts had been initiated by the PEO leadership to address those risks. Whether pilot projects, or other experiments, it would benefit the ETRB to have that awareness so that the results of any of those initiatives could be considered as potential mitigations or guidance for future risks raised within the board. In short, the more interaction there is between the risk board and leadership the more effective the enterprise risk management efforts can be. These interactions should not be solely event driven, but schedule driven as well. As an added benefit, having these regular information exchanges on potential areas of risk will also provide the opportunity to gain feedback from leadership on proposed mitigation efforts to existing risks. This improves the ability to have cross-team coordination on enterprise risks, though in this case one of the teams is the overall PEO leadership group.

d. Requiring Regular ETR Status Updates to Leadership

This recommendation is in regards to an item that was considered a strength from the organizational alignment perspective. The ETRB does define a path to get enterprise-level assistance from both the top PEO engineering board and the top programmatic board. Utilization of either of those paths, however, is left to the discretion of the risk board leadership. This indicates that there are no regular updates to PEO leadership from a risk perspective but rather only in extraordinary circumstances.

Relating to the previous recommendation, if there was a regular meeting to gather feedback from leadership on areas of potential enterprise risk that on those they desired the risk board to focus, it would also provide an opportunity for the risk board to discuss current risks that were being tracked and mitigated. This not only would provide a means to raise leadership awareness on these areas of risk, but would also allow for any

necessary reprioritization from leadership to adjust the board's focus if it was not currently on areas that leadership felt warranted the most attention.

If an additional meeting were too challenging logistically, another path would be to ensure enterprise risks were a regular input to the PEO existing risk review processes. Current processes allow for each PMW to enter their most critical risks, in the view of the Program Manager, for a monthly review with the PEO and associated staff. Adding the enterprise risks as an input to this existing process would not only get leadership review of those enterprise risks, but would put them in a context to be evaluated against existing PMW risks that were already in the monthly review. An enterprise technical risk discussion could also be made a recurring agenda item for the PGB, ensuring a regular discussion of enterprise risks with leadership without needing to add a new meeting to already busy calendars.

Given that one of the key benefits of enterprise risk management is that it raises the level of risk consideration beyond the project execution level up to the enterprise strategy level, a regular briefing to leadership on current priority risks would provide the pathway for the board to get that strategic risk perspective. This would help keep leadership more informed on current efforts but also ensure the board was utilizing its resources in areas that the PEO leadership most needed assistance mitigating existing or future risks.

e. Defining Mechanisms and Criteria for Establishing Multi-team Risk Ownership

There is nothing in the ETRB charter that prohibits establishing multiple owners from multiple teams to own a given enterprise risk, but the ability to do so is limited in two ways. The first is that the membership of the ETRB is currently limited to technical staff and so while multiple different project engineering teams could share a risk, it would still be limited by the technical focus of those members. The second is that since the current technical membership are the only personnel required to evaluate potential impacts to other efforts within the enterprise, some key, non-technical, impacts may be missed so not all potentially impacted teams would be identified to share ownership.

Both of these items could be largely ameliorated through the implementation of the first recommendation in this section. Increasing the breadth of the mandatory board members would increase the potential cross-team impacts both to non-technical areas within existing risks, and help identify additional non-technical teams that would benefit from sharing ownership of a risk.

B. ENTERPRISE RISK MANAGEMENT STRENGTHS, WEAKNESSES AND RECOMMENDATIONS

A review of the PEO C4I ETRB alignment to the enterprise risk management principles identified in Chapter III had decidedly mixed results. There was only one criterion each identified either as a strength or as a weakness. The remaining four criteria were assessed as neutral. These neutral assessments are discussed in detail in the following sections, but generally fall into two categories. The first category is that criteria are simply not addressed by the PEO C4I ETRB charter, and thus the level of their implementation is unclear. The second category is that the criteria's implementation are limited based on the ETRB structure and may be addressed in part by other recommendations either in the organizational alignment section or in this enterprise risk management section.

1. Strengths

In reviewing the ETRB against the core principles of enterprise risk management, there was one area where the ETRB demonstrated a strong alignment. That was, Evaluating a New Risk with Regard to its Impacts on Existing Risks.

One of the core areas of emphasis for the ETRB members is that they are required to consider any and all impacts of a new ETR. This includes consideration for projects in their area of responsibility and any other area they have familiarity with. As this is required with all nominated risks, by definition any risk raised at the ETRB will be considered in the context of all previous ETRs, as well as any localized risks that the ETRB members may also be familiar with.

Even with this being asserted as a strength, there are some limitations, including the fact that the membership of the ETRB required to do an assessment of the

relationship between new and existing risks is limited to the engineering staff. This was cited as a weakness in the previous section. The assessment with regard to implementing best practices of enterprise risk management was focused on having the process and focus on the best practice. On that front, the ETRB is very well aligned to implementing that best practice.

2. Weaknesses

One of the criterion associated with implementing enterprise risk management best practices was analyzed to have very little alignment with the current implementation of the PEO C4I ETRB. That criterion was Presence of Enterprise Engineering Models or Architectures to Provide Objective Context for Technical Risks. To enable employees to assess the impacts of risk at an enterprise level, it is crucial that they all share a common definition of the enterprise. One method to achieve this common understanding is to have one or a set of enterprise engineering models or architectures that can serve as a common reference. These enterprise models would identify the key functions of each enterprise components and how they relate to each other via interfaces and dependencies.

The presence of such a model, combined with the edict that all members of the risk board assess risks across the whole enterprise, not just their area of expertise, would be the desired foundation for developing enterprise-level risks that all members of the risk board would understand. Without these models, it is likely that there are multiple views among multiple members of what the enterprise is, how the various components relate to each other, and what dependencies exist that would either exacerbate or mitigate candidate risks.

Therefore, while not necessarily a task for the risk board itself to implement, the development of these enterprise architecture models are something the members of the risk board should contribute to. By assisting in the development of the enterprise architecture models, the risk board members will have a deeper understanding of the relationships between entities across the enterprise and will have a better foundation for evaluating new enterprise risks in the future.

Developing enterprise architectures will not help only in the enterprise risk management domain, but will also help in defining functionality and boundaries for systems within the enterprise, identifying interfaces amongst those systems, and determining if there are repetitive functions or inefficient connections within the enterprise as a whole. As each of these limitations are discovered, they can then be fed into the enterprise risk management process for adjudication and mitigation.

3. Neutral

The majority of the criteria used to evaluate the ETRB's implementation of enterprise risk management principles demonstrated a neutral alignment, neither strongly nor weakly aligned. Of those four criteria in the neutral assessment grouping, the first two listed in this section are limited by lack of explicit description of their implementation within the ETRB, the second two are limited by other foundational ETRB construct or business rule limitations. These four criteria are: 1) Ability to Consider Short-Term and Long-Term Impacts to Risk, 2) Risks Managed at the Most Detailed Level Possible, 3) Risks Evaluated with Context of System Position in Acquisition Life-Cycle, and 4) Assessment of Ability to Mitigate Risk in Current Enterprise Architecture.

a. Ability to Consider Short-Term and Long-Term Impacts to Risk

There is not anything in the ETRB charter that defines the level of detail that should be associated with a risk. This is relevant to all aspects of risk definition, management and mitigation, including the timeline for taking corrective action on the risk, or the durations at which impacts will start to be seen if the risk is not addressed. The definition of short and long term impacts from a risk are left up to the risk owner to define, and the risk board to modify as they feel is appropriate.

Without any definition or reference for how detailed the risk impact statements should be, or within what durations impacts should be considered, however, it is likely that there will be a wide range of risk impact timelines depending on the risk owner's perspective. This criterion was evaluated as neutral because the lack of definition of impact timeline parameters is not limited by the ETRB charter, it is merely not addressed.

Providing a reference risk as an example, or establishing a template that forces a risk owner to consider various durations into the future and the related risk impacts would help mitigate this. It would also provide for greater commonality in risk definitions and would make them easier to compare in the future as mitigations are enacted.

b. Risks Managed at the Most Detailed Level Possible

Similar to the previous criterion, there is no definition provided by the ETRB charter for what level of detail is necessary within a risk definition. Just as the previous item discussed short and long-term impacts if the risk is not adequately mitigated, there are no given criteria for definition of the risk statement, identification of impacted systems, or level of detail in the mitigation steps.

This again is assessed as a neutral level of implementation as the corrective action would be for the ETRB documentation to provide a reference or other definition of how much detail should be provided for any risk brought before the board. This should include a common level of detail for the risk statement, including how specific the impact should be, whether the impact date should be included in the risk statement or as a separate parameter, and other such details. It should also define how the impacts to other components in the enterprise are defined. It could be just at the product level, or at the most detailed component level possible, which would relate back to the enterprise architecture model weakness described earlier in the chapter. It would also address the level of detail needed in mitigation steps, including identifying the person or group responsible for performing the mitigation step, the time the mitigation should be completed by, and any dependencies among mitigation steps that dictate which could be executed in serial or in parallel.

Just as with the previous criterion, providing a reference or template to ensure all risks have equal levels of detail throughout all the components of the risk will make risks easier to compare. Otherwise, there remains the possibility that risks that are related will not be reviewed because there is not enough information in the risk components to identify such a dependency. Having a common set of information associated with each risk makes every other aspect of enterprise risk management easier to execute.

c. Risks Evaluated with Context of System Position in Acquisition Life-Cycle

The ability for the members of the ETRB to consider the impacts of a systems' position in the acquisition life-cycle, or any other acquisition impacts associated with a risk is partially linked to the personnel included in the ETRB and also partially linked to the emphasis on enterprise risk areas that could be provided by leadership, both weaknesses identified earlier in this chapter. The considerations for the acquisition life-cycle as it relates to enterprise risks could take several forms. One could be that if a risk is discovered late in a systems' life-cycle, it may be that the optimum mitigation is not to change the existing system, but to mitigate the risk with a follow-on system or elsewhere in the enterprise. Another consideration is that the mitigation for a risk might be something that could be addressed via acquisition means, as opposed to technical means.

Having acquisition expertise, as well as logistics, contracts, and other core program functional areas present at the ETRB would aid in assessing each of these areas, not just when technical solutions are not considered ideal, but also in terms of evaluating each new risk that comes before the ETRB. As it is structured now, the emphasis in regard to risk mitigation efforts will tend toward technical mitigations, when other approaches may be easier to implement and yield better results. By addressing the weakness regarding breadth of participating personnel earlier in this chapter, many more options for addressing this neutral implementation of an enterprise risk management practice will become available.

d. Assessment of Ability to Mitigate Risk in Current Enterprise Architecture

As mentioned in the previous evaluation, one option for mitigating a risk to a system is not to change the existing system. Instead the most reasonable mitigation strategy could be to develop a new system, or an additional component to extend an existing system. In Chapter III this criterion was described in the context of the overall DOD acquisition approach where existing capability limitations, and the risks they placed on mission execution, were used to identify potential requirements for new systems.

This approach should be something the ETRB also considers. When a new risk is proposed, it should be evaluated and mitigations considered not only for within the existing enterprise and system boundaries, but also for the potential in developing a new system or component to mitigate the risk. There are considerations at all levels of system development to best implement this principle, which leverages the earlier discussions on ensuring representation from all dimensions of system development, not just engineering but also acquisition, contracting, logistics and any others.

This was not evaluated as a weakness of the ETRB as it could only truly be implemented if all the other organizational and enterprise risk management principles had already been implemented or assessed as strengths. Once the other recommendations of this chapter are implemented, the inclusion of this consideration is the next extension that should be applied to the ETRB.

4. Recommendations

The following are recommendations for implementation by the ETRB to improve its alignment with enterprise risk management best practices. As was stated in the organizational alignment recommendations, if any of these limitations is by intent, then PEO C4I should use that knowledge to tailor the implementation of these recommendations.

a. Define a Common Risk Definition Template

Two of the criteria that were evaluated as neutral are directly related to there being no pre-defined level of definition required for enterprise risks. This includes consideration of impacts at various points in the future but also more fundamentally in the definition of the risk itself.

The development both of a risk template, and a set common evaluation criteria would ensure that all risks had the same level of definition, easing the ability of the board to compare them to past enterprise risks, and better understand the impacts and mitigation strategies. Without these templates and reference implementations, risks will continue to be defined at varying levels of detail depending on the risk owner, and as a result will

likely have potential mitigations or enterprise impacts missed just through lack of understanding of the scope of the risk.

b. Develop Common, Enterprise Engineering Models and Architecture Products

While this recommendation is not solely for the risk board to implement, as stated earlier this should be an activity that the risk board members should participate in directly. To take it further, this should be undertaken after the broadening of the risk board membership is implemented, as definition of enterprise models and architectures should be done not only with technical considerations, but with input from all aspects of system development.

To further integrate this with prior recommendations, the development of enterprise models should focus on first defining the enterprise in areas that leadership considers the most in need of the attention of the risk board. The enterprise artifacts could then be expanded in stages from this core set of focus areas until the entire enterprise architecture is defined.

This should be done not only for the enterprise as it is currently implemented, but also to provide an enterprise architecture for stages in the future, as decided by leadership, to aid in risk mitigation efforts. This future vision will help the risk board determine if a risk should be mitigated in the current enterprise architecture, or as a future extension of it.

c. Provide Mechanisms to Consider Risk Mitigations within Existing Enterprise or as Expansion of the Enterprise

As with earlier recommendations that were dependent on mutual implementation, this is likely the last recommendation that should be pursued. One of the items the risk board should consider when evaluating a risk is whether it is best addressed in the current enterprise scope, or if it should be addressed by new effort that changes or expands the enterprise. Again, this is best accomplished once the risk board membership is expanded beyond just the technical domain.

Also, this can only truly be considered once an overall enterprise architecture is defined and agreed upon, as that will provide the context for what functions are currently inside and outside the enterprise. Additionally, any efforts that would require new systems or acquisition efforts would benefit from there being a regular interaction with leadership to discuss those potential mitigations, as was recommended earlier in this chapter.

Finally, any recommendations to potentially add new systems or components to the enterprise should be considered in the context of the future enterprise architecture depictions. In the most synergistic of implementations, the evaluation of an enterprise risk that leads to an expansion of the enterprise, would also be evaluated by the group owning the enterprise architecture to result in a modification of their future state model.

C. LIMITATIONS OF ANALYSIS

Many of the evaluation criteria used for both the organizational alignment and enterprise risk management assessments were gathered from research in areas other than DOD. These guidelines were still effective in assessing the PEO C4I ETRB, but some standard aspects of military organizations, such as personnel rotations or documented concepts of operations were not considered. Those limitations are discussed further here.

a. Impacts of Rotational Nature of Military Organizations

The nature of military, or military/civilian hybrid, organizations is that personnel often change with regularity. Almost all military positions are inherently rotational and the same can be said for many civilian positions in military organizations. Therefore, any efforts to expand the membership of the ETRB, or implement enterprise architectures will be limited by any knowledge lost when key organizational members rotate out of the organization.

This can be mitigated somewhat by implementing things such as common definitions and common procedures, but even so there is a natural learning curve when new personnel come into an organization. While viewed as a limitation, it is equally possible that new personnel bring new ideas and approaches to enterprise risk

management that improve the risk board as a whole. It would be prudent to develop some level of intellectual knowledge consistency amongst members of the board to ensure continuity of approach even in the midst of personnel rotations.

b. Rationale for Organizing the ETRB around Technical Risks

The analysis in Chapters II through IV assumed that because the ETRB was the only enterprise risk board within PEO C4I, it would be advantageous to expand its focus to consider all enterprise risks. This was viewed as providing additional value to the PEO as not all risks are inherently technical.

Nonetheless, it is possible that the PEO derives benefits from limiting the enterprise risk board to include only technical risks evaluated only by engineering personnel. This seems unlikely, but should be a consideration when reviewing the analysis and recommendations throughout this thesis.

c. Lack of PEO C4I ETRB Standard Operating Procedures

Several of the recommendations include further defining a risk template to ensure a common level of detail is associated with all risk statements, impact statements, impact timelines and mitigation efforts. These are the sort of items that might be identified in a standard operating procedure (SOP) document. The ETRB Charter does reference an SOP, but through research with PEO C4I, this SOP was not able to be found and therefore was not referenced in this thesis. If the SOP does still exist and defines some of these criteria, those recommendations should be reviewed and revised accordingly.

D. CHAPTER SUMMARY

This chapter served as the primary analysis chapter of this thesis. It focused on two main sections, the first being a review of the assessments of the ETRB's alignment to key organizational principles to implement enterprise risk management, and the second regarding a review of the ETRB's level of adherence to core enterprise risk management principles.

There was a review of each of the five organizational alignment criteria, and an assessment as to whether the ETRB alignment to those criteria was strong, weak, or

neutral. This section also included a set of recommendations with an emphasis on how to improve alignment between the ETRB and the three weak and one neutral criterion.

There was then a review of the six enterprise risk management best practices and an assessment to the level of implementation each of these best practices saw within the ETRB. The level of implementation was assessed again as strong, weak or neutral. The section closed with a set of recommendations on how to best address the one weak and four neutral implementations.

Several of the recommendations between the two categories were inter-related, dependencies between improving the organizational alignment and implementing enterprise risk management best practices. This was not surprising as any best practice has to be implemented within the context of the organization it operates within.

Finally, there was a brief discussion on the limitations of implementing the provided recommendations. This includes the consideration of the rotational nature of personnel within military-aligned organizations as well as the potential that the specifically technical focus of the enterprise risk board had been implemented intentionally.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND FUTURE RESEARCH

This thesis provided a foundational review of key organizational alignment and enterprise risk management principles that were then utilized to provide an analysis on the efficacy of the PEO C4I ETRB. The ETRB was analyzed against both sets of principles. Strengths and weaknesses were identified with regard to the board's overall alignment to those principles. As a result of that analysis, several recommendations were made in regards to both organizational alignment and risk management best practices.

A. CONCLUSIONS

Chapter IV included an in-depth review of areas where the PEO C4I ETRB strongly or weakly aligned with the organizational and risk management evaluation criteria. As a result of the analysis that identified those strengths and weaknesses, several recommendations specific to PEO C4I improving organizational alignment or more specifically implementing enterprise risk management best practices were made. Those recommendations are summarized in Table 13.

Table 13. Summary of Organizational and Risk Management Alignment Recommendations

Review Area	Recommendation
Organizational Alignment	1. Assign risk management responsibilities to every employee 2. Expand membership of the ETRB 3. Request regular enterprise risk focus area inputs from leadership 4. Require regular ETR status updates to leadership 5. Define mechanisms and criteria for establishing multi-team risk ownership
Enterprise Risk Management	1. Define a common risk definition template 2. Develop common, enterprise engineering models and architecture products 3. Provide mechanisms to consider risk mitigations within existing enterprise or as expansion of the enterprise

The organization will have the discretion to implement these in a manner that best supports existing processes and personnel. PEO C4I will also have to make a decision on whether to implement all recommendations at once, or in full. Regardless of future implementation, the analysis methodology proved very effective and also allows for the potential to expand or restrict the criteria used as more research in the organizational alignment and enterprise risk management areas continues.

Criteria could be added, changed, or replaced over time, and increasingly tailored to a given organization's mission set. The evaluation process is consistent and repeatable, allowing for independent reviewers to provide bounded and implementable recommendations. Developing the analysis framework and the process for utilizing the framework was the goal of this thesis, and the use of the PEO C4I ETRB use case demonstrated the effectiveness of both the framework and evaluation process as well as the ability to leverage the framework to provide specific recommendations to improve overall enterprise risk management within the target organization.

B. POTENTIAL FUTURE RESEARCH

This research provides a foundation for organizational analysis, but there are many other areas that were not addressed, or could be studied in more depth. This includes not only additional research into the foundational criteria used to establish this evaluation framework, but also a study of examples where some of the recommendations from this thesis were implemented by organizations and how effective the recommendations proved to be in practice.

Given that one of the core precursors to enterprise risk management was having an enterprise definition or system-of-systems definition of potential risk areas, a potential future area of research could be effective methods of defining enterprise or systems-of-systems design and architecture products as well as a methodology for utilizing these system-of-systems architectures as a tool for identifying potential enterprise risks.

A study of the methods that organizations use to instill personal responsibility for various organizational functions would also be beneficial. In this area of study, it would reflect potential methods to enforce each employee having ownership of risk

management. This would include initial motivation, measuring progress, and evaluation of employee efficacy at performing risk management and mitigation tasks.

A foundational item for implementation of enterprise risk management was to define a common way of identifying, managing and mitigating risks. To enable this, there is a need to provide an enterprise risk management plan that describes how to conduct those activities so that all portions of an organization implement them in a common way. One mechanism to help with this common implementation is to provide an enterprise risk management tool or database where all risks can be stored and viewed by all stakeholders. Additional research on the key features of enterprise risk management tools, to provide the functionality to perform full enterprise risk management, would be valuable information for organizations looking to adjust their risk management approach.

Many of the organizational alignment concepts and associated evaluation criteria were based upon the unwritten premise that there was consistency in the workforce, such that continuous retraining was not necessary. This is often not the case in a military organization and was accordingly listed as a limitation of the evaluation framework. As a result of those military rotations, often civilian employees are placed in temporary positions while awaiting the military replacement. This has the potential trickle-down impact of removing key knowledge from another part of the organization supplying the temporary replacement. A further review of the impacts of personnel shifts, both in military and industry environments, on organizational risk management would be very worthy of future research. This could include research into personnel retention methods as well as knowledge retention for when employees leave an organization.

Finally, as many of the tenets of enterprise risk management assume enterprise leadership engagement in identifying and mitigating risks, more research into the amount of risk management training that executives receive would be valuable. Perhaps there should be a core set of training or other experience with risk management that leaders, especially within DOD, should take before assuming an enterprise management position. Research into effective enterprise risk management techniques and training associated with those techniques would be beneficial to have as a minimum standard.

APPENDIX. ENTERPRISE RISK MANAGEMENT EVALUATION MATRIX

Table 14. Organizational Alignment and Risk Management Evaluation Criteria

Evaluation Criteria	**Ideal Case**	**PEO C4I ETRB Comparison**	**Conclusion**
Organizational Alignment Criteria			
Employee's Responsibility / Accountability for Managing Risk (Liu 2011)			
Cross-Team Coordination for Purpose of Managing Risk (Hardy 2015)			
Allowance for Multiple Teams to Co-Own Risk Mitigation (Liu 2011)			
Enterprise-Level Definition of Risk Management Practices (Galliano 2011) and Risk Areas for Each Organizational Component (Roberts 1991)			
Evaluating Risk in Terms of Impact to Efforts Other Than Your Own (Liu 2011)			

Risk Management Best Practices			
Ability to Consider Short-Term and Long-Term Impacts to Risk (Tonello 2007)			
Evaluating a New Risk with Regard to its Impact on Existing Risks (Liu 2011)			
Risks Managed at the Most Detailed Level Possible (Liu 2011)			
Presence of Enterprise Engineering Models or Architectures to Provide Objective Context for Technical Risks (Brunson et al. 2009)			
Risks Evaluated with Context of System Position in Acquisition Life-Cycle (Stevens et al. 2009)			
Assessment of Ability to Mitigate Risk in Current Enterprise Architecture (Langford et al. 2008)			

LIST OF REFERENCES

Brunson, Karl, Jeffrey Beach, Thomas Mazzuchi, and Shahram Sarkani. 2009. "A Framework for Systems Engineering Development of Complex Systems." *Crosstalk* 22(5): 7–13.

Chairman of the Joint Chiefs of Staff. 2015. *Joint Capabilities Integration and Development System.* CJCS Instruction 3170.011. Washington, DC: Joint Chiefs of Staff, January 23. https://acc.dau.mil/adl/en-US/722172/file/80079/CJCS%20-%20Instruction%2c%20CJCSI%203170.01I%2c%20JCIDS%2c%2023%20Jan%202015%2c%20Errata%2c%20%2023%20May%202015.pdf.

Defense Acquisition University. 2007. *Defense Acquisition Structures and Capabilities Review*. Pursuant to National Defense Authorization Act for FY2006. Washington, DC: Defense Acquisition University. June.

Department of Defense. 2015. *Risk Management Guide for DOD Acquisition*. Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology and Logistics (OSD ATL). June.

Deputy Chief Management Officer. 2015. *DoD Organizational Structure*. Washington, DC: Department of Defense. September 2. http://dcmo.defense.gov/Portals/47/Documents/PDSD/201509_DoD_Organizational_Structure.pdf.

Dickinson, Gerry. 2001. "Enterprise Risk Management: Its Origins and Conceptual Foundation." *The Geneva Papers on Risk and Insurance* 26(3): 360–366.

Galliano, Carlos. 2011. "Implementation of an Enterprise Level Risk Management Process at the Naval Undersea Warfare Center Division, Newport." Presentation to the 14th Annual NDIA Systems Engineering Conference. October 27.

Hardy, Karen. 2015. *Enterprise Risk Management: A Guide for Government Professionals* (1). San Francisco: Jossey-Bass. ProQuest ebrary. Web. 30 May 2016.

Kerzner, Harold. 2013. *Project Management*. Hoboken, NJ: John Wiley and Sons.

Langford, Gary, Raymond Franck, Thomas Huynh, and Ira Lewis. 2008. "Gap Analysis: Rethinking the Conceptual foundations." Proceedings from the 5th Annual Research Symposium, Monterey, California, 14–15 May.

Liu, Xin. 2011. "A Holistic Perspective of Enterprise Risk Management." Doctoral dissertation, Washington State University.

Pomerleau, Mark. 2016. “To Keep Pace, Military Targets Rapid Prototyping and Faster Acquisition.” *Defense Systems*. June 16. https://defensesystems.com/articles/2016/06/16/dod-rapid-prototyping-acquisition-cyber.aspx

Program Executive Officer C4I. 2014. *PEO C4I Organizational Structure*. San Diego, CA: PEO C4I, August 28.

———. 2015. *Enterprise Technical Risk Board Charter*. San Diego, CA: PEO C4I, May 5.

Roberts, Nancy C. 1991. *Limitations of Strategic Management in Bureaus: The Case of the Department of Defense*. NPS-AS-91-008. Monterey, CA: Naval Postgraduate School.

Stevens, Renee G, Margaret King, and Marc Halley. 2009. “Acquisition Strategies for Dealing with Uncertainty.” Proceedings from the 6th Annual Research Symposium, Monterey, California, 13-14 May.

Tonello, Matteo. 2007. *Emerging Governance Practices In Enterprise Risk Management*. The Conference Board R-1398-07-WG. New York: The Conference Board.

Tse, Eric. 2016. “Risk Management on Enterprise Architecture and System Integration.” Project PERFECT White Paper Collection. Sydney, Australia. April 8.

Ulrich, Karl, and Steven Eppinger. 2012. *Product Design and Development*. New York: McGraw-Hill.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California