



NAVAL POSTGRADUATE SCHOOL

THESIS

**AN ANALYSIS OF MANAGEMENT TECHNIQUES AND THEIR
IMPACT ON THE MARINE CORPS IN A NAVY MARINE
CORPS INTRANET ENVIRONMENT**

by

Charles B. Buckley

June 2006

Thesis Advisor:
Second Reader:

Glenn Cook
Thomas Housel

Approved for public release; distribution is unlimited

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 June 2006	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: An Analysis of Management Techniques and Their Impact on the Marine Corps in a Navy Marine Corps Intranet Environment			5. FUNDING NUMBERS	
6. AUTHOR(S) Charles B. Buckley				
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)			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.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) The movement towards a Network Centric environment is changing the requirements for network management. The ability to quickly adapt to changing conditions is crucial to the success of joint forces; Information Technology systems are critical enablers of that flexibility. The challenge facing managers today is to provide robust, integrated, secure, and interoperable information systems and networks; a challenge that has never been more demanding than it is today. As the components of the DoD continue their transformation efforts, it is important to look to successful organizations for management techniques to aid in providing effective and efficient IT services. This thesis will explore current management trends such as outsourcing, the Information Technology Infrastructure Library (ITIL), Real Options, Business Process Reengineering (BPR), and Knowledge Value Added (KVA) to determine their possible impact on the manner in which the DoD manages their IT services.				
14. SUBJECT TERMS Navy Marine Corps Intranet, NMCI, Seat Management, Outsourcing, Knowledge Value Added, KVA, Return On Knowledge, ROK, Business Process Redesign, BPR, Knowledge Management, Information Technology Infrastructure Library, ITIL, Real Options, Marine Corps Enterprise Network, MCEN, U.S. Marine Corps, Enterprise Architecture			15. NUMBER OF PAGES 147	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

NSN 7540-01-280-5500

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**AN ANALYSIS OF MANAGEMENT TECHNIQUES AND THEIR IMPACT ON
THE MARINE CORPS IN A NAVY MARINE CORPS INTRANET
ENVIRONMENT**

Charles B. Buckley
Captain, United States Marine Corps
B.S., Athens State University, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
June 2006**

Author: Charles B. Buckley

Approved by: Glenn Cook
Thesis Advisor

Dr. Thomas Housel
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The movement towards a Network Centric environment is changing the requirements for network management. The ability to quickly adapt to changing conditions is crucial to the success of joint forces; Information Technology systems are critical enablers of that flexibility. The challenge facing managers today is to provide robust, integrated, secure, and interoperable information systems and networks; a challenge of that has never been more demanding than it is today. As the components of the DoD continue their transformation efforts, it is important to look to successful organizations for management techniques to aid in providing effective and efficient IT services. This thesis will explore current management trends such as outsourcing, the Information Technology Infrastructure Library (ITIL), Real Options, Business Process Reengineering (BPR), and Knowledge Value Added (KVA) to determine their possible impact on the manner in which the DoD manages their IT services.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PURPOSE.....	1
B.	BACKGROUND.....	1
C.	RESEARCH QUESTIONS.....	3
	1. Primary Research Question.....	3
	2. Secondary Research Questions.....	3
D.	SCOPE AND LIMITATIONS.....	3
E.	METHODOLOGY.....	4
F.	BENEFITS OF THIS RESEARCH.....	4
G.	ORGANIZATION OF THE THESIS.....	4
II.	FROM THE “AS-IS” ENVIRONMENT OF THE MARINE CORPS ENTERPRISE NETWORK TO THE “TO-BE”.....	7
A.	INTRODUCTION.....	7
B.	DEFINING THE ENTERPRISE.....	7
C.	THE ENTERPRISE ARCHITECTURE MANAGEMENT MATURITY FRAMEWORK.....	10
	1. Stages of Maturity.....	11
	<i>a. Stage 1: Creating Enterprise Architecture Awareness.....</i>	<i>11</i>
	<i>b. Stage 2: Building the Enterprise Architecture Management Foundation.....</i>	<i>11</i>
	<i>c. Stage 3: Developing the Enterprise Architecture.....</i>	<i>12</i>
	<i>d. Stage 4: Completing the Enterprise Architecture.....</i>	<i>12</i>
	<i>e. Stage 5: Leveraging the Enterprise Architecture to Manage Change.....</i>	<i>13</i>
	2. Critical Success Attributes.....	13
	3. Core Elements.....	14
D.	THE “AS-IS” USMC ENVIRONMENT.....	16
	1. Systems and Infrastructure.....	18
	2. Software Portfolio Management.....	19
	3. Data and Storage.....	19
	4. Manpower.....	20
	5. Asset and Lifecycle Management.....	21
E.	JUSTIFICATION FOR CHANGE.....	22
F.	COMPONENTS OF THE MCEN.....	24
	1. The Expeditionary Network.....	25
	2. Marine Corps Enterprise Information Technology Services.....	25
G.	THE WAY AHEAD.....	27
H.	CHAPTER SUMMARY.....	28
III.	THE NAVY MARINE CORPS INTRANET.....	29
A.	INTRODUCTION.....	29
B.	THE INCREASING RELIANCE ON OUTSOURCING.....	29

C.	BEST PRACTICES OF OUTSOURCING	30
1.	Executive Leadership.....	30
2.	Partner Alignment	31
3.	Relationship Management	31
D.	SEAT MANAGEMENT.....	31
E.	NAVY MARINE CORPS INTRANET.....	33
F.	EXPECTED BENEFITS OF SEAT MANAGEMENT CONTRACTS AND NMCI.....	36
1.	Technical Considerations	37
2.	Cost Considerations.....	38
G.	CHAPTER SUMMARY.....	41
IV.	THE INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY	43
A.	INTRODUCTION.....	43
B.	WHAT ARE INFORMATION TECHNOLOGY FRAMEWORKS AND WHY SHOULD THEY BE IMPLEMENTED?.....	43
C.	THE INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY FRAMEWORK	44
1.	What is IT Service Management?	45
2.	The Seven Modules of Information Technology Infrastructure Library	46
a.	Service Delivery.....	47
b.	Service Support	49
c.	Information Communication Technology Infrastructure Management (ICT IM)	50
d.	Planning to Implement Service Management	52
e.	Application Management.....	53
f.	The Business Perspective.....	54
g.	Security Management	55
3.	Benefits of Using the ITIL Framework.....	56
4.	Problems That May Arise When Implementing the Information Technology Infrastructure Library Principles.....	57
D.	HOW DOES THE INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY COMPARE TO OTHER MANAGEMENT FRAMEWORKS?	57
1.	The Control Objectives for Information and Related Technology (COBIT) Framework.....	58
2.	The Capability Maturity Model	58
3.	Six Sigma.....	60
4.	The Information Technology Investment Management Framework	61
E.	CHAPTER SUMMARY.....	62
V.	TRANSFORMATION AND BUSINESS PROCESS REENGINEERING.....	63
A.	INTRODUCTION.....	63
B.	DEPARTMENT OF DEFENSE TRANSFORMATION	63
1.	Business Enterprise Priorities.....	64

	a.	<i>Personnel Visibility</i>	65
	b.	<i>Acquisition Visibility</i>	65
	c.	<i>Materiel Visibility</i>	66
	d.	<i>Common Supplier Engagement</i>	66
	e.	<i>Real Property Accountability</i>	66
	f.	<i>Financial Visibility</i>	67
C.		DEPARTMENT OF THE NAVY AND MARINE CORPS BUSINESS TRANSFORMATION.....	67
D.		BUSINESS PROCESS REENGINEERING	68
	1.	What is Business Process Reengineering?	69
	2.	Information Technology and BPR	70
	3.	BPR Methodology	71
	a.	<i>Preparing for Reengineering</i>	72
	b.	<i>Identify and Analyze the As-Is Processes</i>	73
	c.	<i>Design the To-Be Process</i>	74
	d.	<i>Implementation and Continuous Improvement</i>	74
E.		KNOWLEDGE VALUE ADDED	75
	1.	Knowledge Value Added Theory	75
	2.	How KVA Works	76
F.		ANALYSIS OF THE USMC MORNING REPORT SUBMISSION PROCESS	77
	1.	The As-Is Submission Process	77
	2.	Knowledge Value Added Calculations	79
	3.	Analysis of Results	80
	4.	The Role of Information Technology in the Process	81
	5.	The To-Be Process	82
	6.	KVA Comparison	83
G.		CHAPTER SUMMARY	84
VI.		THE REAL OPTIONS APPROACH TO INFORMATION TECHNOLOGY VALUATION	85
A.		INTRODUCTION	85
B.		OPTIONS THEORY	85
	1.	Definition of Options	85
	2.	Real Options	87
C.		OPTIONS VALUATION TOOLS	88
	1.	The Binomial Model	88
	2.	The Black-Scholes Model	89
D.		TYPES OF REAL OPTIONS	91
	1.	Real Options “On” Projects	91
	2.	Real Options in Projects	93
E.		APPLYING REAL OPTIONS TO INFORMATION TECHNOLOGY INVESTMENTS	93
F.		CONCLUSION	95
VII.		CASE STUDY OF MARINE CORPS AIR STATION, YUMA ARIZONA	97
A.		INTRODUCTION	97

B.	MARINE CORPS AIR STATION YUMA, ARIZONA.....	97
C.	PRE-NMCI ENVIRONMENT	97
1.	IT Infrastructure.....	98
a.	Desktop Computing Environment.....	98
b.	Server Environment.....	99
c.	Base Area Network Infrastructure.....	99
d.	Peripheral Items and Supplies.....	100
2.	IT Support Practices.....	100
3.	Pre-NMCI Financial Analysis.....	102
a.	Distributed Computing.....	103
b.	Wide Area Data Transport.....	104
c.	Cable Plant.....	104
d.	Mandated Requirements.....	104
4.	Pre-NMCI Annual Per-Seat Cost.....	105
D.	POST-NMCI ENVIRONMENT.....	105
1.	The NMCI IT Infrastructure.....	105
2.	NMCI Cost Elements.....	106
3.	MCAS Yuma Site Specific Cost Elements.....	107
4.	Cost Summary	108
E.	PRE-NMCI AND POST-NMCI COST COMPARISON.....	108
F.	CHAPTER SUMMARY.....	109
VIII.	CONCLUSIONS AND RECOMMENDATIONS.....	111
A.	INTRODUCTION.....	111
B.	RESEARCH QUESTIONS.....	111
1.	Creation of the Marine Corps Enterprise Network.....	111
2.	The Information Technology Infrastructure Library	113
3.	Outsourcing Best Practices	114
4.	Business Process Reengineering	115
5.	Real Options Analysis.....	115
C.	RECOMMENDATIONS.....	116
1.	Involve NMCI Personnel in Business Process Reengineering Projects.....	116
2.	Develop Standard Information Technology Infrastructure Library Practices to be Used Throughout the Marine Corps Enterprise Network	116
3.	Investigate the Use of Real Options as a Method of Evaluating Strategic Investments in Information Technology Projects.....	116
	LIST OF REFERENCES.....	117
	BIBLIOGRAPHY	121
	INITIAL DISTRIBUTION LIST	129

LIST OF FIGURES

Figure 1.	EAMMF Matrix (GAO, April 2003)	11
Figure 2.	EAMMF matrix with the five maturity stages identified in bold (GAO, April 2003).....	13
Figure 3.	EAMMF matrix with critical success attributes added (GAO, April 2003)	14
Figure 4.	Summary of EAMMF (GAO, April 2003)	15
Figure 5.	USMC IT Strategic Framework (USMC, February 2004)	24
Figure 6.	Functional Architecture Overview (USMC, March 2005)	25
Figure 7.	Conceptual view of the relationship between Supporting Establishment IT services (USMC, January 2006)	27
Figure 8.	Relationship between NMCI and the MCEN (USMC, 2003)	34
Figure 9.	Comparison of seat costs (NMCI, 2002)	40
Figure 10.	The ITIL framework (IT Service Management Forum, July 2004).....	47
Figure 11.	The ITIL security management process (IT Service Management Forum, July 2004).....	56
Figure 12.	ITIM Framework (GAO, 2004)	61
Figure 13.	Assumptions of KVA (Housel and Kanevsky 1995).....	75
Figure 14.	Three Approaches to KVA (Housel and Bell, 2001).....	76
Figure 15.	As-Is Morning Report Submission Process	78
Figure 16.	As-Is KVA Analysis	81
Figure 17.	To-Be Morning Report Submission Process.....	82
Figure 18.	To-Be KVA Analysis.....	84
Figure 19.	Option Payout (Gaynor and Bradner, 2001)	86
Figure 20.	Types of real options (Devaraj and Rajiv 2002).....	88
Figure 21.	The Binomial Model (Mauboussin 1999).....	89
Figure 22.	Black-Scholes formula (Smit and Trigeorgis, 2004)	89
Figure 23.	Framework of Real Options On Projects (Wang 2005).....	92
Figure 24.	MCAS Yuma IT Department Organizational Structure	100

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Popular BPR Methodologies.....	72
Table 2.	Comparison of Real Options On and In Projects.....	91
Table 3.	MCAS Yuma Desktop Computing Environment	98
Table 4.	MCAS Yuma Server Environment	99
Table 5.	Comparison of Pre-NMCI and Post-NMCI Costs	109

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

The author would like to convey sincere appreciation to Mr. Glenn Cook and Dr. Thomas Housel for their professional guidance and assistance throughout the thesis process.

The author would also like to thank his family for being incredibly patient and supportive during the last twelve years.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE

This thesis explores the impact of the Navy Marine Corps Intranet (NMCI) on the management of Marine Corps computer networks. The research provides a history of Marine Corps network management and shows how network management methodology has changed under the NMCI contract and how leveraging the NMCI provided environment can assist the Marine Corps in transforming into a more efficient and effective, fully interoperable fighting force. This work evaluates NMCI as a tool that enables business process reengineering, a critical component of force transformation. As part of this research, the Information Technology Infrastructure Library (ITIL) management framework will be explored as a means of managing the NMCI environment. This thesis also evaluates Real Options Analysis as a method of capturing the costs and benefits associated with IT projects.

B. BACKGROUND

The drive to transform the warfighting capabilities of the Department of Defense (DoD), as well as the business processes that control, support, and sustain it, are by-products of the effects of globalization on the international security order and the transition from the industrial age to the information age. Transformation, however, is more than just acquiring new equipment and embracing new technology. It is the process that shapes the changing nature of military cooperation through new combinations of concepts, capabilities, people, and organizations that exploit our nation's advantages and protect against our vulnerabilities. Transformation of the DoD is a vital component of U.S. defense strategy; successful implementation of the Department's force transformation strategy will accelerate the ongoing shift from an industrial age to an information age military. The keys to operating in the information age are: new rules, new behaviors, new competencies and new relationships. Investing in the transformation strategy is the first step towards achieving a network-centric force that will conduct information age military operations. The realization of the DoD's vision for a joint, network-centric force capable of conducting military operations in accordance with the

principles of this emerging way of war will depend on a significant improvement in the volume and quality of information available to commanders, staffs, units, and individuals at all levels. In order to develop increasingly capable forces, the DoD must leverage information technology (IT) products and services. A critical IT element is the networking infrastructure.

In support of DoD transformation efforts, the Department of the Navy has developed the Sea Power 21 concept. Sea Power 21 focuses on three fundamental concepts – Sea Strike, Sea Shield, and Sea Basing, which are linked by FORCEnet, an envisioned architecture of sensors, networks, decision aids, weapons, and supporting systems. The FORCEnet functional concept defines FORCEnet as the “operational construct and architectural framework for naval warfare in the information age”, or more simply, FORCEnet refers to the systems and processes required to provide fully networked naval command and control. FORCEnet capabilities support network-centric warfare through the use of communications and data networks; the common operational and tactical picture; and intelligence, surveillance, and reconnaissance concepts, systems, and programs. FORCEnet is the future implementation of Network Centric Warfare in the Naval Services. One of the major programs developed in support of FORCEnet is the Navy Marine Corps Intranet (NMCI). NMCI supports the underlying premise of FORCEnet; the network effect, which causes the value of a product or service in a network to exponentially increase as the number of those using it increases.

NMCI is a department-wide, multiyear IT services contract that will replace independent networks, applications, and other hardware and software with one secure network. Awarded in 2000, Electronic Data Systems (EDS), the prime contractor for NMCI, the NMCI contract is expected to provide service for approximately 400,000 Navy and Marine Corps personnel located at more than 300 bases throughout the US and overseas. The contract, valued between \$9 and \$13 billion, was initially awarded as a five-year base contract covering fiscal years 2001 through 2005. After implementation was delayed, the contract was extended to cover through Oct 2007, with a one year option remaining. This was done to allow the Navy and Marine Corps a few years of operating within the NMCI environment to achieve the increased warfighting

effectiveness and enhanced business goals envisioned at the start of NMCI. This modification was sought by both the Navy and EDS, with the approval of Congress. The NMCI environment is expected to enhance system and software interoperability, leading to enhanced information exchange capability for garrisoned and deployed forces as well as individual users. Commonly referred to as “seat management”, NMCI involves transitioning a number of distinct workstations or “seats” to a contractor who then takes responsibility for operating and maintaining the workstations, including applications and supporting infrastructure.

C. RESEARCH QUESTIONS

1. Primary Research Question

How does NMCI facilitate the creation of the Marine Corps Enterprise Network?

2. Secondary Research Questions

- How should the principles of the Information Technology Infrastructure Library (ITIL) management framework be implemented within the MCEN?
- What outsourcing best practices did the Navy and Marine Corps use when preparing to outsource network services?
- How can the NMCI platform enable the Marine Corps to improve business processes?
- Could Real Options Analysis provide useful insight to the value of IT projects?

D. SCOPE AND LIMITATIONS

The scope of this thesis includes an in-depth analysis of the NMCI contract from a network management perspective. This analysis will discuss network management of Marine Corps assets in the pre-NMCI environment as well as the post-NMCI environment. This analyzes the effects of implementing NMCI on the Marine Corps methodology of network management. As part of this thesis, a case study of network management at the Marine Corps Air Station Yuma, Arizona will be conducted. This case study will outline and compare the pre-NMCI environment and the post-NMCI environment. This analysis is from a business perspective. Therefore, any technical analyses of NMCI are beyond the scope of this thesis.

E. METHODOLOGY

The research for this thesis consisted of several steps. First, a comprehensive review of Marine Corps orders, policies, and other documents related to network management procedures was conducted. Second, an in-dept content analysis was conducted of the NMCI contract, as well as other NMCI related documents to identify the programs management methodology. Interviews with both government and NMCI personnel were also completed during this time. Third, an investigation into the decision to pursue NMCI was conducted; this consisted of a review of business case analyses, re-organization proposals, and contract options. Fourth, a comprehensive literature review of books, articles, General Accounting Office (GAO) reports, and other library resources was conducted. Fifth, investigation of best practices and current network management techniques was accomplished through web research and interviews. As a result of these steps, the researcher was able to evaluate the history of Marine Corps network management, how the NMCI framework has solidified network management, and the effects that NMCI could have on the Marine Corps business practices.

F. BENEFITS OF THIS RESEARCH

This thesis analyzes the history of Marine Corps network management and what changes have been brought on by the implementation of the NMCI contract and if the Information Technology Infrastructure Library could improve the Marine Corps Enterprise Network, to include NMCI. Research is conducted to determine if Real Options Analysis could be a useful tool to discover the value of IT projects. The ability of NMCI to provide a platform that enables business process redesign is also evaluated. This thesis is available to the Marine Corps NMCI program management office as well as other organizations seeking to outsource network services designed around a seat management contracting approach.

G. ORGANIZATION OF THE THESIS

Chapter II provides a history of Marine Corps management of network services. Chapter III gives a detailed analysis of the NMCI contract and the effect its implementation has on the network management methodology. Chapter IV will present the Information Technology Infrastructure Library as a management framework that is quickly becoming a best practice. Chapter V investigates the benefits that NMCI

provides when re-engineering business practices. Chapter VI investigates the use of Real Options Analysis to quantify the strategic value of IT projects. Chapter VII is a case study involving the Marine Corps Air Station, Yuma, Arizona. This chapter compares the pre-NMCI environment and the post-NMCI environment from a management perspective. Chapter VIII contains research conclusions and answers to the research questions.

THIS PAGE INTENTIONALLY LEFT BLANK

II. FROM THE “AS-IS” ENVIRONMENT OF THE MARINE CORPS ENTERPRISE NETWORK TO THE “TO-BE”

A. INTRODUCTION

This chapter discusses the theory of enterprise architecture (EA) and how the Marine Corps defines their enterprise, both prior to the implementation of the Navy Marine Corps Intranet (NMCI) as well as recent efforts to re-define the enterprise that includes the NMCI environment. Included in this chapter is a discussion of key legislative and other requirements that guide the Marine Corps implementation of (1) IT strategic planning and performance measurement and (2) investment management, to involve selecting, controlling, and evaluating investments.

B. DEFINING THE ENTERPRISE

Enterprise Architecture can be defined as a strategic information asset base, which defines the mission, the information necessary to perform the mission, and the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to the changing mission needs. (GAO, April 2003) An EA normally includes a baseline architecture (the as-is environment), target architecture (the to-be environment), and a sequencing plan which describes the transition from the baseline to the target architecture. (CIO Council, February 2001) Effective use of EAs is recognized as a best-practice of today’s most successful public and private organizations. The goal of an EA is to create an IT architecture that can help map agencies business processes with its IT systems. Successful definition and implementation of EAs are crucial to creating operational structures that are optimally defined, in both business and technological environments. EAs can assist an organization in creating improved operational processes that are standardized, provide business continuity, and provide information conformity throughout the organization. (Computer Associates International, June 2004) This in turn, enables agencies to free up funds for more value-added, mission critical activities. The alternative to an EA, and the main reason for the emergence of them, is an operational environment in which there is a lack of integration among business operations and supporting IT resources which may lead to

organizational inefficiency and duplication of efforts. In short, an enterprise can be defined as any purposeful activity, and architecture can be defined as the structure of that activity.

The concept of architecture to describe an enterprise first emerged in the mid-1980's, when John Zachman identified the need to use a logical blueprint (i.e., an enterprise) to define and control the integration of systems and their components. (Zachman, 1987) Zachman developed a structure or "framework" to assist in defining and capturing the architecture. Throughout his work, he drew parallels to the field of classical architecture, in which different work products (e.g., architect plans, shop plans, and bills of lading) represent different views of the planned building. EAs do much the same thing, they provide an explicit, common, and meaningful frame of reference that enables a structural understanding of: (1) what the enterprise does, (2) when, where, why, how, and who in the agency does what, and (3) what the agency uses to accomplish its goals. The EA is a framework for communication, interpretation, and implementation of agency objectives, with the purpose of enabling the evolution of a strong IT-business alignment.

Since the late 1980's when Zachman introduced his framework, several government agencies have proposed a number of similar frameworks. These frameworks were developed in response to the rapid growth in the number of disconnected or "stove-piped" information systems that have been implemented in virtually every federal agency over the past few decades. This could be the result of a miscommunication between IT technicians and top management officials within the various agencies, or it may also be attributed to the individual agencies desires to have and control their own support systems. These disconnects between IT capability and business leads to degraded capabilities. EA initiatives provide answers to critical questions regarding IT-business alignment and how IT can support business goals. For EAs to be useful and provide business value, their development, maintenance, and implementation should be managed effectively.

Beginning in 1989, the National Institute of Standards and Technology published its first architecture guidance: *Information Management Directions: The Integration*

Challenge. This was followed by the U.S. General Accounting Office issuing their architecture guidance: *Strategic Information Planning: Framework for Designing and Developing System Architectures* in 1992. The GAO's research focused on successful public and private sector organizations' IT management practices and identified the use of architectures as a critical factor to these organizations' success. Since then, other federal agencies have issued their own frameworks that define the content of EAs, including the Department of Defense. The emergence of newer federal frameworks and guidance over the past few years is largely owing to Congress passing the Clinger-Cohen Act in 1996. (U.S. Code, 1996) This act requires Chief Information Officers for government agencies and departments to develop, maintain, and facilitate the implementation of architectures as a means of integrating business processes and agency goals with IT. The need for greater federal agency awareness and use of EAs was further recognized in the E-Government Act of 2002, (Public Law, 2002) which established the Office of Management and Budgets Office of Electronic Government with the responsibility of overseeing the development of EAs across federal agencies. Collectively, these documents and guides provide a recommended model for effective EA management.

While these post-Zachman frameworks and guidance differ in their naming conventions and modeling approaches, they consistently provide for defining an enterprise's operations in both (1) logical terms, such as interrelated business processes and business rules, information needs and flows, and work locations and users, and (2) technical terms, such as hardware, software, data, communications, and security attributes and performance standards. The newer frameworks also provide for defining these perspectives both for the enterprise's current or "as-is" environment and for the target or "to-be" environment. Also included is a transition plan for moving from the "as-is" to the "to-be" environment. One of the most followed frameworks is the General Accounting Office's *Framework for Assessing and Improving Enterprise Architecture Management* which was first published in 2002 and updated in 2003. (GAO April 2003, GAO-03-584G)

C. THE ENTERPRISE ARCHITECTURE MANAGEMENT MATURITY FRAMEWORK

The GAO defined Enterprise Architecture Management Maturity Framework (EAMMF) consists of three basic and interrelated components: (1) hierarchical stages of management maturity, (2) categories of attributes that are critical to success in managing endeavors, and (3) elements of EA management. (GAO, April 2003) The EAMMF was developed to provide agencies with a standard that provides meaningful measures that an agency can use to assess progress toward a desired end state and to take corrective action to address deviations, should any arise. Successful implementation of the EAMMF also enables agencies to base IT investment decisions on an explicit and common understanding of both today's operating environment and tomorrow's goals.

The EAMMF is similar to the IT Service Capability Maturity Model (CMM), which is a maturity growth model aimed at IT service providers. The IT Service CMM captures the maturity with which IT services are provided in five maturity levels. The IT Service CMM can be used by both IT service providers and customers of IT services. The IT Service CMM is similar in nature to the software CMM, which describes the maturity of software development and maintenance organizations. The software CMM provided a generic structure that could be reused to develop the IT Service CMM.

The EAMMF also defines five maturity stages, each of which is associated with four critical success attributes, each of which represent a category or type of management practice. Also identified are 31 core elements, or descriptions of a practice or condition that is required for effective EA management. Each element is associated with one of the five hierarchical maturity stages. Figure 1 below is a representation of the EAMMF matrix. Each attribute represents a category or type of management practice and core element that is needed to effectively discharge any function. One difference between the EAMMF matrix and a classical matrix is that each maturity stage not only includes the core elements defined for that stage, but also the core elements from previous maturity stages. For example, maturity stage 3 will contain its own core elements as well as the core elements of maturity stages 1 and 2. Once an agency recognizes which maturity

level they are operating at, managers can then use the framework to determine the steps required to improve their architecture management.

	maturity stage 1	maturity stage 2	maturity stage 3	maturity stage 4	maturity stage 5
critical success attribute 1		core elements (2)	core elements (1)	core elements (1)	core elements (1)
critical success attribute 2		core elements (3)	core elements (1)	core elements (1)	core elements (2)
critical success attribute 3		core elements (3)	core elements (3)	core elements (5)	core elements (3)
critical success attribute 4		core elements (1)	core elements (1)	core elements (1)	core elements (2)

maturation 

Figure 1. EAMMF Matrix (GAO, April 2003)

1. Stages of Maturity

The EAMMF is made up of five stages of increasing EA maturity, with each following stage including all elements of the prior stages.

a. *Stage 1: Creating Enterprise Architecture Awareness*

As the Figure above shows, the first maturity stage is Creating EA awareness. Stage 1 agencies are in one of two situations. Either (1) they do not have plans to develop and implement an EA, or (2) they have plans that do not demonstrate an awareness of the value of having and using an architecture. Agencies operating at stage 1 may have initiated some EA activities, however, their efforts are largely ad-hoc, unstructured, lack institutional leadership, and do not provide the foundation necessary for successful EA development.

b. *Stage 2: Building the Enterprise Architecture Management Foundation*

At Stage 2, Building the EA management foundation, agencies recognize that EAs are a corporate asset and create an executive body that is accountable to and represents the entire enterprise. EA management roles, such as a chief architect, and responsibilities are assigned and plans are established for developing EA products and for measuring program progress and quality. An EA steering committee has been established for the purpose of governance. Members of the steering committee should

include both business and IT representatives to ensure enterprise-wide representation. A Stage 2 agency either has plans for developing or has begun developing some EA products, and has developed an awareness of the value of EA and its intended use in management of IT investments. A framework has been selected along with a methodology that will form the basis for developing EA products, as well as a tool for automating management related activities.

c. Stage 3: Developing the Enterprise Architecture

Stage 3 is focused on further refining and developing architecture products according to the framework, methodology, tools and management plans that were selected and implemented in stage 2. The roles and responsibilities assigned in the previous stage are still in place, and resources are being applied to develop actual EA products. One of the major components of stage 3 is to identify the scope of the architecture as related to the entire enterprise, independent of how the enterprise is defined (i.e., organization-based or function-based). While products may not be complete at this time, they are intended to describe the organization in business, performance, information or data, service or application, and technology terms. This is all done in relation to the direction provided by the steps taken to achieve proficiency in stage 2. In addition to earlier work, the products begin to describe the current or “as-is” and future or “to-be” environments and provide a plan for transitioning from the “as-is” to the “to-be” environment. The agency is now tracking and measuring progress against the established EA management foundation. This enables the agency to measure progress against plans, identify and address shortcomings, and report on progress.

d. Stage 4: Completing the Enterprise Architecture

For an agency to be considered as having reached stage 4, several things must have happened. The steering committee, as established in Stage 2, must have approved EA products. This can also be accomplished through the use of an IT investment review board. The completed products should describe the enterprise in terms of business, performance, information and data, service and application, and technology for both its “as-is” and “to-be” operating environments. The products must also include a transition plan. This is the same as the requirement for stage 3; however, stage 4 takes it a step further. To be considered as having reached stage 4, an independent agent must

assess the quality (i.e., completeness and accuracy) of the EA products. Stage 4 also requires that a written maintenance policy govern the evolution of approved products. This policy is normally written by the head of the agency for which it applies.

e. Stage 5: Leveraging the Enterprise Architecture to Manage Change

Stage 5 is the pinnacle of EA maturity. At this level, senior leadership has approved of the EA products and has written and approved an institutional policy stating that IT investments must comply with the agencies architecture, unless an explicit compliance waiver is granted. Agency decision makers must use the architecture to identify and address ongoing and proposed IT investments that may conflict, overlap, are not strategically linked, or are redundant. Stage 5 agencies are able to avoid unwarranted overlap across investments and ensure that the procured systems will be interoperable with one another. This process ensures that the selection and funding of IT investments with manageable risks and returns. The agency tracks and measures EA benefits, or return on investment, and adjustments are continuously made to both management processes and EA products.

The figure below is a representation of the EAMMF matrix, including the five maturity stages.

	Stage 1: Creating EA awareness	Stage 2: Building the EA management foundation	Stage 3: Developing EA products	Stage 4: Completing EA products	Stage 5: Leveraging the EA to manage change
critical success attribute 1		core elements (2)	core elements (1)	core elements (1)	core elements (1)
critical success attribute 2		core elements (3)	core elements (1)	core elements (1)	core elements (2)
critical success attribute 3		core elements (3)	core elements (3)	core elements (5)	core elements (3)
critical success attribute 4		core elements (1)	core elements (1)	core elements (1)	core elements (2)

Figure 2. EAMMF matrix with the five maturity stages identified in bold (GAO, April 2003)

2. Critical Success Attributes

The critical success attributes, each of which is associated with each maturity stage, are essential to the successful performance of any enterprise management function. The critical success attributes are defined as follows:

- Showing a commitment to perform the function;
- Putting in place the capability (i.e., people, processes, and technology) needed to perform the function;
- Demonstrating, via production and results, that the function has been performed; and
- Verifying, via quantitative and qualitative measurement, that the function was satisfactorily performed.

Taken together, these attributes form a basis for agencies to institutionalize management of any given function or program, such as EA management. Figure 3 is a representation of the EAMMF matrix with the critical success attributes included.

	Stage 1: Creating EA awareness	Stage 2: Building the EA management foundation	Stage 3: Developing EA products	Stage 4: Completing EA products	Stage 5: Leveraging the EA to manage change
Attribute 1: Demonstrates commitment		core elements (2)	core elements (1)	core elements (1)	core elements (1)
Attribute 2: Provides capability to meet commitment		core elements (3)	core elements (1)	core elements (1)	core elements (2)
Attribute 3: Demonstrates satisfaction of commitment		core elements (3)	core elements (3)	core elements (5)	core elements (3)
Attribute 4: Verifies satisfaction of commitment		core elements (1)	core elements (1)	core elements (1)	core elements (2)

Figure 3. EAMMF matrix with critical success attributes added (GAO, April 2003)

3. Core Elements

EA management elements (i.e., practices and conditions) form the core of the EAMMF. The core elements identified in the framework originate in the CIO Council's *Practical Guide*. Different core elements exist for each maturity stage, with the assumption being that organizations at a specific stage have completed and incorporated the core elements from the previous stage. The Figure below shows all the core elements and relates them to the applicable stages of maturity and critical success attributes.

Figure 4 below is a summary of the EAMMF. It is important to remember that each stage includes all elements of previous stages.

	Stage 5: Leveraging the EA to manage change				
	Stage 4: Completing EA products				
	Stage 3: Developing EA products				
	Stage 2: Building the EA management foundation				
	Stage 1: Creating EA awareness				
Attribute 1: Demonstrates commitment		Adequate resources exist. Committee or group representing the enterprise is responsible for directing, overseeing, or approving EA.	Written and approved organization policy exists for EA development.	Written and approved organization policy exists for EA maintenance.	Written and approved organization policy exists for IT investment compliance with EA.
Attribute 2: Provides capability to meet commitment		Program office responsible for EA development and maintenance exists. Chief architect exists. EA is being developed using a framework, methodology, and automated tool.	EA products are under configuration management.	EA products and management processes undergo independent verification and validation.	Process exists to formally manage EA change. EA is integral component of IT investment management process.
Attribute 3: Demonstrates satisfaction of commitment		EA plans call for describing both the "as-is" and the "to- be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as-is" to the "to-be." EA plans call for describing both the "as-is" and the "to- be" environments in terms of business, performance, information/data, application/service, and technology. EA plans call for business, performance, information/data, application/service, and technology descriptions to address security.	EA products describe or will describe both the "as- is" and the "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as- is" to the "to-be." Both the "as-is" and the "to-be" environments are described or will be described in terms of business, performance, information/data, application/service, and technology. Business, performance, information/data, application/service, and technology descriptions address or will address security.	EA products describe both the "as-is" and the "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as- is" to the "to-be." Both the "as-is" and the "to-be" environments are described in terms of business, performance, information/data, application/service, and technology. Business, performance, information/data, application/service, and technology descriptions address security. Organization CIO has approved current version of EA. Committee or group representing the enterprise or the investment review board has approved current version of EA.	EA products are periodically updated. IT investments comply with EA. Organization head has approved current version of EA.
Attribute 4: Verifies satisfaction of commitment		EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment.	Progress against EA plans is measured and reported.	Quality of EA products is measured and reported.	Return on EA investment is measured and reported. Compliance with EA is measured and reported.

maturation

maturation →

Figure 4. Summary of EAMMF (GAO, April 2003)

The importance of developing, implementing, and maintaining an EA is a basic tenet of both organizational transformation and successful IT management. When properly managed, EAs can clarify and help optimize the interdependencies and relationships among business operations and the underlying IT infrastructure and applications that support these operations. EAs, when employed together with other management controls, can greatly increase the chances that organizations' operational and IT environments will be configured to optimize mission performance. Public and private sector experience has shown that IT management, without defining an architecture often results in systems that are duplicative in nature, are not well integrated with existing systems, and are expensive to maintain.

D. THE "AS-IS" USMC ENVIRONMENT

The existing IT infrastructure capabilities within the Marine Corps were developed and implemented prior to the development of the Network Centric Operations concept and its required technical capabilities. From the beginning, this environment grew into an infrastructure with multiple standards, a variety of ad-hoc hardware packages, reliance on proprietary software and tools, gaps in network planning, and sub-optimal IT operations planning and staffing. (USMC, March 2005) Locally developed, funded and hastily installed client-server solutions created stove-pipe repositories of data that are not easily accessed for use in enterprise analysis or decision making. While it is easy to focus on a lack of funding as a reason for the current environment, there are several other reasons that should be considered.

IT services in the Marine Corps have been operated in a decentralized manner using an informally developed management hierarchy consisting of four echelons; system sponsors, regional representatives, local/base management organizations, and information system coordinators. Each echelon has specific roles and responsibilities that help organize coordination and helps to institutionalize IT support practices by ensuring network support is consistent across all commands, regardless of location. The four echelons of support are:

- The first echelon is the Information System Coordinator (ISC), who works under the authority of local commanders to provide first echelon support. The ISC is appointed by the commander to serve as the local area network

administrator to provide users day-to-day operational IT support. Technical problems beyond the scope of the ISC's capabilities are referred to the second echelon of support.

- The Local Area Network (LAN) manager is the second echelon of support. The LAN manager is normally located within the communications department or IT divisions at major subordinate commands and bases and stations. The LAN manager is responsible for all LANs operating within the various subordinate command organizations and functional areas of the command. Specifically, the LAN manager is tasked with providing technical support and guidance to ISCs that fall under the operational control of the LAN, regardless of location (i.e., garrison, embarked, deployed, combat, or outlying bases/stations). As with the first echelon, technical problems beyond the scope of the LAN managers' capabilities should be referred to the next echelon of support for resolution.
- The third echelon is the base or station network control center (BNCC or SNCC), which provides third echelon network support to the LAN managers of the various tenant commands that are within the physical confines of a Marine Corps base or air station. The BNCC/SNCC is in possession of the NIPRNET and SIPRNET access point to the DISN. Each BNCC/SNCC manager provides site specific support to all tenant commands, as well as commands that are temporarily located aboard the installation for exercises.
- The fourth and final echelon is the USMC NOC, located in Quantico, Va. The USMC NOC serves as the DISA designated service Local Control Center (LCC) and as such, serves as the system sponsor for all elements of the Marine Corps Enterprise Network Infrastructure. The USMC NOC serves as the support element for all problems that can not be resolved by third echelon managers as well as all units that are not served by a third echelon organization. Problems that are beyond the scope of the USMC NOC are referred to the DOD, DISA, or commercial vendors that are responsible for the product being used. The USMC NOC, in order to ensure secure, end-to-end connectivity, centrally manages and controls the network architecture down to, and including the point of presence (POP) that is located at each third echelon organization. Configuration changes by third echelon organizations to hardware such as POP routers, firewalls, intrusion detection devices, and screening routers that are managed by the USMC NOC is not allowed. If changes are required, a request must be submitted to the USMC NOC by the third echelon organization.

The USMC NOC provided guidance in the form of administrative messages that attempted to standardize some of the management aspects for the MCEN.

In 2000, the Marine Corps published MARADMIN 263/00 for the purpose of replacing a series of messages and advisories with a centralized reference. The message limited the purchasing of software products by listing approved and recommended products. Also identified in this message was a waiver process through which non-approved software could be submitted and considered for approval. The purchase of hardware products was governed by the MARCORSYSCOM produced Buyers Guide. MARADMIN 264/00 expanded the guidance of 263/00 related to the acquisition and leasing of hardware. This MARADMIN established MARCORSYSCOM as the point of contact for procurement and refreshment of all desktops, laptops, and servers. Hardware procurement was now centrally managed as local commands were no longer authorized to acquire hardware using operational funds. However, although these messages were released with good intentions, the results were not as expected.

1. Systems and Infrastructure

Marine Corps information systems have evolved over the past 20-30 years to meet specific requirements, usually within a single functional area (i.e., supply, facilities maintenance). This decentralized approach has led to a multitude of systems, applications, and data that satisfy a relatively narrow community of interest. These systems were not designed to be interoperable with other, similar systems leading to an infrastructure that has competing technical standards and vendor-proprietary components. In some cases, systems were built by local commands, using available resources, which are typically inadequate to develop, operate, and maintain throughout the full lifecycle. Often, as personnel and corporate knowledge changed location, the systems that they built fell to the side and a new system was put into place.

In most cases, lack of knowledgeable personnel was the least of many problems. One of the biggest problems with the home-grown systems and applications was the inadequate resources to properly develop, operate, and maintain the systems through its full lifecycle. Since the communications training school focused on technical capabilities, most personnel filling the role of IT managers have never had any formal project management training. This led to problems from the start of most locally developed projects. The result was hundreds of stove-piped, single purpose systems that

lacked the basic maintenance needed to keep them operating, including hardware and software refreshment. This environment eventually led to high failure rates of these systems, with some failures never being resolved and the system being “shelved” and a new, locally grown system put in its place.

2. Software Portfolio Management

An enterprise approach to IT portfolio management is currently being developed; however, it has not reached maturity. For now, the Marine Corps utilizes the Functional Area Managers process as identified in MARADMIN 226/04 to manage its current IT portfolio management efforts. The FAMs are tasked with eliminating redundant and/or obsolete applications that reside within their organization. Due to a lack of visibility and control of current applications, as well as a lack of resources to perform the necessary tasks associated with this effort, the FAMs are becoming very frustrated with the process. (USMC, May 2004).

As with local systems and infrastructure, software acquisition has been mostly a local effort; FAMs have held little influence over software acquisition. Adding to the lack of FAM influence could be the guidance of MARADMIN 263/00. For example, while the USMC FAM for fire services declared that only one type of software would be used for reporting and historical record keeping; an investigation revealed that there were five different reporting systems in use across the Marine Corps. As the Marine Corps transitions to NMCI, more and more of these type of situations are coming to light.

3. Data and Storage

MARADMIN 123/99, *IT Advisory 99-01, USMC Data Management Program*, established early guidance and assigned roles and responsibilities, and established a plan of action and milestones for implementation of the Marine Corps data management program. Included in the message was guidance for standards, modeling, integration, storage, retrieval, and protection of data. The focus of this message was on acquisition of information systems and did not provide guidance for local file servers and networked storage requirements.

The Marine Corps owns many data centers at all levels. The third echelon, or base and station network control centers, have tried to keep pace with the demands for

network storage space as best they could. Most BNCC/SNCCs have multiple servers that are made into file storage as needed. A result of this assortment of servers, applications, and vendors is greater complexity and increasing IT management costs, due to the increased training and manpower required for operation and maintenance. Many of the servers are underutilized for various reasons, including that the network infrastructure is not reliable enough to be trusted at all times. As part of a study conducted by SANZ, Inc (USMC, March 2005), it was discovered that across 19 sites throughout the Marine Corps, average storage utilization is 25%, far below the industry average of 65% or more. System backups are not done often enough and hardware failures occur all too frequently for the users to feel comfortable enough to leave critical files on a networked server. At one installation, due to a lack of manpower and efficient equipment, backups were performed once a month, while outages occurred between two and three times a month which is far below the industry goal of 99.999% reliability. (Zittle 2006) Most users continue to keep critical files in isolated databases that are unavailable to users on other systems. In the end, ad hoc data center growth has resulted in facilities that are full of incompatible hardware and applications that could be eliminated or consolidated if a more efficient system was available.

4. Manpower

One of the greatest concerns to the Marine Corps is providing the right mix of people, processes, data, and technology to deliver IT services. NCW is only possible when the qualified and properly trained people are teamed with state of the art technology to provide crucial information at the proper time.

Many garrison billets have been transitioned from military personnel to government civilian employees. This move has helped to provide continuity of operations as Marines either change duty stations or exit the Marine Corps, taking their knowledge with them. Having civilians provides some corporate knowledge of locally grown systems; however, most civilians are at a higher level than their Marine counterparts (i.e., GS-11 vs. LCPL). One of the drawbacks to this is that the civilians tend to operate at a higher level, not necessarily hands-on. Sample civilian T/O billets include, Information Systems Security Officer, Network Coordinator, and Deputy

Director. This leaves the junior Marines to troubleshoot network problems, repair computers, and maintain applications. Even if the civilians know about the application or systems, the knowledge is usually not there to maintain it after the Marine departs. One of the key decisions the Marine Corps has made in recent years was to outsource system development, and eliminate the Military Occupational Specialty (MOS) 4067, Computer Programmer. With no organic programming expertise, it has become difficult to find qualified personnel to maintain the locally grown systems and applications. Further compounding the problems faced by IT departments is the lack of qualified web designers.

The Internet is the fastest way of passing information to both the general public, as well as internal to an organization. Company and Squadron level intranets are exploding in use and capabilities, from signing up for required training to daily muster. As such, most units request web capabilities that are far beyond the capabilities of a basically trained Marine communicator. Most commands send a Marine to outside training to gain the education necessary to provide counsel and development to those organizations requesting web services. This however; is not without problems. First is the cost of training, which is fairly high, as well as the cost of maintaining proficiency in new technologies. Second, the Marine comes away from the training with a basic understanding of web technologies and how to perform basic programming. Some of the tasks that are requested are far beyond those the Marine possesses, which requires the department to outsource the capability, usually increasing the amount of systems and software the command is now responsible for. As with locally grown applications, the web designer will eventually depart, requiring training for a replacement and time to assume the duties of the previous Marine.

5. Asset and Lifecycle Management

Having decentralized execution, even with centralized guidance has led to asset and lifecycle management problems for the Marine Corps. (USMC, March 2005) Recent data calls have identified that there is no accurate accountability of hardware, software, databases, and infrastructure components in use throughout the Marine Corps. Not knowing what equipment and applications reside on a network results in an increased

cost for IT services. Local commands have found that they were supporting multiple operating systems, thousands of applications, and a multitude of equipment brands. All of this leads to higher operating costs, including a lack of oversight on service warranties. This lack of visibility makes it hard, if not impossible to implement the new systems and hardware required by NCW.

The following is an excerpt from MARADMIN 568/03, dated 12/09/2003 and summarizes the above points:

Formerly, legacy applications developed to satisfy specific business or operational objectives included procurement of independent and diverse hardware as well as accompanying databases and were hosted in a variety of locations. As a result, we have a proliferation of application servers and databases throughout the Marine Corps that are excessively expensive to purchase, deploy, manage, and maintain. Industry benchmarking and limited USMC surveys have indicated that only a small fraction of this infrastructure capacity is used, leaving critical resources idle.

Additionally, the numbers of trained and skilled personnel available to support our current infrastructure continues to dwindle while user expectation and system sophistication increases.

E. JUSTIFICATION FOR CHANGE

The Marine Corps faces significant IT related challenges during the transition to Network Centric Warfare. Speed and data will be key catalysts for both the business as well as the warfighting domains. NCW demands a new approach to managing IT services and resources that requires a realignment of IT programs and assets to take advantage of advances in architectures and technology. The existing, “as-is” Marine Corps IT infrastructure was not designed with a NCW environment in mind; in fact, it is not possible to implement NCW with the current architecture. In order to prepare the Marine Corps IT infrastructure for the implementation of NCW, an Enterprise Architecture has to be defined and implemented.

Enterprise Architecture initiatives help to create improved operational processes, a key building block of NCW. Looking at other EA benefits, it is easy to see how difficult it would be to implement NCW without first defining the enterprise. Some of the benefits of EA include:

- Process discovery and alignment
- Management of requirements and business rules
- Standardization
- Information conformity throughout the organization
- Business continuity
- Impact, gap, and risk analysis
- Business process management
- A common repository

In order to be successful, the Marine Corps has to identify; (1) What the enterprise does, (2) When, where, how, why, and who in the organization does what, and (3) What the enterprise uses to accomplish its goals. The Marine Corps Enterprise Network (MCEN) is a global network that supports all data requirements for Marine forces and the supporting establishment.

The MCEN is the Marine Corps contribution to FORCEnet and the Global Information Grid (GIG) and provides an enterprise framework for the provision of IT products and service throughout the Marine Corps. The MCEN is the Marine Corps end-to-end solution for information exchange between the operational forces and the supporting establishment, spanning both warfighting and business domains. As a part of FORCEnet, the MCEN connects the garrison, maritime, and expeditionary infrastructures, it is the union of information assets. Critical components of the MCEN are: NMCI in the garrison environment; the expeditionary network (eXNET) for deployed forces; and the Marine Corps Information Technology Services (MCEITS), which is a critical initiative for supporting net-centric transformation. Figure 5 shows the Marine Corps strategic framework for IT.

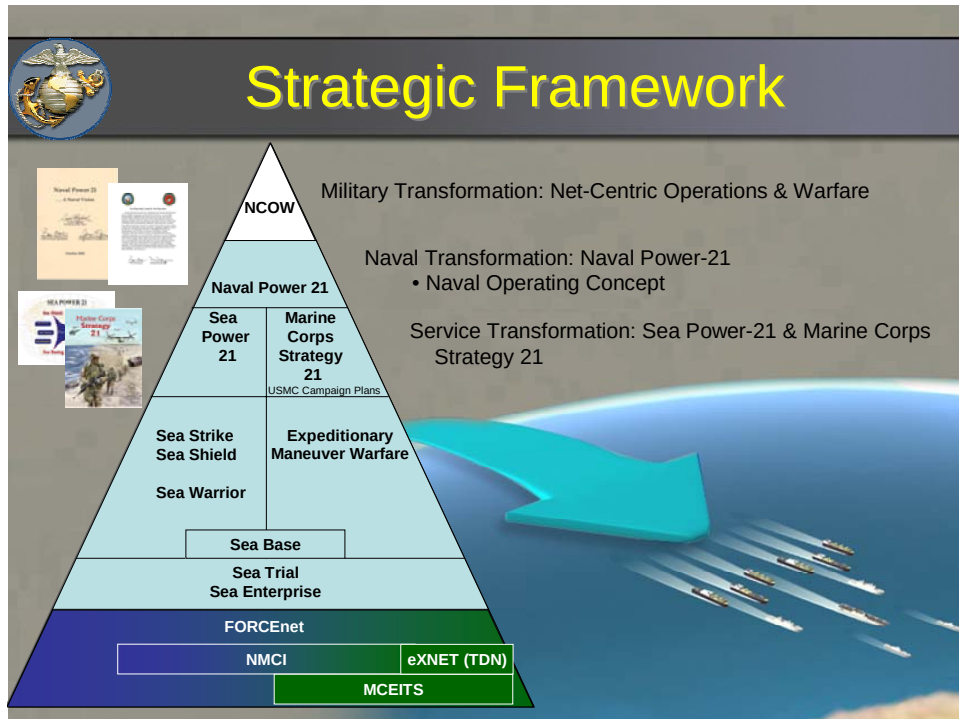


Figure 5. USMC IT Strategic Framework (USMC, February 2004)

F. COMPONENTS OF THE MCEN

The MCEN is a global enterprise network of integrated systems, personnel, and training programs designed to ensure effective information exchange for all Marine Forces worldwide. The MCEN is composed of NMCI, which will be discussed in the next chapter; the eXNET, which is the tactical component; and the MCEITS, which will provide a fundamental shift in the way the Marine Corps provisions IT services. Figure 6 is a representation of the Marine Corps functional IT architecture.

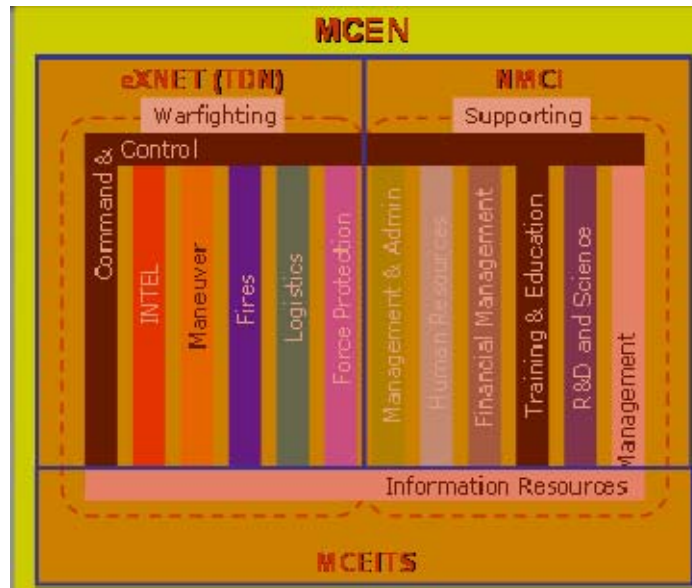


Figure 6. Functional Architecture Overview (USMC, March 2005)

1. The Expeditionary Network

The eXNET is the Marine Corps expeditionary network and is part of the MCEN. It requires improvements to the existing Marine Air Ground Task Force (MAGTF) Tactical Data Network (TDN), to ensure interoperability with the Army's Future Combat System/Warrior Information Network-Tactical (FCS/WIN-T), as well as the Air Force's future C4 systems. These improvements will support agile command and control through the use of current and future technologies such as adaptive, flexible, responsive, self-networking/self-healing networking capabilities that will be based on secure, web-enabled, mobile, ad hoc, and wireless technologies.

eXNET will also incorporate new satellite systems such as the Transformational Communication System (TCS) and the Mobile User Objective System (MUOS) to provide joint capabilities that are essential to tomorrow's net-centric capable deployed forces. The TCS and MUOS services will replace the current SATCOM capabilities and, along with the Joint Tactical Radio System (JTRS), will provide the backbone of eXNET.

2. Marine Corps Enterprise Information Technology Services

The purpose of the MCEITS is to provide a common framework, reusable software components, and to establish data interoperability by capitalizing on the availability and power of modern IT tools and business methods. It is a broad vision that

is composed of programmatic components as well as policies, strategies, and processes. As a framework, it must describe the operational, technical, and systems architectures that are required to transform business and warfighting mission areas both in garrison and in the deployed environment. It is important to remember that the MCEITS is not a conventional information technology system, it is an integrated suite of information capabilities designed to align IT resources to improve user access to relevant information. This will provide the Marine Corps with a set of consistent, integrated, centrally funded and managed components of the next generation IT systems that are required by NCW.

The MCEITS framework consists of:

- A family of centrally managed and funded services
- User services for application hosting, data centers, and network management
- Reusable application modules supporting DoD's GIG Enterprise Services for common and sophisticated functions like knowledge discovery, metadata queries, and messaging
- Regional IT centers for centralized management of core services with skilled operations staffs
- Data management services for an Enterprise Shared Data Environment (ESDE) (USMC, March 2005).

One of the requirements the Marine Corps has set for MCEITS is that it must allow for a fundamental shift in how networks and systems are planned and implemented. The current inventory of isolated system implementations need to be moved to a controlled, net-centric environment, where all data and information are exposed and available to all authorized users. These users are put into groups called Communities of Interest (COIs) that are formed around functional information and data sets. The use of COIs will allow authoritative data and common data conventions to emerge, which improves the overall quality of data. Figure 7 is a representation of the relationship between the MCEITS and other MCEN components in the supporting establishment.



Supporting Establishment 2010

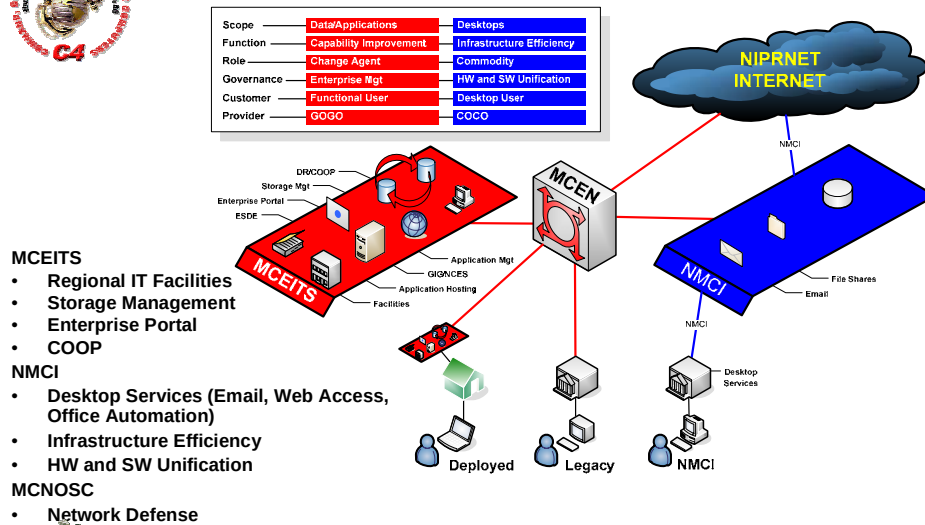


Figure 7. Conceptual view of the relationship between Supporting Establishment IT services (USMC, January 2006)

G. THE WAY AHEAD

The USMC has established five strategic goals for the C4 community in order to accomplish the mission. The goals will allow the Marine Corps to develop the MCEN and the capabilities associated with it to enable the Marine Corps to provide a robust, reliable, usable, and secure network that is capable of NCW operations. Each goal has a number of objectives associated with it.

The goals and objectives are:

- Goal 1: Build the Network
 - Develop future USMC IT infrastructure
 - Develop the MCEN
 - Expand the USMC Expeditionary C4 capabilities
 - Acquire integrated systems
 - Provide C4 guidance for C2 platform development
 - Implement a USMC IT capital planning process
 - Develop IT policies and standards
 - Establish governance over the network

- Goal 2: Man the Network
 - Enhance the health of the C4 occupational fields
 - Ensure that C4 training and education satisfy Marine Corps mission requirements
- Goal 3: Populate the Network
 - Develop Marine Corps Enterprise IT Services
 - Web-enable the Marine Corps
 - Create a Shared Data Environment
 - Leverage innovation
 - Conduct network operations
- Goal 4: Protect the Network
 - Provide Computer Network Defense (CND)
 - Provide Computer Emergency Response
- Goal 5: Exploit the Network
 - Enable MAGTF, joint, naval, and multinational network operations
 - Provide strategic agility, allowing rapid transition from a pre-crisis state to full operational capability in a distant theater
 - Provide operational reach, allowing the projection and sustainment of relevant and effective power across the depth of the battle space
 - Employ an agile supporting establishment. (USMC 2004).

These goals are aligned with current Defense Planning Guidance. Goal two was added by the Marine Corps to emphasize the importance of the Marine to the network. Each goal has a number of strategic objectives associated with it. These objectives are designed to provide a roadmap to success. Once these goals are reached, the MCEN will provide revolutionary capabilities throughout the Marine Corps.

H. CHAPTER SUMMARY

This chapter discussed Enterprise Architecture and explored one framework for assisting in development and measuring success. In addition, the chapter also discussed the Marine Corps current IT architecture and the requirement for change that is necessitated by NCW. The chapter concluded with a discussion of the proposed Enterprise Architecture that will enable the Marine Corps to transition to a NCW environment.

III. THE NAVY MARINE CORPS INTRANET

A. INTRODUCTION

This chapter will discuss the Navy Marine Corps Intranet (NMCI) contract and how NMCI relates to the Marine Corps Enterprise Network. This chapter will have a discussion of what outsourcing is and best practices for success. Included in this chapter will be a discussion of what seat management is, why it was chosen, and the benefits of a seat management approach.

B. THE INCREASING RELIANCE ON OUTSOURCING

Outsourcing of IT services, which involves the activities associated with acquiring services from one or more external providers, has become increasingly popular in both the private and public sector. During outsourcing, a client organization will transfer responsibility for one or more IT services to one or more external partners. Outsourcing is normally done for several reasons, including: to reduce and/or control costs, make up for a lack of internal skills, to offload a function that is too difficult to manage internally, and the organization lacks the core competency to perform the necessary tasks. Outsourcing offers the opportunity to leverage new technologies and industry innovation to better achieve the mission of the organization. While some organizations are searching for cost savings by outsourcing, one of the most obvious benefits of outsourcing is quality. Organizations that turn to outsourcing for services that they can not reliably provide see an increase in IT performance and service quality, fewer outages, increased reliability of equipment, and better disaster preparedness are examples of increased quality that can be gained by outsourcing IT services. In many organizations, particularly those that practice decentralized management, IT costs are distributed across the organization, making it difficult to discover the true cost of IT service provision. These organizations do not maintain much oversight about what services are being procured and the total cost to the organization. Many IT related costs are found hidden in other accounting lines and are not recognized as IT costs.

The last ten years has seen a vast increase in the number of outsourcing projects. A 2005 outsourcing study by Diamond Cluster has identified that 74% of the current

buyers of outsourcing services expect to increase their use of IT outsourcing in the coming year, compared to 64% in 2004. (Diamond Cluster, 2005) During that same time, satisfaction with IT outsourcing has slightly risen from 74% in 2004 to 78% in 2005. When providers of outsourcing services were asked for their thoughts, they were less optimistic than in the past. Overall, 81% of providers expect organizations to spend more on IT outsourcing than they have in the past, however, this is a decrease from 90% in 2004.

Although outsourcing continues to increase, more and more organizations are becoming less satisfied with the services they are receiving. Even though overall satisfaction has increased of late, so has dissatisfaction. In 2004, 10% of survey participants stated they were dissatisfied with their outsourcing projects, in 2005 that number has increased to 15%. One important statistic was the number of abnormal terminations of outsourcing relationships. In 2004, 21% of organizations had reported terminating an outsourcing project, in 2005 that percentage has more than doubled to 51%. Service providers also report an increase in abnormal terminations. The most cited reasons for terminating a project were: poor provider performance (36%), a change in strategic direction (16%), the function was moved in-house (11%), and the projected cost savings were not achieved (7%). (Diamond Cluster, 2005)

C. BEST PRACTICES OF OUTSOURCING

Successful outsourcing projects rely on ensuring that best practices are identified and followed. By not using best practices during outsourcing projects, the complexity and difficulty is greatly increased, raising the chances that the project will not succeed. Projects sometimes fail even though best practices are used. There are many different ideas on what constitutes a best practice, however, some are readily identifiable.

1. Executive Leadership

Support of the executive leadership is essential to obtaining and maintaining organizational support for IT outsourcing and should be obtained before eliciting organizational support. As with any project an organization undertakes, no matter how big or small, executive leadership support can either cause the project to succeed or fail. Communication begins with top-level executives and flows downward through the

organization. It is essential that this communication continue throughout the course of the project. Executive support makes all phases of a project easier by providing the ability to keep the entire organization informed throughout the project. Even if the executives are not the personnel directly communicating to the organization, a program management office or communications team that has the support of senior executives will have a much smoother path and meet with much less resistance than a program management office without that support.

2. Partner Alignment

Aligning client and provider objectives in a partnership is essential to building consensus and is imperative to establishing early trust among all stakeholders. A partnership between the client and the vendor can only occur when the two entities are able to mesh their goals. The success depends on mutual benefit. In order to achieve this, the vendors must be flexible and willing to adapt to their clients' changing business conditions. The client must be willing to bend their expectations and behaviors to allow the vendor to perform optimally. The recipe for success lies not in contract negotiations, but in day-to-day interaction throughout the life of the contract.

Despite the potential for mutual benefit, these types of projects are also risky. According to a recent survey, approximately 50% of projects that utilize partnerships were successful. It is important to remember that both sides must work together to establish common project goals beyond the objectives stated in the request for proposals.

3. Relationship Management

Relationship management focuses on strengthening the interaction between the client and provider at the operational level and is crucial to achieving the expectations of the outsourcing arrangement. Relationship management goes beyond the structure of the contract. Having the service provider establish an on-site support team to serve as a liaison between the client and provider is essential to ensure good relations. This support team should be involved in all aspects of the project, from start to finish and beyond.

D. SEAT MANAGEMENT

Seat management, sometimes referred to as “desktop outsourcing”, has been defined in many ways due to the flexibility that seat management provides to the

customer. The most common definition is that a seat management contractor will provide desktop computing as a unified service which encompasses the day-to-day operational control and support of the desktop and its associated network infrastructure. Seat management does not include relinquishing the right of the organization to create policy, it is not a program that is intended to usurp the managers policy making function. Seat management is a customer selected set of desktop and networking functions that may include contractor provided computers and network hardware, desktop and network software, the management of the hardware and software assets, help desk, training, and the maintenance of the hardware and software. According to the General Services Administration (GSA), the goal of seat management is to mirror commercial managed life cycle support of the desktop, adapted for the Federal Government. Seat management has the potential to provide the government with a better capability to control the technology cycle and better manage the desktop environment.

When an organization buys its desktop computing services through a seat management contract, the pricing is computed on a per user (or per seat) basis and the contractor becomes responsible for delivery of all hardware, software, network support, help desk services, planning/design, and maintenance/installation services. The details of seat management contracts will vary, as the details and requirements are contract specific. Seat management is more than leasing and should not be considered as such. In a seat management contract, the service provider owns all the hardware and delivers the resultant computing capability and all service support.

There are benefits to an organization not owning their own desktop computers, associated hardware, software, and network equipment. The pace of technology changes so rapidly that by the time a specific technology has been accessed, acquired, deployed, and implemented through the normal acquisition cycle, the technology may no longer be current. For example, seat management contracts can be written with the with basic service level agreements (SLAs) that may provide for a baseline of computing power or software versions. For example, a contract may be written that states that a desktop computer will provide at least 75% of the capabilities of a current high-end,

commercially available system (i.e., if the current high-end processor speed is 3.8 GHz, a desktop provided under a seat management contract must be at least 2.85 GHz).

Seat management first appeared in the Federal Government during the 1990s, as the rate of technology improvement exceeded the capability of most organizations to manage their current services. Two examples were the Outsourcing Desktop Initiative for NASA (ODIN) and the GSAs Seat Management Services contract. Seat management contracts have routinely been used in the private sector. The largest seat management contract in both the private and public sector to date is the Navy Marine Corps Intranet (NMCI).

E. NAVY MARINE CORPS INTRANET

NMCI offers the opportunity for the Department of the Navy (DON) to leverage new technologies and industry innovation to better achieve the global mission. It is designed to build the modern Navy and Marine Corps on the transformational power of networking, enabling a connection to the National infrastructure, extend sharing and creation of knowledge and expertise, empower innovative work and training, and enhance the quality of life for every Marine, Sailor, and DON civilian. (NMCI, April 2002).

The NMCI contract was awarded in October 2000 as a multi-year performance based indefinite deliver /indefinite quantity (IDIQ) contract. The original contract called for a five-year base period, covering fiscal years 2001 through 2005 with a maximum value of \$4.1 billion. A three-year option period covering fiscal years 2006 through 2008, with a value of \$2.8 billion, followed the five-year base period. At the time, the contract had a total value, if the option period was exercised, of \$6.9 billion. The contract was amended, to allow for delays, to expire in fiscal year 2007, with a new value of \$6 billion. A three year option still exists, but will cover the fiscal years 2008 through 2010, with the same \$2.8 billion value. Total contract value, if the option is exercised, is now almost \$9 billion. (NMCI, April 2006).

NMCI has a mission of providing IT services to over 400,000 sailors, Marines, and civilian employees that are employed at over 300 bases and stations, located both in the U.S. and overseas. As part of the MCEN, as shown in Figure 7, NMCI provides IT

services to and between elements of the supporting establishment. The Marine Corps has approved a fiscal year 2006 NMCI budget of almost \$340M that will cover the cost of NMCI for all commands except MARFORNORTH, which will provide local funds for FY06. This will provide approximately 87,500 NMCI seats and associated services such as peripherals, Blackberries, and all network devices and support. (USMC, November 2005). The \$340M amount above does not account for locally funded additions to the HQMC provided NMCI funding. Marine Forces Pacific (MARFORPAC) for example, has a little over \$215M provided by Headquarters Marine Corps (HQMC) to be distributed throughout its subordinate commands for NMCI services. Throughout MARFORPAC, there are orders for additional, unfunded NMCI services totaling over \$1.4M that uses local funding. There is also a funding deficiency of approximately \$14.4M that is identified for an additional 3,787 unclassified NMCI seats and 346 classified NMCI seats that are considered essential to mission completion. (USMC, February 2006).

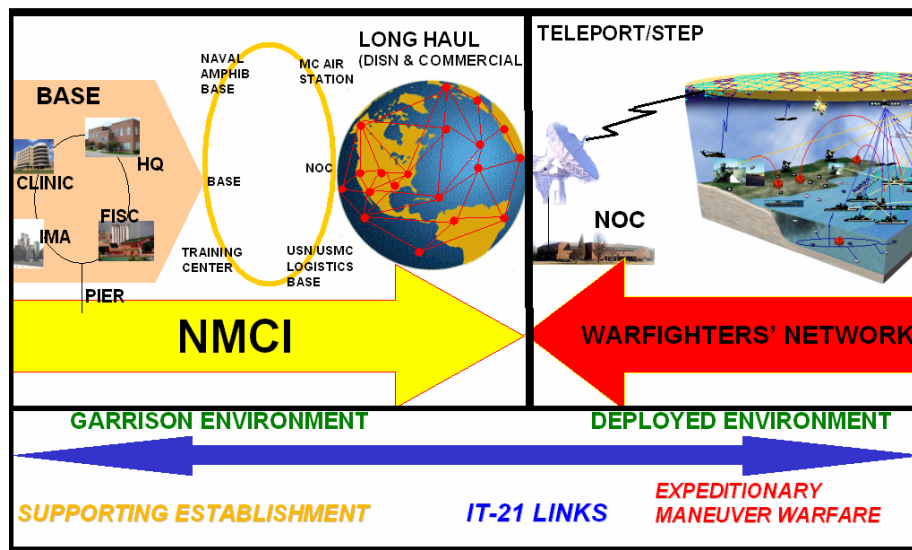


Figure 8. Relationship between NMCI and the MCEN (USMC, 2003)

NMCI is expected to standardize IT services across the DON, providing:

- Enterprise configuration management
 - Inventory of all software and hardware on the network

- Asset control and visibility
- Increased bandwidth
 - On demand surge service
- Internet access
 - Adequate / consistent bandwidth at all DON sites
- Capacity planning
 - Ability to consolidate and coordinate changes to the infrastructure
 - Enterprise-wide integration of new technologies
- Increased security
 - PKI
 - Consistent enterprise security
 - Certification and compliance of all legacy applications on the network
 - Consistent security testing and measurement
- Portal development and support, increasing enterprise programs and knowledge management
- Records management consistent with DoD standards
- Single directory service
- Tested and measured enterprise-wide interoperability (USMC, April 2002).

It is widely accepted that provision of IT services should be governed by service level agreements (SLAs) and NMCI is no exception. SLAs are essential to define the parameters of service, for the benefit of both the provider and the recipient. The purpose of SLAs is to set the expectations between the consumer and provider, helping to define the relationship between the two parties. A good SLA addresses several key aspects:

- What the provider is promising
- How the provider will deliver on those promises
- Who will measure delivery and how
- What happens if the provider fails to deliver as promised
- How the SLA will change over time

When the initial contract was signed in 2000, SLAs were established that EDS had to meet in order to receive payments and bonuses in accordance with the incentive

laden contract. The SLAs were established to measure factors such as customer satisfaction, application response time, help desk availability, and WAN performance. All SLAs were designed to give Navy and Marine Corps officials an accurate picture of the project's problem areas.

F. EXPECTED BENEFITS OF SEAT MANAGEMENT CONTRACTS AND NMCI

In July 1998, the Association for Federal Information Resources Management (AFFIRM) conducted a survey related to seat management contracts and management expectations. This survey was distributed to senior information technology and finance community officials and managers within Federal departments, agencies, and other Federal entities. There were five major reasons why an agency would consider the services of Seat Management, they are:

- Free staff to focus on core mission (41%)
- Improve service delivery (41%)
- Eliminate daily management headaches related to managing networks and desktop computers (39%)
- Reduce per seat costs (cost savings) (32%)
- Make it easier to implement the latest desktop software (32%) (AFFIRM, July 1998)

As the results show, most people who consider seat management do not think that outsourcing is simply about saving money, in fact, most gains with outsourcing of IT services have been in quality improvement.

NMCI is designed to solve a number of problems with the way the Marine Corps has been provisioning IT services. In the current environment, it is difficult, if not impossible to determine the actual annual IT costs and achieve consistency throughout the Marine Corps. The lack of an integrated, enterprise-wide approach to IT has resulted in duplicative services, uneven compliance with security standards, and a lack of configuration management. Additionally, prior to NMCI, it had been difficult to implement enterprise software applications, which is a key strategic goal of the Marine

Corps. As the results of the AFFIRM survey showed, the reasons for contracting IT services through a seat management contract appear to be evenly split between cost savings and technical issues.

1. Technical Considerations

One may think that lower costs is the sole benefit of using a seat management approach, however, quality improvement is where the most gains are seen when outsourcing IT services. With proper structuring of the requirements and of the contract itself, commercial expertise and best practices can be leveraged to result in better response time, increased system availability, reduced downtime, etc. Could an enterprise-wide management structure be implemented without outsourcing through a seat management contract, of course, but the main reason for outsourcing is that an organization alone can not do what is needed. Saving money is not the primary driver of the NMCI project, providing an enterprise-wide management structure is.

Once fully implemented, the NMCI contract will have consolidated over 300 Navy and Marine Corps bases and their associated networks into a single, enterprise-wide managed service. While the Navy and Marine Corps has laid the foundation for an enterprise network, the means of fully realizing the enterprise network were not within the grasp of the services. The only answer was to outsource network services. The benefits expected from the enterprise-wide approach include improved interoperability and access, more visibility into the actual cost of IT services, and others.

NMCI provides a common operating environment across the Marine Corps, which increases the ability of personnel working within the environment to collaborate using common sets of software. When the Navy and Marine Corps began preparing for NMCI, the estimate of the number of software applications in use was around 5,000. In reality, over 100,000 different software applications were in use, many of these were homegrown and served redundant purposes. (Onley, 2005) Most detrimental to operations was that almost none of the applications had the ability to be used across an enterprise. While streamlining the number of applications in use will create cost savings from lowering licensing costs, the bigger gain will be seen in the interoperability gained from standardizing applications across the enterprise.

Periodic refreshment of technology is another benefit of seat management contracting. Historically, this has been a problem for the Marine Corps, where technology refreshment usually takes a back seat to operations and maintenance of equipment. In the current state of decentralized management, it is difficult for local commands to keep pace with the advances in technology. In a 2000, MARADMIN, it was directed that all procurement and refreshment of all desktops, laptops, and servers would be centrally managed by MARCORSYSCOM. (USMC, May 2004) Local commands were no longer authorized to use O&MMC funds to procure systems. The NMCI contract contains technology refreshment requirements that provide for annual updates for software, or to maintain one revision from the current version while hardware is due to be updated every three years. A service level agreement incorporated into the contract requires that seats meet a percentage of the current “state of the shelf” when they are installed. NMCI considers technology refresh to be the replacement or addition of components with components of comparable functionality and technology offering expected or predictable cost or performance improvements. (NMCI, April 2006)

2. Cost Considerations

For most organizations, it is difficult to fully capture any possible cost savings that can be achieved through use of a seat management contract. NMCI is designed to solve the problem of accurately accounting for IT services by adapting commercial best practices for the acquisition of IT for government use. In June of 2000, a business case analysis was conducted to demonstrate whether the NMCI strategy was a sound business decision, when compared to the way that IT requirements were being met in the current environment. The June 2000 NMCI BCA documented:

- The scope of DON IT infrastructure that would be supplanted by NMCI
- The As-Is Cost and Performance Baseline
- Cost and Performance Estimates of the To-Be (NMCI RFP) environment
- An assessment of current and projected commercial and Defense Information Network (DISN) WAN transport costs and performance
- Performance and service level benefits that correlated to the Service Level Agreements (SLAs) specified in the NMCI RFP

During this BCA, twenty-one Navy sites and four USMC installations were used as data collection sites to obtain an enterprise Pre-NMCI (As-Is) inventory, cost, and service level data. The overall findings of the June 2000 NMCI BCA analysis were:

- A weighted average of the Navy and Marine Corps annual As-Is (Pre-NMCI) per seat cost of \$3,817, including distributed computing (\$3,621) and wide area networking (\$196). The annual per seat costs were projected to rise in the To-Be (NMCI) environment up to \$5,162 (\$FY00). This included \$4,814 for distributed computing, and \$153 for wide area networking. Additionally, two other costs would be incurred in NMCI, a Tier 1 DISN surcharge of \$111 and Government Management costs of \$84 per seat. This increase in direct costs of \$1,136 annually (or nearly 26%) was to be offset by indirect cost savings from improvements in productivity resulting from the improved IT infrastructure. Projected quantifiable benefits included a 58% reduction in indirect costs associated with improved service levels and productivity improvements.
- The anticipated annual Return On Investment (ROI) was between 7-13%, depending on the achieved level of indirect cost savings.

The June 2000 NMCI BCA concluded that there was a sound business case for NMCI, supported by evidence including quantitative and qualitative measures of costs and benefits, ROI, performance and service levels, risk, feasibility, core mission support, and mission performance. The aggregate risk and uncertainty of continuing with the current IT environment was greater than the risks associated with the deployment of a common commercial enterprise with integrated public key Public Key Infrastructure (PKI), Information Assurance (IA) and security infrastructure.

In 2002, as directed by Congress and the Office of Management and Budget (OMB), another BCA was conducted to validate the results of the earlier BCA by looking at a snapshot of the actual costs and performance of the Pre-NMCI and NMCI computing environments at seven of the first sites to migrate to the NMCI environment. The results of the updated BCA show that the Pre-NMCI average seat cost is \$3,545, which is \$262 lower than the June 2000 BCA estimate, and the average NMCI seat cost of \$4,179 is \$983 less than before, as shown in Figure 9 below.

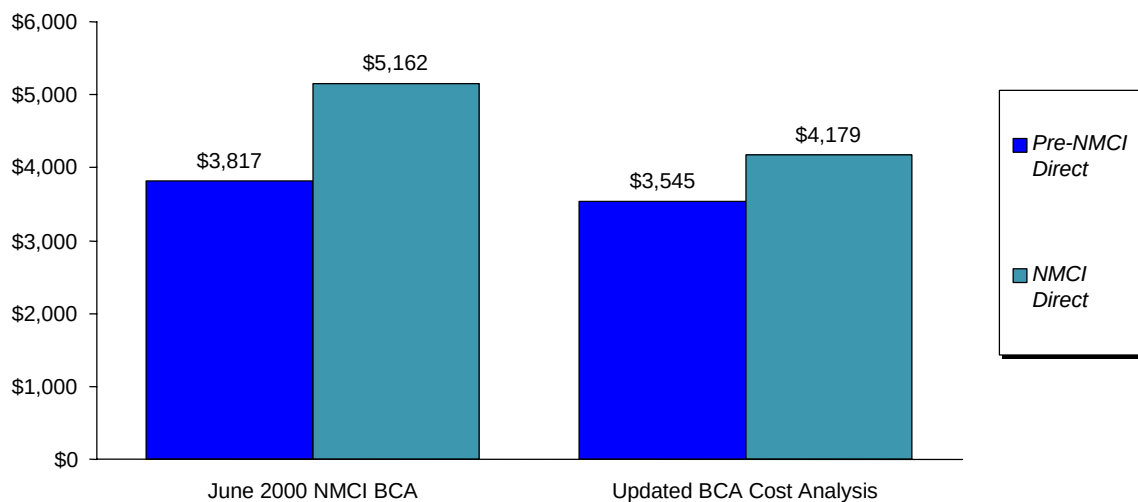


Figure 9. Comparison of seat costs (NMCI, 2002)

As shown, the cost of a NMCI seat is higher than the cost of a Pre-NMCI seat. However, the reasoning for this is that the price of an NMCI seat includes capabilities that are not available in the Pre-NMCI environment. These capabilities include compliance with DoD mandated requirements (Federal Records Management, Public Key Infrastructure (PKI), and other security upgrades, as well as Defense Information Technology Security Certification and Accreditation Process (DITSCAP) testing). Also included are contractual SLAs that provide increased network performance, capacity, reliability, and interoperability. When the cost of implementing the DoD mandated capabilities is taken into account for the Pre-NMCI environment seat cost, the per seat cost increases to \$4,286, which is 2% higher than the NMCI seat cost. (NMCI, April 2002)

One of the fundamental reasons for selecting NMCI as the IT enterprise solution was the inability to determine actual IT costs or the ability to achieve IT consistency among all commands. Both the initial BCA and the updated BCA show that NMCI is a viable alternative to the current IT service structure. When the potential cost of achieving comparable performance through an organic solution is considered, NMCI presents itself as the best method for achieving the desired performance goals.

G. CHAPTER SUMMARY

This chapter discussed the increasing reliance on outsourcing as well as some best practices associated with outsourcing projects. In addition, the chapter also discussed seat management contracts as a vehicle for providing IT services. The chapter then discussed NMCI, the Navy and Marine Corps answer to shortcomings in their network service provision and management. The chapter concluded with a discussion of the benefits associated with seat management contracts and expected benefits of NMCI.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THE INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY

A. INTRODUCTION

This chapter will discuss the Information Technology Infrastructure Library (ITIL) as a management framework. This chapter will compare ITIL to other frameworks, such as the Control Objectives for Information and Related Technology (COBIT), Capability Maturity Model (CMM), Six Sigma, and the Information Technology Investment Management (ITIM) framework. This chapter will also explore the framework that is used by NMCI for client-facing support.

B. WHAT ARE INFORMATION TECHNOLOGY FRAMEWORKS AND WHY SHOULD THEY BE IMPLEMENTED?

In recent years, managers at all levels have begun to recognize that information is the most important strategic resource that an organization has. It is essential that the importance of IT systems is recognized and that the appropriate levels of resources are invested in their support, delivery, and management. In many organizations, these aspects of IT are often overlooked or are only superficially addressed. The challenge for today's IT managers, as well as business managers from other departments, is to coordinate and work in partnership with the business to deliver high quality IT services that are strategically aligned to ensure that the organizations goals are accomplished and improve the organizations overall performance. In order to meet these goals, the need exists for a systematic management approach that addresses critical elements of the strategic planning process.

To help Federal agencies effectively manage their IT investments, they must follow laws such as the Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996 that require agency heads, acting through CIOs to:

- Better link IT planning and investment decisions to program missions and goals
- Develop and maintain a strategic information resources management (IRM) plan that describes how IRM activities help to accomplish agency missions

- Develop and maintain an ongoing process to establish goals for improving IRM's contribution to program productivity, efficiency, and effectiveness; methods for measuring progress toward these goals; and clear roles and responsibilities for achieving these goals
- Develop and implement a sound IT architecture
- Implement and enforce IT management policies, procedures, standards, and guidelines
- Establish policies and procedures for ensuring that IT systems provide reliable, consistent, and timely financial or program performance data (GAO, March 2004)

These laws were enacted to help organizations keep pace with evolving management practices that are necessary to precisely define critical information needs and to select, apply, and control changing information technologies. Even with the above guidance requiring such practices, agencies did not always have proper strategic planning processes, performance measurement practices, or investment management practices in place. Without these processes and practices in place, agencies faced significant challenges when attempting to effectively plan for and manage IT services. Poor service, wasted resources, high costs, low productivity and too little evidence of meaningful results are consequences of poor IT management. One method that agencies can utilize to improve their IT management is to implement management frameworks.

The purpose of frameworks is to improve the management of IT, so that it enables more efficient and cost effective delivery of services to the organization. There are several frameworks that have been developed; however each has a different focus. Some of the more popular frameworks include the Capability Maturity Model (CMM), Six Sigma, Control Objectives for Information and Related Technology (COBIT) and the IT Investment Management (ITIM) framework. Since the Information Technology Infrastructure Library is the only framework that provides comprehensive guidance, it is quickly becoming an increasingly popular framework.

C. THE INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY FRAMEWORK

ITIL is the IT Infrastructure Library, a set of publications that provides descriptive guidance on IT service management. Created by the United Kingdom's

Office of Government Commerce (OGC) in the late 1980s, ITIL was founded on two key premises:

- Create comprehensive, consistent and coherent standards of best practices for quality IT Service management promoting business effectiveness in the use of IT
- Encourage the private sector to develop ITIL-related services and products (training, consultancy, and tools) (Ranvijay, August 2005)

In a recent survey, Evergreen Systems of the 167 CIOs and other IT executives that participated, 95 percent said they had budgeted for or approved ITIL projects during 2005. (Worthen, September 2005) The adoption of ITIL principles is rising in the U.S., where implementation of ITIL principles appears to be focused around customer-facing processes such as those found in service support and service delivery.

The ITIL was developed as a partnership of government, private organizations, and editorial boards. The books were written by a consortium of representatives from leading organizations and quality audits were done by international reviewers. The main purpose for the involvement of the OGC was to provide editorial functions and to examine the processes presented in the books. The result of this is that ITIL books are non-proprietary and available to the public.

1. What is IT Service Management?

IT services are normally provided by an IT department and consists of an IT infrastructure. The ITIL defines the IT infrastructure as the hardware, software, procedures, computer-related communications, documentation, and the human skills required to support IT services. Since these components must be managed, the overall IT services and management of the IT infrastructure is referred by ITIL as IT service management. Service management, as used as a core principle of ITIL is defined as any aspect of the management of IT service provision and should include the whole of ITIL and not be limited to specific core modules of ITIL.

Service management focuses on the satisfaction of business and customer requirements. Examples of activities that are considered vital to successful service management are:

- Documenting, negotiating, and agreeing customer and business quality targets and responsibilities in Service Level Agreements (SLAs)
- Regular assessment of customer opinion through feedback and satisfaction surveys
- IT personnel regularly sampling the experience that customers receive from the IT department
- IT personnel taking the customer and business perspective and always trying to keep customer interactions as simple and enjoyable as possible

ITIL provides comprehensive best practice guidelines that cover all aspects of end-to-end service management, including people, processes, products, and the use of partners. Service management and the ITIL framework help to assist IT service providers, both in-house and outsourced, to improve IT efficiency and effectiveness while improving the overall quality of service to the business, within imposed cost constraints. (IT Service Management Forum, July 2004)

2. The Seven Modules of Information Technology Infrastructure Library

There are seven modules, also called books that constitute the core of ITIL. ITIL has been developed to be process driven and yet scalable and flexible enough to fit any size organization. The relationship between the seven ITIL modules, the organization, and the supporting technology is shown in Figure 10 below. At the heart of ITIL is the service delivery and service support modules. There is a balance between the customer facing modules and the technology facing modules that is required for effective IT service management.

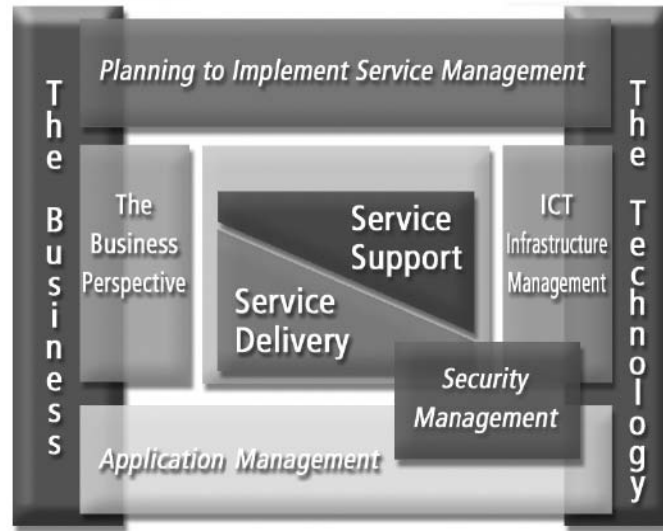


Figure 10. The ITIL framework (IT Service Management Forum, July 2004)

a. Service Delivery

Service delivery covers the process required for the planning and delivery of quality IT services and looks at the longer term processes associated with improving the quality of IT services delivered. This module defines the more forward-looking delivery aspects of service provision and consists of service level management (SLM), financial management for IT services, capacity management, IT service continuity, and availability management. The focus of these processes is to assist with developing plans for improving the quality of IT services delivered.

Service level management principles are most often used when negotiating, documenting, agreeing to and reviewing business service requirements and targets, and when developing Service Level Agreements (SLAs). Other major roles of the SLM process is the production of the essential information on the complete portfolio of IT services provided. The overall improvement plan, consisting of the Service Improvement Plan (SIP), helps plan for continuous improvement in the quality of IT services delivered to the organization. The SLM processes can be applied to service providers, both in-house and external.

Financial management of IT services can be one of the more difficult tasks for an IT department. The financial management processes described in the service

management module provides the basis for running IT as a business within a business and helps to develop a cost conscious and cost effective organization. The concept of understanding and accounting for the costs of provisioning IT services and the forecasting of future expenditures within the IT financial plan is difficult for IT departments, as well as other business units to grasp. Service delivery provides the basis for processes to recover IT costs from business units in a fair and equitable manner. SLM demonstrates the level of service that is being delivered to the business. As long as the level of service meets the business' specified requirements, you can show the financial value of those services.

A Capacity Plan, developed as part of the capacity management process, ensures that adequate capacity is available at all times to meet the requirements of the business by balancing business demand with IT supply. The Capacity Plan is closely linked with the business strategy and is produced and reviewed on a regular basis. Some of the common activities associated with capacity management are: performance management, workload management, demand management, and application sizing and modeling.

IT service continuity is focused on protecting the businesses essential IT systems from loss of usability due to disruptions of service caused by major incidents. This is where recovery plans are developed and implemented to ensure that IT services are provided to an agreed level, within an agreed schedule. Periodic exercises such as business impact analysis, risk analysis, and risk management are undertaken along with the maintenance and testing of recovery plans to ensure that recovery plans are kept in line with changing business needs.

Availability is a key aspect of service quality. Availability management helps to ensure that the availability of each service meets or exceeds targets and is improved on an ongoing basis. Availability management monitors, measures, reports, and reviews key metrics for each service, including availability, reliability, maintainability, serviceability, and security.

b. Service Support

This module describes the processes associated with the day-to-day support and maintenance activities that provide stability and flexibility for IT service provision. Processes such as incident management, problem management, change management, configuration management, release management, and the service desk function are described in the service support module. Where service delivery is more focused on the customer, service support focuses on the technology behind the service delivery.

The exception to service support focusing on the technology is the service desk. The service desk is a customer facing entity that provides a single, central point of contact for all users of IT within the organization. The purpose of the service desk is to handle all incidents, queries, and requests from users and to provide the interface to all of the other service support processes.

The management of all Incidents from detection and recording through to resolution and closure is known as incident management. The objective of incident management is the restoration of normal service as soon as possible with minimal disruption to the business. Incident management is similar to problem management, which attempts to minimize the adverse impact of incidents and problems on the business. Problem management assists incident management by recording all problem solutions, including temporary or “quick-fixes” and by raising changes to implement permanent solutions when possible. The analysis of trends is done here to prevent further incidents and problems.

Changes can be one of the most problematic areas for an organization. In order to provide efficient and effective handling of changes, a single centralized change management process is required. Changes should be managed throughout their entire lifecycle, from initiation and recording through implementation, review and closure. One of the deliverables of change management is the forward schedule of change, which is a central program of change that is agreed upon by all areas, based on impact and urgency. To assist in change management, a configuration management board can be established to review and approve all changes that are made to a networks configuration.

Configuration management provides the foundation for successful IT service management and is the foundation for every other process. The Configuration management database is comprised of one or more integrated databases detailing all the organization's IT infrastructure components and other important associated assets. These assets are known as configuration items and deliver the IT services. The configuration management database is different from other asset management programs in that activities such as impact analysis and 'what if?' scenarios can be carried out. The database also contains details of any incidents, problems, and changes associated with each configuration item.

Release management is a process that takes a holistic view of changes to IT services, both technical and non-technical. It is responsible for all legal and contractual obligations for all hardware and software in use throughout the organization. In order to protect IT assets, release management establishes secure environments for both hardware and software using the definitive hardware store and the definitive software library.

c. Information Communication Technology Infrastructure Management (ICT IM)

The ICT IM module is related to all aspects of ICT Infrastructure Management from identification of business requirements to the testing, installation, deployment, and ongoing operation and optimization of the ICT components and IT services. The management processes this module covers are; overall management and administration, design and planning, technical support, deployment and operations. The processes in this module are closely associated with the technology on which the IT services run.

The goal of the management and administration areas of ICT IM is to improve the effectiveness and efficiency of the ICT infrastructure, while maintaining the overall quality of the IT services provided. This is done by creating the most appropriate environment under which a secure infrastructure is maintained. The delivery of quality IT services, both current and planned, to the business is monitored during this process.

ICT infrastructure managers take part in the business change program by working with the ICT steering group. The ICT infrastructure managers participate in quality and audit review and in crisis management situations. The managers also ensure that proper support processes are in place to ensure that all areas of IT can operate effectively and efficiently.

The design and planning function is responsible for all of the strategic issues placed on the ICT by the organization. This is where the future plans of the business and the plans of IT are aligned. Architectures and strategies required for the provision of current and future ICT business solutions are developed. The key task is to include all requirements, not just the functional ones, for a new service, considering them from the initial stages of requirements through the lifecycle of the service. This helps to ensure that the services are designed for operational excellence and that all requirements are identified at the earliest possible and most cost effective stage of the service lifecycle. Business managers and planners must work closely with IT personnel during the design and planning process to ensure that all business plans and strategies are aligned with ICT plans.

Deploying new and changed ICT solutions to the business is the focus of the deployment process. This involves establishing projects and project methodologies to ensure that new ICT solutions are delivered to the business with minimum disruption to the business process and that the use of ICT is optimized. The deployed projects must meet agreed upon quality, cost, and timescales. Close liaison with the business is important to ensure a projects success. The deployment process also includes items such as training for the new ICT system and acceptance criteria. This ensures that the business is receiving a fully operable system that is usable from the first day it is installed.

The operations management function is responsible for managing and controlling the IT services and environments. The role of the operations management team is to use management tools to ensure that all services and components meet all operational targets, as agreed upon in service level agreements. This also involves the tuning and optimization of all operational areas of the ICT infrastructure.

Technical support provides the backbone of the organization. Ensuring that the necessary support, skills, and knowledge are available to provide reliable ICT services is the primary responsibility. A pool of in-depth technical expertise is required to provide information, guidance, and resources for the research and development of new technology solutions.

d. Planning to Implement Service Management

This module examines the issues and tasks involved in planning, implementing, and improving ITIL processes within an organization. It also addresses the issues associated with addressing cultural and organizational change, project and program planning, process definition, and performance improvement. This is also a plan of continuous improvement. The overall vision for IT is produced, a vision for IT service management is agreed upon by both the organization and IT. This vision describes the aim and purpose of service management for the organization.

Once the vision is developed, the next step is to establish the “where are we now?” By using an overall IT organizational growth model, this assessment can be made. The model determines the current maturity of the IT organization in terms of: Vision and strategy, steering, processes, people, technology, and culture. Other techniques can be used, including internal review, benchmarking, and assessing current processes against industry standards and guidelines.

In order to understand the future of IT services, the organization and IT must agree on the future roles and characteristics required of the IT organization. This involves a gap assessment that determines what capabilities are required that the current environment is lacking.

The plan that shows how to get from the current environment to the future environment is then produced. This plan considers: how the changes will be achieved, where to start, and which elements are essential. The answers to these questions determine the approach, final scope, and terms of reference for the project. To assess the projects progress and performance, a set of measurable milestones and deliverables is developed. These need to be regularly measured, monitored, and reviewed at each stage of the project to ensure success.

Throughout the process, it is important to maintain organizational focus, priority, impact, and alignment to ensure that all improvements realize the true organizational benefits.

e. Application Management

Application Management describes how to manage applications from the initial business need, through all stages in the application lifecycle, up to and including retirement. It places emphasis on ensuring that IT projects and strategies are tightly aligned with those of the business throughout the application lifecycle, to ensure that the business obtains best value from its investment. Applications need to be deployed with service management requirements included; they should be designed and built for operability, availability, reliability, maintainability, performance, and manageability. The applications should also be tested for specification compliance. Application management differs from application development in that application management describes the overall handling of the application as it progresses through its entire lifecycle. Application development consists of the activities needed to plan, design, and build an application.

Throughout the application lifecycle, it is essential that the organizations requirements, as well as the service management requirements are considered at each stage. Joint strategies form the foundation of application development or deployment project, which helps to ensure that the objectives are clear, concise, and achievable. One of the problems that an organization faces with respect to applications is that the number of applications is constantly increasing. A process is required to manage that complex environment. An application portfolio is one method of documenting, viewing, and evaluating the entire suite of applications in use throughout the organization.

Many organizations do not assess their ability to build, maintain, and operate the IT services that the organization requires. A readiness assessment can provide a mechanism to help determine the organizations state of readiness and capabilities for delivering a new or revised application. This assessment can be used to help develop the delivery strategy for the application or IT service. The delivery strategy

is an approach that is developed after reviewing the readiness assessment and comparing that to a desired state that is determined by the organizations goals.

f. The Business Perspective

This module provides advice and guidance to help IT personnel to understand how they can contribute to the business objectives and how their roles and services can be better aligned and exploited to maximize that contribution. This awareness of the organization enables service management to ensure the most effective relationships, interfaces, and delivery of services to maximize the benefits of IT.

There are several objectives of the business perspective approach to delivering IT services:

- To enable IT personnel to understand how they contribute to the organizations objectives
- To enable IT personnel to deliver or improve IT services to help the organization achieve objectives
- To enable IT personnel to assist the business in maximizing the exploitation of IT
- To enable a complementary and integrated culture with the business
- To influence, innovate, and enable change that provides an advantage
- The alignment of IT with the organization

By adhering to the principles of the business perspective approach, a “business led” IT organization is developed. This type of organization has strong partnerships between IT and the organization, which ensures that IT services are aligned to meet the organizations requirements.

Process such as business relationship management (BRM); supplier relationship management (SRM); the review, planning, and development of IT; and the liaison, education, and communication of IT are developed to achieve alignment. BRM processes focus on developing relationships between IT service providers and their customers and business managers, while SRM processes focus on developing the relationship between IT and their suppliers. This is necessary since the suppliers provide services to the organization that have a direct impact on the quality of service that is delivered to the customers and the organization.

g. Security Management

Security Management details the process of planning and managing a defined level of security for information and IT services, including all aspects associated with reaction to security incidents. It also includes the assessment and management of risks and vulnerabilities, and the implementation of cost justifiable countermeasures. IT security management ensures that:

- Security controls are implemented and maintained to address changing circumstances such as changed business and IT service requirements, IT architecture elements, and threats
- Security incidents are managed
- Audit results show the adequacy of security controls and measures taken
- Reports are produced to show the status of information security

Security of information and systems is one of the main areas of concern for IT managers, as well as other organization managers. Security management implemented as part of ITIL is no exception. Management is responsible for taking appropriate steps to reduce the chances of a security incident occurring to acceptable levels. This process is known as risk assessment and management. Executive management is responsible for defining the security policy that governs IT security management. The purpose of the policy is to reinforce the organizations dedication to the security of information and information systems. The security policy provides management with guidelines, roles, and responsibilities that assist the organization in providing safe, secure, and reliable IT systems.

One of the most difficult tasks is to balance security with availability of IT systems. Security management must be closely aligned with all other areas of service management, as well as the customers so that vulnerabilities are reduced to an acceptable level, while maintaining maximum usability. The Figure below shows an overview of the ITIL IT security management process. Central to the process is the customer's requirements, around which the development and implementation of the security management process takes place.

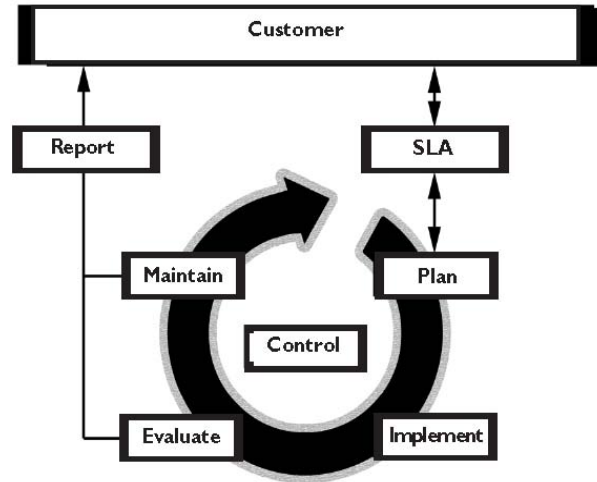


Figure 11. The ITIL security management process (IT Service Management Forum, July 2004)

The modules of ITIL provide a total life-cycle management approach to managing an organization's computing infrastructure, its resources, people, and the organization of IT services. While organizations are likely to gain the most benefit from total implementation of the ITIL guidance, it is designed to be adaptable to suit the needs of an organization; however, caution is required to avoid omitting activities without considering the consequences.

3. Benefits of Using the ITIL Framework

ITIL is not a step-by-step manual for IT management; instead, it offers a systematic, yet common sense approach to the processes involved in the management of IT services. ITIL recognizes that there is no universal solution to the design and implementation of an optimized process for the management and delivery of quality IT services. In fact, organizations are encouraged to adapt the guidance to meet their particular needs. The implementation of ITIL creates benefits for both the customer and service providers. Among the many benefits of ITIL, the one that stands out is that it enables organizations to better align IT initiatives with business goals and helps provide a quantitative answer about a project's value to the organization. This allows for better management of projects, both in-house and outsourced. Organizations that have adopted ITIL have seen increasing customer satisfaction with IT services, reduced costs, and greater productivity. ITIL can also be used for client-facing services. When used

properly, ITIL helps IT departments improve their quality of service, including increased system reliability, faster problem resolution, and better security.

Organizations that have implemented ITIL have realized many benefits. Some examples are:

- Continuous improvement in the delivery of quality IT services
- Reduced long term costs through improved ROI or reduced TCO through process improvement
- Reduced risk of not meeting business objectives, through the delivery of rapidly recoverable, consistent services
- Improved communications and better working relationships between IT and the organization
- The ability to absorb a higher rate of change with an improved, measurable rate of success

Many of the benefits of ITIL are not tangible; they are often organizational and difficult to accurately measure.

4. Problems That May Arise When Implementing the Information Technology Infrastructure Library Principles

ITIL provides operational guidance for IT processes related to the delivery of services to the customer. It states what should be done; the design of the process is left to the organization. ITIL requires substantial changes throughout an organization, which can lead to cultural resistance to the adoption of process discipline. It is also difficult to capture the cost of adopting the framework, along with the associated training, consulting, and software tools. This can be a large cost for a small or mid-sized organization, or an IT department that faces continual budget cuts. Since ITIL is a generic framework, it can be difficult to determine how long it will take to implement the processes, which may lead to tension between the IT organization and the customer.

D. HOW DOES THE INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY COMPARE TO OTHER MANAGEMENT FRAMEWORKS?

As IT becomes increasingly automated, more companies are embracing a best-practices approach that is outlined in IT frameworks. The ITIL, Control Objectives for Information and Related Technology (COBIT), Capability Maturity Model (CMM), Six

Sigma, and the government developed Information Technology Investment Management are all popular frameworks in use today.

1. The Control Objectives for Information and Related Technology (COBIT) Framework

COBIT was developed in 1996 by the Information Systems Audit and Control Association and is now maintained by the IT Governance Institute as a standard for IT security and control practices. (Violino, February 2005) COBIT identifies 34 high-level control objectives that are grouped into four main domains: planning and organization, acquisition and implementation, delivery and support, and monitoring. These domains work together to provide a framework for information security.

Planning and organizing covers a range of topics including the strategy and tactics used by IT to achieve business objectives, strategy planning, strategy communication, strategy management, risk management, and resource management. Acquisition and implementation identifies, develops or acquires, and implements solutions. The management of life-cycle for existing systems is also managed through this domain. Delivery and support is the domain that is concerned with delivering services to customers. Included in delivery and support are such issues as performance and security, as well as training. All IT processes are monitored to ensure quality and compliance with control requirements. The monitoring domain is where management's oversight of the control processes takes place.

COBIT represents a comprehensive framework for implementing IT security governance with a strong auditing and controls perspective. ITILs service management processes can be used to provide support for COBITs focus on audit and control. COBIT allows organizations to check their ITIL implementation to make sure they are addressing the appropriate risks.

2. The Capability Maturity Model

The Capability Maturity Model (CMM) was published by the Software Engineering Institute at Carnegie Mellon University in 1991. Since then, CMM has evolved into a framework to help guide process improvements in software development, systems engineering, and research and development. The framework is used to improve

the quality of products and services, increase development efficiency and reduce the risks associated with software development projects. The CMM was replaced by the Capability Maturity Model Integration (CMMI), which is a process improvement approach that provides organizations with the essential elements of effective processes. One of the differences between the CMM and the CMMI is that the CMMI can be used to help integrate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes. The CMMI is composed of models that cover four disciplines; Systems engineering, software engineering, integrated product and process development, and supplier sourcing. In order to measure an organizations maturity, there are five maturity levels of process improvement, each of which provides a layer for ongoing process improvement. The maturity levels consist of a predefined set of process areas. The five levels are:

- Initial – Processes are usually ad hoc and chaotic. The organization does not provide a stable environment and success depends on the competence of the people in the organization and does not rely on processes. Organizations operating at this level tend to over commit and abandon processes in times of crisis. Past successes are normally not repeated.
- Managed – The projects that the organization undertakes ensure that requirements are managed and that processes are planned, performed, measured, and controlled. At this level, requirements, processes, work products, and services are managed and the status of projects are visible to management at defined points. Projects are reviewed with stakeholders and are controlled to ensure success.
- Defined – At the defined maturity level, processes are well characterized and understood and are described in standards, procedures, tools, and methods. Standard processes are used to establish consistency across the organization. The processes of level 3 organizations are more detailed than those of a level 2 organization and are more proactively managed.
- Quantitatively managed – An organization at level 4 has achieved all the specific goals of levels 2, 3, and 4. Quantitative objectives for quality and process performance are established and used as criteria in managing processes. Quality and performance are understood in statistical terms and are managed throughout the life of the processes.
- Optimizing – This level focuses on continuous improvement of processes, based on quantitative understanding of the causes of variation.

The CMMI differs from the ITIL in that the CMMI is used to develop and enhance processes by developing specific goals, practices, common features, and subpractices.

3. Six Sigma

Six Sigma is a disciplined, data-driven approach and methodology for eliminating defects in processes. By improving process performance along with decreasing process variance, organizations can realize defect reduction and improvements in profit. The goal of the methodology is to reduce defect levels below 3.4 defects per million opportunities (DPMO). There are two basic methodologies that can be used; DMAIC (define, measure, analyze, improve, and control) and DMADV (define, measure, analyze, design, and verify).

DMAIC is a basic methodology that consists of five phases; define, measure, analyze, improve, and control. Goals for process improvement are defined to ensure that they are consistent with customer demands and organizational strategy. Baseline measurements that can be used for future comparison are defined based on current practices, which are mapped and measured. Analysis of processes is conducted to verify any relationships and causality of factors. The processes are then optimized based on the analysis. Under control, test runs are used to establish process capability, transition to production, and then continuously measured to control variances before any defects result.

The DMADV also consists of five phases; define, measure, analyze, design, and verify. As with DMAIC, the goals are defined to be consistent with customer demands and organizational strategy. During measurement, product capabilities, production process capability, and risk assessment are identified. Design alternatives are developed and evaluated during analysis to ensure that the best design is selected. Detailed designs are developed in the design phase, which may require simulations. Designs are then verified, pilot runs setup, and the process is then implemented and control handed over to the process owners.

Six Sigma provides a quantitative methodology for process improvement, while ITIL is a framework that provides a comprehensive set of management procedures.

4. The Information Technology Investment Management Framework

The Information Technology Investment Management (ITIM) framework is a Government Accountability Office defined framework designed to assess and improve process maturity. Like the CMMI, it is composed of five progressive stages of maturity that an organization can achieve in its IT investment management capabilities. The framework can be used to assess an organizations investment management processes and as a tool for organizational improvement. ITIM is a tool that supports organizational self-assessment and improvement and provides a standard against which an evaluation of an organization can be conducted. Figure 12 is a representation of the five defined levels of ITIM maturity.



Maturity stages	Critical processes
Stage 5: Leveraging IT for strategic outcomes	- Optimizing the investment process - Using IT to drive strategic business change
Stage 4: Improving the investment process	- Improving the portfolio's performance - Managing the succession of information systems
Stage 3: Developing a complete investment portfolio	- Defining the portfolio criteria - Creating the portfolio - Evaluating the portfolio - Conducting postimplementation reviews
Stage 2: Building the investment foundation	- Instituting the investment board - Meeting business needs - Selecting an investment - Providing investment oversight - Capturing investment information
Stage 1: Creating investment awareness	- IT spending without disciplined investment processes

Figure 12. ITIM Framework (GAO, 2004)

Stage 1, creating investment awareness, is characterized by ad hoc, unstructured investment processes, much like the initial level of the CMMI. Building the investment foundation, stage 2, focuses on establishing basic selection capabilities and forms the foundation for stage 3. This is where IT investment boards are created and business needs are identified. This knowledge is used in the selection process for IT projects. At this level, IT investment control processes should be repeatable and successful. Stage 3, developing a complete investment portfolio, focuses on the structure and repeatability of

project-centric management processes established in stage 2. A consistent and well-defined IT investment portfolio perspective is established along with mature, integrated selection, control, and evaluation processes. Using evaluation techniques to improve IT investment processes is the focus of stage 4, improving the investment process. Regular analysis of the IT portfolio is done to ensure that investments continue to be aligned with the current version of the enterprise architecture. Stage 5, leveraging IT for strategic operations, organizations use benchmarking to ensure its IT investment processes are similar to other “best-in-class” organizations. Throughout stage 5, continuous monitoring for breakthrough technologies that can enhance and improve business performance is conducted.

ITIM differs from ITIL in that ITIM describes and improves an organization’s IT investment management processes so that strategic plans and decisions can and will be supported by effective IT investments. The framework does not address day-to-day operation once the IT systems and services are implemented.

ITIL can be used in conjunction with other frameworks to ensure that an organization effectively manages their IT assets throughout the entire life-cycle.

E. CHAPTER SUMMARY

This chapter discussed the reasons for choosing and implementing a management framework to support IT service management. In addition, the chapter also introduced the ITIL framework and compared it to other management frameworks that are available for use.

V. TRANSFORMATION AND BUSINESS PROCESS REENGINEERING

A. INTRODUCTION

This chapter will explore the Transformation efforts of the Department of Defense, specifically the objectives, business enterprise priorities and governance of the efforts. This chapter will also discuss the transformation efforts of the Department of the Navy, as well as those of the United States Marine Corps. There will also be a discussion of knowledge value added and business process re-engineering.

B. DEPARTMENT OF DEFENSE TRANSFORMATION

Quite possibly, the Department of Defense (DoD) is the largest and most complex organization in the world. The annual budget is more than twice that of the world's largest corporation, it employs more people than the population of a third of the world's countries, medical care is provided for as many patients as the largest health management organization, and the inventory carried is five hundred times larger than the world's largest commercial retail operation. (DoD, 30 September 2005) The responsibility of maintaining national security against today's enemies demands that the DoD be as adaptive, flexible, and accountable as any organization. The challenge for the DoD's business transformation efforts is to reconcile the apparent contradiction between size and flexibility and provide equally flexible and responsive business and financial support that is capable of adapting to conditions that are constantly changing.

The Business Mission Area (BMA) has the responsibility to ensure that the capabilities, resources, and materiel are delivered to the warfighter. In order to do this, the DoD requires a cost-effective business and financial management infrastructure, consisting of processes, standards, and data, to ensure that the warfighter receives what is needed, when it is needed, and where it is needed. This is the focus of the DoD's efforts at business transformation, (DoD, 30 September 2005) providing end-to-end integration of operations in support of missions in times of peace and war.

In 2001, the Government Accountability Office (GAO) recommended that the DoD develop an enterprise architecture to guide and constrain its transformation efforts.

(GAO, July 2005) In response to the GAO, the DoD initiated the Business Management Modernization Program (BMMP). The BMMP was a broad and comprehensive initiative to coordinate the transformation efforts and served as the basis for transformation within the business mission area and established the Business Enterprise Architecture (BEA). (GAO, July 2005)

The BEA provides the architectural framework for the DoD's information infrastructure, including business rules, requirements, data standards, system interface requirements, and policies and procedures. It is the future vision for the BMA. The key products of the BEA are:

- A description of end-to-end business processes
- Foundational standards and business rules
- The basis for DoD investment management criteria for systems certification
- The standardization of interoperable IT systems
- Acceleration of outcome based architecture development and implementation

The BEA also guides the Enterprise Transition Plan (ETP). The ETP is a comprehensive management tool that supports the BEA by providing a systematic approach to achieve the future state of desired capabilities. The ETP has a clear set of priorities, milestones, and performance metrics for information systems that will be part of the BEA, as well as providing a termination schedule for legacy systems that will not be part of the BEA.

1. Business Enterprise Priorities

The ETP details the business transition plan that is organized around six DoD-wide Business Enterprise Priorities (BEPs) that cover a range of personnel, logistics, real property, acquisition, purchasing, and financial requirements. Over the past years, each of the BEPs has seen an increasing reliance on IT services and the transformation efforts are focused on integrating existing systems, people, and business processes. The BEPs were chosen for the possible impact and support for the Core Business Missions of the DoD, which include Human Resources Management, Weapon System Lifecycle

Management, Materiel Supply and Service Management, Real Property and Installations Lifecycle Management, and Financial Management. (DoD Pamphlet, 2005)

a. *Personnel Visibility*

Personnel visibility focuses on providing access to reliable, timely, and accurate personnel (service members, civilian employees, retirees, and contractors) information to assist in mission planning. The benefits associated with increased personnel visibility include accurate and timely access to compensation, decreased operational costs, reduced cycle times, and enabled management of DoD human resources in a combined (military, civilian, and contract support) environment. (DoD Pamphlet, 2005) Personnel visibility programs will allow for better personnel tracking and enable the DoD to rapidly identify who has been deployed and who is available to deploy. Support for service members and civilian employees will improve through more timely and accurate pay and compensation. The solutions for personnel visibility will enable secure information sharing in a responsive, streamlined systems environment that will allow managers at all levels to perform effective analyses of personnel issues through standardization of data and business rules while reducing associated costs.

b. *Acquisition Visibility*

Acquisition Visibility, defined as timely access to accurate, authoritative, and reliable information supporting acquisition oversight, accountability, and decision making throughout the DoD for effective and efficient delivery of warfighting capabilities. (DoD, September 2005) Through the programs associated with acquisition visibility, the DoD will gain a method for managing the critical information for supporting the process lifecycle for delivery of weapons systems and automated information systems. This will be done by addressing the full lifecycle of acquisition management, to include; requirements definition, technology development, production, deployment, sustainment, and disposal. Standard data requirements will be developed, along with authoritative data sources, relevant business rules, standard interfaces, and enterprise-wide solutions. This will provide the ability to quickly share information that is accurate, relevant, and consistent that will reduce oversight workloads of both acquisition employees and management. Acquisition management will provide the DoD the ability to continually assess the status of acquisition programs, including milestone

and budgetary performance, and compliance with statutory and regulatory information reporting requirements and guidelines.

c. Materiel Visibility

The Materiel Visibility BEP is defined as the ability to locate and account for materiel assets throughout their lifecycle and provide transaction visibility across logistics systems in support of the joint warfighting mission. (DoD, September 2005) The programs associated with materiel visibility are designed to provide users with timely and accurate information on the location, movement, status, and identity unit equipment, materiel and supplies in an effort to improve the efficiency of the supply chain to the warfighter. IT support is essential to materiel visibility transformation efforts. Proper use of IT will enable the implementation of programs that allow hands-off processing of transactions designed to improve process efficiency of shipping, receiving, and inventory management. IT systems and networks are also needed to provide the capability to accurately account for materiel costs. Improved access to historical data during the systems design process, as well as throughout the life-cycle of a program will increase the efficiency of the design and acquisition of systems and programs. The objectives of materiel visibility will allow real-time information regarding the DoD's inventory of equipment, leading to improved readiness and cost reductions while enabling the services to optimally deploy the equipment when and where it is needed.

d. Common Supplier Engagement

Common Supplier Engagement is focused on the alignment and integration of the policies, processes, data, technology and people in order to simplify and standardize how the DoD interacts with commercial and government suppliers. CSE objectives will also create standard business processes, rules, data, and interoperable systems that will be used across the DoD. IT solutions will enable the DoD to provide efficient and standardized management processes for procurement of materiel and services.

e. Real Property Accountability

The efforts associated with Real Property Accountability are focused on providing access to near real-time, accurate, and reliable physical, legal, financial, and environmental information related to real property assets of the DoD. IT systems and

programs will assist installation managers with requirements such as improved accuracy and auditability of financial statements by providing increased access to reliable and accurate information that can be used for planning purposes. Consolidated and interoperable process and information support systems will replace the disparate systems that have been in use. This lack of interoperability has hampered the ability to address customer requirements adequately. Once the Real Property Accountability objectives are met, the DoD will be able to link people to the physical assets with greater accuracy, leading to improved readiness.

f. Financial Visibility

To support the missions of the DoD, accurate and reliable financial information such as planning, programming, budgeting, accounting, and cost information is required to make effective decisions. The objectives of Financial Visibility will provide this by creating authoritative data sources that, when combined with a common financial language that is used across the DoD, will create financial data that is transparent throughout the enterprise. Since Financial Management is engaged at all levels within the DoD, it is essential to have timely, reliable, and accurate financial information that provides a shared understanding of how funds enter the DoD and how they are allocated.

C. DEPARTMENT OF THE NAVY AND MARINE CORPS BUSINESS TRANSFORMATION

The business improvement objectives of the Department of the Navy are guided by and designed to help achieve the Naval Power 21 vision and facilitate the implementation of Sea Power 21 and the Marine Corps Strategy 21. The vision of the DON is to increase readiness, effectiveness, and availability of forces by employing business process change to create efficient operations at reduced costs and to exploit process improvements, technology enhancements, and personnel to ensure mission superiority.

There are five objectives that the DON has determined necessary to enable the achievement of the Naval Power 21 vision and facilitate the implementation of Sea Power 21 and Marine Corps Strategy 21:

- Develop and maintain a secure, seamless, interoperable Information Management/Information Technology (IM/IT) infrastructure as the transport layer for transformed business processes.
- Create optimized processes and integrated systems
- Optimize investments for mission accomplishment
- Transform applications and data into web-based capabilities to improve effectiveness and gain efficiencies
- Align Business Mission Area governance to produce a single, integrated enterprise (DON, 2002)

The DON recognizes the importance of alignment of senior leadership at an enterprise level if transformation efforts are to be successful and has placed great emphasis on their efforts. The DON Business Process Transformation Council has been formed to provide senior leadership guidance and provide enterprise-wide policy direction and oversight. The Navy has also created functional areas that are aligned with the DoD's core business mission areas, with representatives assigned as voting members of the DoD investment review boards. The DON recognizes the importance of IT systems to their efforts and realizes that alignment with DoD initiatives is essential to provide interoperability. As a part of transformation efforts, some of the systems being designed are focused on logistics management, personnel management, and financial management. These systems were designed in an effort to reduce costs, provide interoperability, and enhance mission readiness.

D. BUSINESS PROCESS REENGINEERING

Business Process Reengineering (BPR) is an important part of the DoD's efforts at transformation of business management. Since BPR efforts involve changing of organizational structures, management systems, employee responsibilities, performance measurements, and the use of information technology, it has the potential to affect every aspect of an organization. Successful BPR can result in reductions in cost, improvements in quality and business objectives, which are some of the goals of DoD transformation.

Many of the current business processes, control mechanisms, and organizational structures in use throughout the DoD were designed before the advent of modern computers and computer networks. Many of the processes are paper-intensive, prone to human error, or reside on stove-piped systems that were not developed for

interoperability. This has resulted in a lack of reliable information needed to make decisions, decreased operational efficiency, adversely affected mission performance, and left the organizations that make up the DoD vulnerable to fraud, waste, and abuse. Due to the rigid hierarchical structures and complex procedures that were not designed for a network-driven age, it was not possible to take advantage of new IT capabilities. As IT systems evolve, if used correctly, they can begin to enable processes to be done in different ways.

1. What is Business Process Reengineering?

BPR echoes the long standing belief that there is one best way to perform tasks. In a book written jointly with James Champy, Dr. Michael Hammer defined BPR as:

The fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance, such as cost, quality, service, and speed. (Hammer and Champy, 2001)

BPR is not downsizing, restructuring, reorganization, or automation. It is the examination and change of business components such as strategy, processes, technology, organization, and culture. The capabilities that new technology brings to an organization have both enabled organizations to change and accelerated the need to improve current business processes, many of which were developed before technology became an ever present part of an organization. BPR is not designed for an organization that is looking for a 10 percent improvement; BPR is a radical restructuring of practices. Hammers definition of BPR contains four key words; fundamental, radical, dramatic, and processes.

The first step in reengineering processes is to understand the fundamental operations of the organization. Asking questions related to how an organization operates leads to an understanding of the fundamental operations and to question the old rules and assumptions. In order for a redesign of processes to be radical, all existing structures and procedures must be discarded and new ways of accomplishing the work must be invented. In general, there are three reasons for an organization to undertake reengineering efforts. First are organizations that are in deep trouble and have no choice but to reengineer. The next group is organizations that, due to changing economic

environments, see trouble in the future. Third are companies that are in the peak conditions, where reengineering provides a chance to further their lead over their competitors. The most important concept in reengineering is the process. Most organizations have task-based processes, where tasks could be distributed across multiple departments. A company may have a process for order fulfillment with fragmented tasks such as receiving the order form, picking the goods from the warehouse, and processing the payment that are possibly delayed by crossing departmental boundaries. This thinking needs to shift to process-based thinking to gain efficiency.

2. Information Technology and BPR

Advances in IT system performance are revolutionizing how organizations communicate and what is communicated. Network bandwidth has been growing at a rate of 36 percent per year, a rate that is expected to increase to 43 percent by the end of 2006. (The International Engineering Consortium, October 2002) This growth in bandwidth is fueled by the increased demand for the Internet and network resources. This dramatic growth has resulted in revolutionary new ways of communicating and conducting business, creating a critical issue for today's leaders. IT plays a crucial role in business process reengineering. IT allows organizations to break the assumptions of existing processes, which, due to new capabilities, are no longer regarded as hard and fast rules. It is important however, to remember that IT is only part of the solution in that it allows managers to collect, store, analyze, and communicate and distribute information in a more efficient manner.

In today's global economy, IT enables process automation and increased speed. Traditional assumptions about the physical world no longer apply in a society that is always connected, no matter the distance. IT can also be seen as a detriment to BPR efforts. As a result of poor performance in the past, many organizations feel that IT departments are unable to participate in reengineering due to an inability to do anything in a timely manner, that they lack the advanced technology, or there is not enough technical or organizational knowledge to succeed. Over the past decades, senior managers especially have developed a skeptical attitude about the effectiveness of IT due to the non-performance of many IT systems that delivered little or no business value.

Many IT personnel do not know what the mission of the organization is, they are not involved in day-to-day operations outside the IT arena and therefore, lack the organizational knowledge required to help provide solutions. On the other side, many managers that do not interact with IT do not realize the potential difficulty that exists when attempting to implement an IT solution, and do not place enough emphasis on their efforts at working with IT to find a solution that is effective.

There are two main theories regarding when to involve IT in BPR efforts. While most companies see IT and reengineering as linked, there is some debate as to what role IT should play. While many reengineering efforts are initiated as a result of a perceived IT opportunity, organizations have found that the actual technical solution is often far less important than using IT as both a strategic initiative and as a tool in the reengineering process. That is where the debate occurs, is it better to ignore IT capabilities when developing a reengineering strategy, or should the strategy be built around the capabilities that are enabled by IT. There is no correct answer, while one method may work for one organization; it may not work for another. No matter which method is chosen, it is important that organizations recognize that IT is only part of the solution. Another best practice is to include IT personnel, either internal to the organization or external experts, on the BPR team. This helps create an environment that fully understands the requirements and identify potential solutions, eliminating the need for extensive reviews and revisions. Since reengineering utilizes IT as a utility, after implementation, IT performance should be continually monitored and new capabilities should be explored.

3. BPR Methodology

There are many methodologies that have been developed to assist in reengineering processes. Table 1 summarizes five popular methodologies that are available for use. As with the management frameworks discussed earlier, these methodologies are recommendations and can be used exclusively or in combination with each other.

Methodology #1 (Underdown, 1997)		Methodology #2 (Harrison and Pratt, 1993)	
Develop vision & strategy		Determine customer requirements & goals for the process	
Create desired culture		Map and measure the existing process	
Integrate & improve enterprise		Analyze and modify existing process	
Develop technology solutions		Design a reengineered process	
		Implement the reengineered process	
Methodology #3 (Furey 1993)	Methodology #4 (Mayer and Dewitte, 1998)	Methodology #5 (Manganelli and Klein, 1994)	
Set direction	Motivating reengineering	Preparation	
Baseline and benchmark	Justifying reengineering	Identification	
Create the vision	Planning reengineering	Vision	
Launch problem solving projects	Setting up for reengineering	Technical & social design	
Design improvements	As Is description & analysis	Transformation	
Implement change	To Be design & validation		
Embed continuous improvement	Implementation		

Table 1. Popular BPR Methodologies

The popular methodologies have similar steps that can be combined as five steps; prepare for reengineering, identify and analyze the As-Is processes, design the To-Be processes, implement the reengineered processes, and ensure continuous improvement.

a. Preparing for Reengineering

Reengineering is drastic change, something that all organizations may not need to undertake. A thorough analysis of how an organization operates is necessary to determine whether BPR is really necessary or if programs designed for marginal change,

such as Continuous Process Improvement, is needed. During this stage, an organization should evaluate its current state; how things are done, what changes may be occurring, and what new circumstances exist in the business environment. After this stage, the need for change should be clear, as well as the desired end state or future vision. People are an organizations most valued resource and they should not be left out of reengineering efforts. A communications plan should be developed and communicated to all levels of personnel prior to any reengineering begins. Reengineering efforts can falter when there is not a common understanding about what is happening. Everyone must understand the where the organization is today, where it is headed, and the need for change.

Reengineering efforts require a support structure. It is necessary to identify the personnel who will be responsible for reengineering, outline their responsibilities, and who they will report to. Executive level representation is required on the reengineering team. This will provide an authority that can make people listen and provide the motivational power to make them follow. The team should involve the individuals that either participate in, or manage the process. Team members should possess an understanding of the existing process, but is not an unwavering advocate of it. It is important that the members are able to understand, evaluate, and create alternatives objectively and without prejudice.

b. Identify and Analyze the As-Is Processes

Before any reengineering plans can be made, it is essential that the current or as-is processes are understood. The objective is to identify anything that can prevent the process from achieving the desired results and identify the value adding processes. At this point, the organizations core processes are identified in an attempt to discover the process boundaries. Once the major processes have been defined, it is possible to decide which processes are candidates for reengineering. Once a process has been designated for reengineering, new performance objectives should be formulated, key characteristics are established and potential barriers to implementation should be identified.

Once a process has been chosen, several steps should be followed. There is a need to understand why the current steps are performed. Some proponents of BPR, such as Hammers and Champy, feel that analyzing the current structure can possibly

inhibit the creative process required for designing the new environment; however, this can lead to the failure of a project when steps in the current process are overlooked and forgotten about. After examination of the process there are several items that should be understood; how technology is currently used, how information is currently used, and the current organizational structure should be identified. At the end of this phase, the current process should be compared with the new objectives.

c. Design the To-Be Process

During this phase, one or more alternatives to the current situation are produced, each of which should satisfy the strategic goals of the organization. New technologies are investigated and evaluated for the impact they could have on the process. Benchmarking is an important step in this phase. During benchmarking, the performance of the organization's processes and the processes of other similar organizations are compared in an effort to obtain ideas for improvement. When designing new processes, the BPR team must consider the impact on external process that interact with the reengineered process.

Detailed plans are developed to identify all the necessary details of the reengineered process. The process flow is modeled to illustrate how the workflow will be different. This should be done for several process candidates, which allows the BPR team to select the best possible To-Be scenario.

d. Implementation and Continuous Improvement

Once the previous steps have been completed, the organization is ready to implement the new process and transform. Transformation requires a plan of action that details the migration from the old process to the reengineered one. Different strategies are available and include; a full cutover to the new process, a phased approach, a pilot project, or creating an entirely new business unit. Successful transformation also requires managing behavior as well as structural change. BPR implementation requires the reorganization, retraining, and retooling of business systems to support the reengineered process. Once the transition to a newly implemented process is complete, a cycle of continuous improvement should be started. Any new process is likely to have issues arise that were not known about or planned for, but they must be managed. By

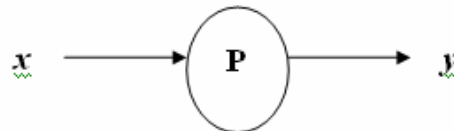
continuously monitoring the new process and investigating possible refinements through the use of a framework like continuous process improvement, it is possible to realize more overall improvement gains.

E. KNOWLEDGE VALUE ADDED

Once a process has been reengineered, it must be applied in real situations and a key concern of management is how to identify the key control factors that allow a business process to achieve maximum performance in a real situation. The Knowledge Value Added (KVA) methodology provides a way to objectively measure the value of knowledge assets that are deployed throughout an organization's core processes. KVA provides a theory and methodology for estimating return on knowledge by using knowledge in people and systems as a method of describing process output in a common unit of measure. KVA analysis produces a return-on-knowledge (ROK) ratio to estimate the value added by knowledge assets.

1. Knowledge Value Added Theory

As illustrated in Figure 13, the theory of KVA is simple enough: $P(x) = y$.



$$P(x) = y$$

Process P is a business process.

If input x is equal to output y , no value has been added by process P .

If input x is changed by process P into output y , value has been added and is $\approx$ change.

Change can be measured by the amount of knowledge required to make the change.

This knowledge $\approx$ the amount of time it takes for an average learner to acquire the knowledge.

So, value added by process $\approx$ change $\approx$ knowledge required to produce the outputs

Housel, T. & Kanevsky, V. (1995) "Reengineering Business Processes: A Complexity Theory Approach to Value Added," *INFOR* 33(4): 251.

Figure 13. Assumptions of KVA (Housel and Kanevsky 1995)

The fundamental assumptions associated with this formula are:

- That in any process (P), there is an input (x), a process (P) that changes the input, and an output (y)

- If the input (x) is equal to the output (y), then the process has added no value
- If a process produces an output that is different from the input, then change has occurred. The amount of change is proportional to the amount of value added by the process. This is the creation of value.
- Change can be explained in terms of the amount of knowledge that it takes to produce that change
- A relationship exists between value and the knowledge required to make change

KVA makes it possible to measure how well a particular process knowledge is doing by converting existing knowledge into value, enabling a determination of how the investment in knowledge is adding to value, not just how much it costs.

2. How KVA Works

Housel and Bell have identified three approaches to simply establish the value of knowledge within an organization. Each approach consists of seven steps, as outlined in Figure 14:

Steps	Learning time	Process description	Binary query method
1.	Identify core process and its subprocesses.		
2.	Establish common units to measure learning time.	Describe the products in terms of the instructions required to reproduce them and select unit of process description.	Create a set of binary yes/no questions such that all possible outputs are represented as a sequence of yes/no answers.
3.	Calculate learning time to execute each subprocess.	Calculate number of process instructions pertaining to each subprocess.	Calculate length of sequence of yes/no answers for each subprocess.
4.	Designate sampling time period long enough to capture a representative sample of the core process's final product/service output.		
5.	Multiply the learning time for each subprocess by the number of times the subprocess executes during sample period.	Multiply the number of process instructions used to describe each subprocess by the number of times the subprocess executes during sample period.	Multiply the length of the yes/no string for each subprocess by the number of times this subprocess executes during sample period.
6.	Allocate revenue to subprocesses in proportion to the quantities generated by step 5 and calculate costs for each subprocess.		
7.	Calculate ROK, and interpret the results.		

Figure 14. Three Approaches to KVA (Housel and Bell, 2001)

Learning time measures how long it takes an “average person” to learn how to complete the function or process correctly. Once the learning time has been determined, it is then multiplied by the number of times that function is performed over a period of

time. Using common units of output allows us to view learning time as a proportion of the amount of knowledge embedded in the process; enabling learning time to be used as a common sense indicator of the amount of knowledge embedded in a given process.

KVA addresses both halves of the Return on Investment (ROI) ratio, net benefit and total cost. The ROI formula is shown below;

$$ROI = \frac{\text{Revenue} - \text{Cost of Investment}}{\text{Cost of Investment}} = \frac{\text{Net Benefit}}{\text{Total Cost}}$$

The numerator (net benefit) represents the amount of knowledge embedded in a process required to reproduce the output and the denominator (total cost) represents the cost to use that knowledge to produce that output.

While the Binary Query Method has been identified as the most accurate KVA approach, this thesis will use the Learning Time method to calculate the ROK in an example of how NMCI provides the capability to reengineer current business practices.

F. ANALYSIS OF THE USMC MORNING REPORT SUBMISSION PROCESS

This section provides an example analysis of a USMC morning report submission process, using a generic Headquarters and Headquarters Squadron from an Air Station as an example. It will show how the KVA methodology and BPR principles can be used to model the As-Is process, capture the value added within the process, and analyze and diagnose the current morning report submission process. All of the core sub-processes involved in the submission of the morning report were examined and evaluated against one another to determine which sub-processes provided the least return on knowledge. It was discovered during the initial stages of research that, due to varying IT support and available systems, there was no standardized submission process and each command defined their own methodology.

1. The As-Is Submission Process

The As-Is submission process flowchart was developed after several interviews with personnel responsible for the submission of morning reports, as well as the researchers personal knowledge. The morning report is a document that identifies the location and status of all Marines and Sailors assigned to a unit. Morning reports are required for every unit throughout the Marine Corps. Each unit has their own standard

operating procedure to follow when completing and submitting their morning report. The basic process is captured in the flowchart, shown in Figure 15.

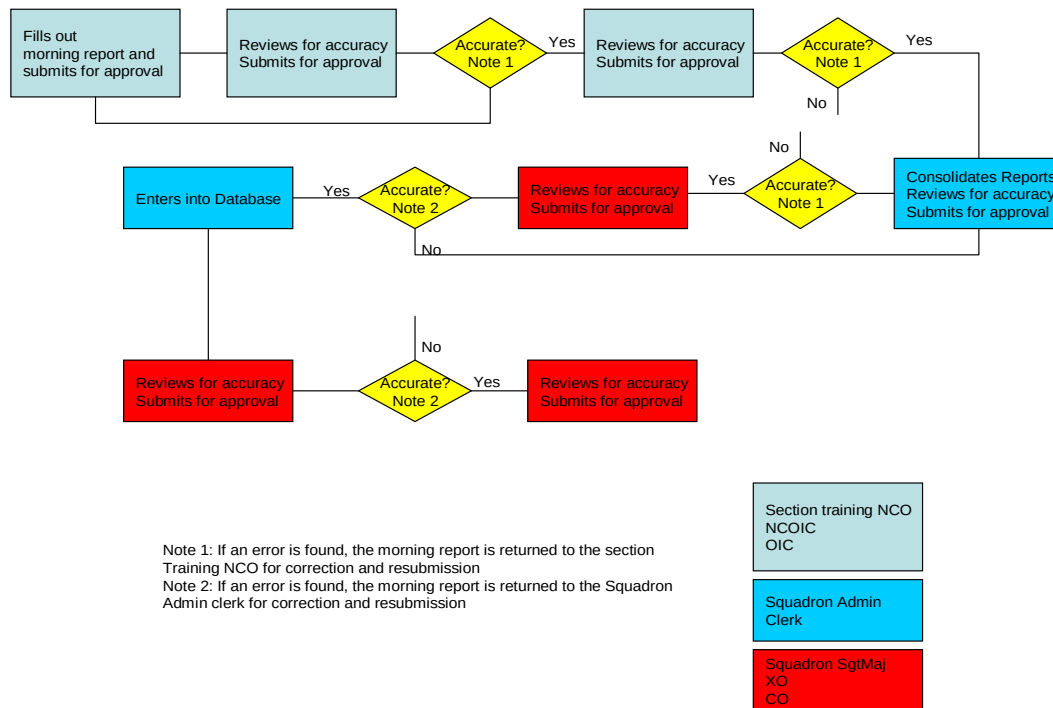


Figure 15. As-Is Morning Report Submission Process

The process is as follows:

1. The section's training NCO is responsible for keeping an up-to-date roster of all Marines and Sailors assigned to that section. This is normally done utilizing a Word document or Excel spreadsheet, that is kept on a local PC under the training NCO's profile. Each morning, the training NCO will update the information kept on the morning report. The report identifies each Marine and Sailor and their duty status (i.e., on leave, limited duty, in custody, etc). Once the document has been updated, it is normally sent via e-mail to the sections NCOIC for their review.

2. The section NCOIC will then check the document for accuracy. If any errors are found, the document is sent back to the training NCO for correction. The section NCO then sends the document via e-mail to the section OIC.

3. The section OIC also reviews the document for errors; however, the copy sent to the OIC is normally for information purposes only. If an error is found, the document is sent back to the training NCO for correction.

4. Once the document has been approved by the section NCOIC, the training NCO sends the document, via e-mail, to the Squadron administrative clerk that is responsible for maintaining the morning report.

5. Once each section has submitted their reports, the Squadron admin clerk will then consolidate the reports, review for accuracy, and submit, again via e-mail, to the Squadron's report to the Sergeant Major for approval. If the Squadron admin clerk finds any errors with the section's submission, the report will be returned to the training NCO for correction.

6. The SgtMaj will then review the report for any errors or omissions before approving the document and forwarding it to the Commanding Officer and Executive Officer.

7. The report is then submitted to the next higher headquarters, to be included in their morning report.

2. Knowledge Value Added Calculations

The Learning Time methodology is one method of applying the KVA principles to a process and is used in this example. Learning time represents the amount of knowledge embedded in a process in reference to the time necessary for an average person to learn how to complete the process correctly. In order to use the learning time method, Housel and Bell recommend a correlation of 80% or higher between the Actual Learning Time and the Nominal Learning Time used in the KVA calculation. If the learning time estimates contain an error or are inaccurate, the correlation will be lower and is an indication that the estimates should be reworked. A high correlation, above 80%, enables the assumption that there is some statistical validity between the two estimates. For this example, the correlation between the nominal learning time (NLT) and actual learning time (ALT) was used to determine the reliability of the estimate.

3. Analysis of Results

To calculate the “benefit” or numerator for each step in the process, the number of units involved in the step was multiplied by the number of people from each section that are involved times the number of times each step was fired/week times the TLT (hours). TLT takes into account the learning time and the percentage of IT that is involved in the step. The “cost” or denominator for this analysis was found by multiplying the number of units involved times the number of people involved per unit times the number of times the step was fired/week/person times the time it takes to complete the step.

Return on Knowledge (ROK) is a measure that brings meaning to KVA analysis. ROK is a performance ration that uses the formula:

$$ROK = \frac{K}{C}$$

Where:

K = Knowledge output generated by a step in the process

C = The cost, or surrogate assigned to represent cost, assigned to Time to Complete a step in the process

The ROK ratios represent the amount of knowledge generated for every unit of “cost” for that knowledge. For example, the first step in the morning report submission example (section training NCO preparation/submission) has a ROK of 40%.

Figure 15 shows the results of the As-Is KVA analysis.

COG	Subprocess	Number of Units Involved	# People Involved (Per Unit)	Times Fired (per Week/person)	Time to Complete (hours)	ALT (Hours)	NLT (Hours)	IT %	TLT (Hours)	Numerator	Denominator	ROK (Revenue / Expense)
Section Training NCO	Preparation / Submittal	20	1	5	0.5	15	12	25%	20.00	2000.00	50	40%
Section SNCO	Review / Approval	20	1	5	0.25	8	5	15%	9.41	941.18	25	38%
Section OIC	Review / Approval	20	1	5	0.25	5	2	15%	5.88	588.24	25	24%
Squadron Admin Clerk	Review / Approval	1	1	5	1	10	15	15%	11.76	58.82	5	12%
Squadron SgtMaj	Review / Approval	1	1	5	0.5	5	2	25%	6.67	33.33	2.5	13%
Squadron Admin Clerk	Database Input	1	1	5	1.5	20	25	75%	80.00	400.00	7.5	53%
Squadron Executive Officer	Review / Approval	1	1	5	0.25	5	2	15%	5.88	29.41	1.25	24%
Squadron Commanding Officer	Review / Approval	1	1	5	0.25	5	2	15%	5.88	29.41	1.25	24%
TOTALS										4080.39	117.5	35%

Figure 16. As-Is KVA Analysis

Analysis of the ROK for the different steps in the process reveals that there are two that stand out as the lowest ROK producing steps and should be considered priorities for reengineering. In this case, the steps involving the Squadron Administration Clerk reviewing and approving the morning report and the Squadron Sergeant Major reviewing and approving the morning report are the two lowest ROK producing steps in this process.

4. The Role of Information Technology in the Process

IT services plays a supporting role to this process. Each step requires IT support in the form of network services (e-mail) or application services (MS Word or Excel). Analysis of the As-Is process shows that the current use of IT services is evidence of a lack of advanced knowledge related to the capabilities of the applications in use. A common sentiment of administrators and clerks is that there is a lack of trust in the network, which when combined with a lack of knowledge related to IT capabilities, results in a process that is not as efficient as it could be.

Once the As-Is analysis has been developed and analyzed, it is possible to develop a proposed To-Be solution. The To-Be process flow and KVA were determined and

developed by conducting research into the capabilities of applications that are identified as “Gold Disk” applications under NMCI and are available to all system users. This thesis does not produce a prototype, only analysis.

5. The To-Be Process

This thesis does not produce a prototype as part of the To-Be analysis, however, after a thorough literature review; the suggested course of action is possible. Figure 17 is a representation of the To-Be process.

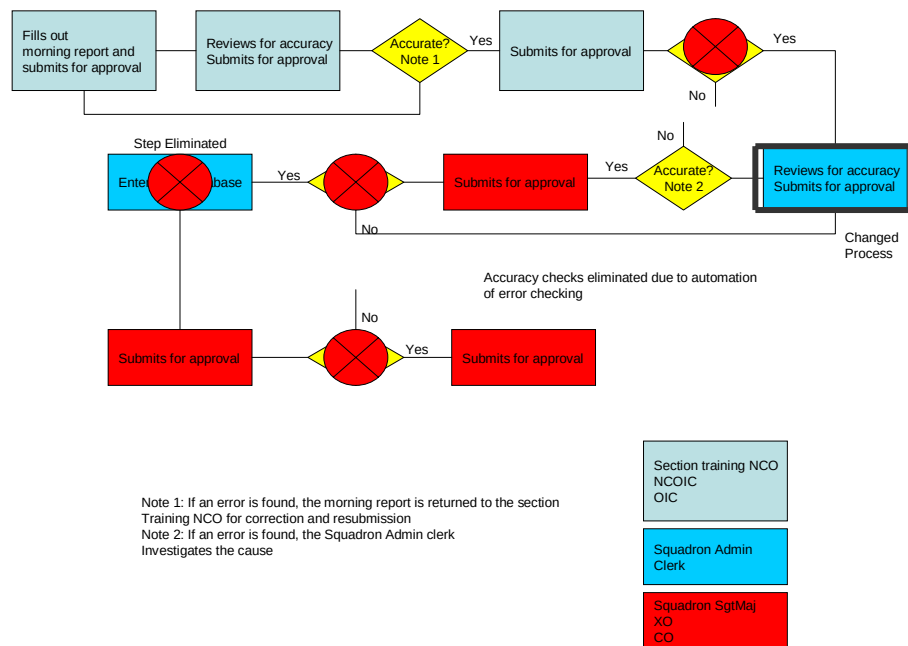


Figure 17. To-Be Morning Report Submission Process

The changed process is as follows:

1. The section training NCO logs into the database, either directly or through a web site, and updates the morning report. Any changes are automatically highlighted, improving accuracy. Once the training NCO reviews the identified changes, the report is submitted, sending an e-mail summarizing the sections report to the NCOIC and OIC.

2. The section NCOIC can then log into the database and review the report or send it back to the training NCO for correction.

3. The OIC receives a daily e-mail from the database with changes related to his/her section highlighted. Since accuracy is greatly improved, there is no need for the OIC to provide verification of the report and that step is removed from the process.

4. Once every section has entered their information into the database, an e-mail is sent to the Squadron Admin Clerk, acknowledging receipt of each section's input. The admin clerk can then log into the system and review all changes. Once they have approved and submitted the report, an e-mail is automatically sent to the Sgt Maj, XO, and CO. Removed from the duties of the Admin clerk is the step requiring the consolidation of each section's report into one report for the Squadron, this is now done by updating one database.

5. Due to increased accuracy, there is no longer a need for the Sgt Maj and the XO to verify the accuracy of the consolidated report. The database automatically sends an informational copy of changes and total numbers to their e-mail account.

6. The CO receives an e-mail stating that the report is ready for his validation. Since the e-mail also contains the current numbers and daily changes, the CO only has to log into the database and approve the report.

Through the use of IT services and BPR principles, recommendations to improve the morning report process have been developed and if implemented could reduce the time it takes to complete the process and improve the accuracy of the report.

6. KVA Comparison

KVA analysis enabled the researcher to identify potential candidate process steps for reengineering. There were two steps that returned low ROK, the Squadron Admin clerk reviewing and approving the report and the Squadron Sgt Maj reviewing and approving the report. Applying the principles of BPR and designing technology into the process enabled the researcher to identify process steps that could be reengineered or removed altogether. The increase in accuracy enabled the removal of most of the accuracy checks as well as the need to consolidate the section's reports and input them into a database. The review and approval of the XO was also removed, due to no value

being added from that step, as well as the ability of technology to provide an update automatically, keeping the XO informed of changes.

KVA analysis of the As-Is process resulted in a ROK of 34%. KVA analysis of the To-Be process resulted in a ROK of 168%. The time of completion was also reduced, from the As-Is time of 5 hours to the To-Be completion time of 1.1 hours. Figure 18 shows the results of the To-Be KVA analysis.

COG	Subprocess	Number of Units Involved	# People Involved (Per Unit)	Times Fired (per Week/person)	Time to Complete (hours)	ALT (Hours)	MLT (Hours)	IT %	TLT (Hours)	Numerator	Denominator	ROK (Revenue Expense)
Section Training NCO	Preparation / Submittal	20	1	5	0.25	5	6	75%	20.00	2000.00	25	80%
Section SNCO	Review / Approval	20	1	5	0.1	3	5	90%	30.00	3000.00	10	300%
Section OIC	Review / Approval	20	1	5	0.1	2	2	90%	20.00	2000.00	10	200%
Squadron Admin Clerk	Database Accuracy Check	1	1	5	0.5	20	15	90%	200.00	1000.00	2.5	400%
Squadron Commanding Officer	Review / Approval	1	1	5	0.15	2	2	90%	20.00	100.00	0.75	133%
TOTALS										8100.00	48.25	168%

Figure 18. To-Be KVA Analysis

There are other benefits that are not measured. One issue is access to the documents when the responsible party is out of the office. Under the current system, since the documents needed for submission reside under their profile on the network, it is necessary to either give out usernames and passwords to whoever is filling in that day or keep multiple copies on multiple machines. Under the To-Be recommendations, there would be a central system that could have two or three Marines authorized access, eliminating the need to keep several copies on different systems. Another benefit is the security and reliability that comes from having the database reside on a network server.

G. CHAPTER SUMMARY

This chapter began by discussing the DoD's business transformation organization, as well as those of the DON and USMC. The definition of Business Process Reengineering was provided, followed by a description of the theory of Knowledge Value Added. For demonstration purposes, the morning report submission process was analyzed using KVA and BPR methodology.

VI. THE REAL OPTIONS APPROACH TO INFORMATION TECHNOLOGY VALUATION

A. INTRODUCTION

This chapter will discuss the theory of the Real Options approach to investing in enterprise architectures. This chapter will compare different options valuation tools, such as the Black-Scholes model and Options valuation and decision tree analysis, and discuss the use of Real Options as integral part of implementing an enterprise architecture.

B. OPTIONS THEORY

Many organizations struggle with decisions related to investment in technology, which are often difficult and complex. Often, organizations find it difficult to align IT with business strategy, particularly in today's global economy, where organizations are being forced to adjust and change at a blinding pace. When business-technology priorities change, IT projects change. Some projects, particularly long-term ones, are slowed or frozen while projects that have a quicker payback period are sped up. Typical valuation approaches, such as Net Present Value or Return on Investment that are used to evaluate many IT projects do not leave room for flexibility in uncertain markets. Many of these approaches require a single, upfront forecast and investment plan and fail to account for the value of change and flexibility. The use of real options can help organizations create a portfolio of options for IT investments, giving executives a set of choices that can be made in response to changing conditions. The real options approach does not make difficult decisions easier, but it does offer a mechanism to manage the risk that is inherent in IT investments over time. Using real options to value IT opportunities, especially in uncertain times, provides flexibility for projects, which can lead to better project valuation, more accurate budgeting, and improved strategic planning.

1. Definition of Options

A option gives the owner the right to buy (call) or sell (put) an asset at a given price within a certain period of time, without the obligation to do so. If the option is not exercised, the only cost is the price of the option, providing large potential with limited risk. This is what gives value to the option, protection from downside risk with the potential of a large upside gain. The option payout is shown in Figure 19 below.

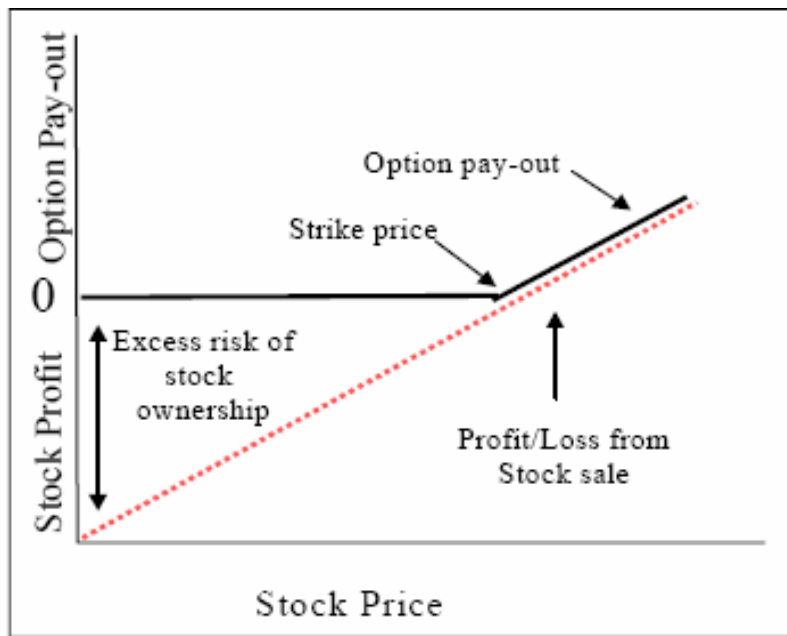


Figure 19. Option Payout (Gaynor and Bradner, 2001)

The value of an option is determined by a number of variables, each of which related to the underlying asset and financial markets:

1) Asset Price; Options are assets that derive value form an underlying asset. As such, changes in the value of the asset affect the value of the option on that asset. An increase in the value of the asset will increase the value of call options, while decreasing the value of put options.

2) Volatility; When an option is purchased, the buyer acquires the right to buy or sell the underlying asset as a fixed price. If there is high variance in the value of the underlying asset, the option's, both calls and puts, value is greater.

3) Dividends; If dividend payments are made during the life of the option, the value of the underlying asset can be expected to decrease.

4) Exercise price; The exercise, or strike price of an option is a key characteristic. The strike price is the price on an option at which the contract may be exercised. As the strike price increases, the value of a call option will decline. The value of a put option will increase as the strike price increases.

Options are also categorized by the time when they can be exercised; American style options can be exercised at any time, up to the expiration date while European style options can be exercised only on the expiration date. The possibility of exercising options early makes American style options more valuable than similar European style options as well as making them more difficult to value.

2. Real Options

Real options is a term defined by Stewart Myers that refers to the application of option pricing theory to the valuation of non-financial or “real” investments, such as multi-stage research and development and manufacturing plants. (Myers and Turnbull 1977) The goal of using real options is to provide insights about organizations and their strategic investments. In financial options, the owner has the right, but not the obligation to purchase or sell a security at a given price; real options give an organization the right, without obligation, to make a potentially value-accretive investment.

Analysis of capital investments involves justification and assessment of the investments and is frequently used as a criterion for decision making and budgeting. Standard methodologies such as discounted cash flow shows how much a project will cost and how much it will return per year and discounts the net based on the organization’s risk adjusted cost of capital. This is a static model that explicitly assumes the project will meet the expected cash flow with no intervention by management, leaving the discount rate to account for uncertainty. This type of valuation methodology takes away a manager’s ability to make decisions as conditions change. Using real options gives the organization the ability to defer, abandon, expand, or contract an investment as needed to provide added value to the organization. Real options provide manager’s with a method of managing risks and uncertainties. Figure 20 below describes types of real options.

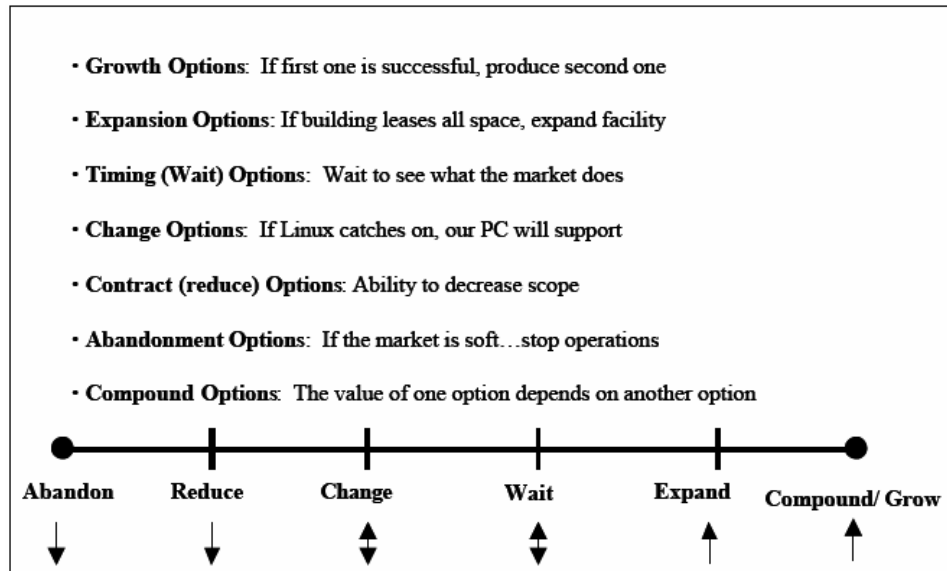


Figure 20. Types of real options (Devaraj and Rajiv 2002)

C. OPTIONS VALUATION TOOLS

There are several valuation methodologies that can be used when analyzing real options, including the binomial model and the Black-Scholes model. The same underlying assumptions regarding value underpin both the binomial and Black-Scholes models.

1. The Binomial Model

The binomial model describes price movements over time, where the asset value can move to one of two possible prices with associated probabilities. The time to expiration is broken into a number of time intervals, or steps. At each step it is assumed that the value will move up or down by an amount that is calculated using volatility and time to expiration. The starting value of the underlying asset is multiplied by the up and down factors to create the binomial lattice, which represents all the possible paths that the value could take during the life of the option. These factors provide a method of determining the change in project value based on different outcomes with up equaling good and down indicating bad outcomes. Figure 21 below is an illustration of a two step binomial lattice.

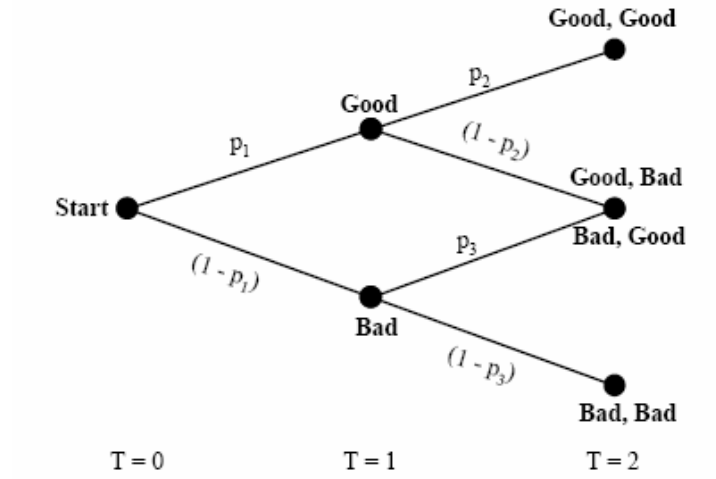


Figure 21. The Binomial Model (Mauboussin 1999)

Binomial models, while not as precise as the Black-Scholes model, are useful in providing a graphical method of understanding the range of alternatives available based on the probabilities of various outcomes. The binomial model is particularly useful when pricing American options since it is possible to check the value at every point in an option's life for the possibility of early exercise.

2. The Black-Scholes Model

The Black-Scholes model uses five key determinants when pricing options: asset price, strike price, volatility, time to expiration, and short-term (risk free) interest rate.

The original formula for calculating the theoretical option price is as follows:

$$OP = SN(d_1) - Xe^{-rt}N(d_2)$$

Where:

$$d_1 = \frac{\ln\left(\frac{S}{X}\right) + \left(r + \frac{v^2}{2}\right)t}{v\sqrt{t}}$$

$$d_2 = d_1 - v\sqrt{t}$$

Figure 22. Black-Scholes formula (Smit and Trigeorgis, 2004)

The variables are:

S = Asset price

X = Strike price

t = time remaining until expiration, expressed as a percent of a year

r = current continuously compounded risk-free interest rate

v = annual volatility of stock price

The most critical parameter for option pricing is volatility. Option prices are very sensitive to changes in volatility, which cannot be directly observed and must be estimated. There are two measures of volatility that affect the pricing of an option. Implied volatility will give you the price of an option; historic volatility will give you an indication of its value. In a simple example, if a forecast of volatility based on historical prices is greater than current implied volatility, the option is undervalued and you may want to buy the option; if the historical forecast is less than implied volatility, it may be time to sell the option.

While volatility plays an important part in determining the fair value of an option, opinions on whether it will go up or down in the future and by how much are completely irrelevant. Also, the expected rate of return of the asset is not a variable in the Black-Scholes model. The implication in this is that the value of an option is completely independent of the expected growth of the underlying asset and is therefore risk neutral. Risk neutral valuation is a key underlying concept in the valuation of all derivatives. The fact that the price of an option is independent of the risk preferences of investors means that all derivatives can be valued by assuming that the return from their underlying assets is the risk free rate.

The main advantage of the Black-Scholes model is that it lets you calculate a very large number of option prices in a very short time. The disadvantage is that it cannot be used to accurately value options with an American-style exercise. This is because it only calculates the value of the option at one point in time, the expiration.

D. TYPES OF REAL OPTIONS

There are two common types of real options that are recognized today, real options on projects and real options in projects. Real options on projects are the most common and are designed to provide opportunities when making capital budgeting decisions during a projects implementation, this type of real option does not consider technical design. Real options in projects provide system engineers with flexibility, or options that are created, throughout a projects design phase, for this type of real option, in-depth knowledge of the underlying technology is essential. Table 2 is a summary of the differences between real options on projects and options in projects.

Options “on” projects	Options “in” projects
Value opportunities	Design flexibility
Valuation important	Decision important (go or no-go)
Relatively easy to define	Difficult to define
Interdependency/Path-dependency is less of an issue	Interdependency/Path-dependency is an important issue

Table 2. Comparison of Real Options On and In Projects

1. Real Options “On” Projects

Real options give an organization the right, not the obligation to invest in a project, making an opportunity equivalent to a call option. In cases of real options on projects, the organization treats the project as a “black box” and values that box. Traditional valuation tools ignore the value of flexibility of a project. Real options on projects allow business decisions that can be implemented flexibly through deferral, abandonment, expansion, or in a series of stages. The types of real options are described below.

- Option to defer. When an organization has the option to defer, it can wait to see if prices justify the proposed investment. This type of option is important in real estate development and industries that extract natural resources.
- Time to build option. Organizations can stage investments as a series of outlays, creating the option to abandon the enterprise midstream if new information is unfavorable. Each stage can be viewed as an option on the value of subsequent stages and valued as a compound option. Organizations that are embarking on long-development, capital-intensive projects often find this type of option useful.

- **Scaling option.** If market conditions change, the organization has the flexibility to respond. When the conditions are more favorable than expected, expand the scale of production. If conditions are unfavorable, reduce the scale of operations. Scaling options are useful to organizations that produce consumer goods and cyclical industries such as construction.
- **Option to abandon.** If market conditions decline severely, organizations have the ability to permanently abandon current operations, allowing them to realize the resale value of capital equipment and other assets in second hand markets. This type of option is useful to capital-intensive industries such as airlines and railroads.
- **Multiple interacting options.** Real-life projects can employ a variety of options that provide protection in down times and can enhance the position of the organization in boom times. This type of option could be useful in all industries.

Prior to employing real options on projects to evaluate a project, an organization first needs to understand what decisions need to be made and ensure that this approach is advantageous over more traditional methods. A framework consisting of six steps can help make this decision. Figure 22 below represents the six steps.

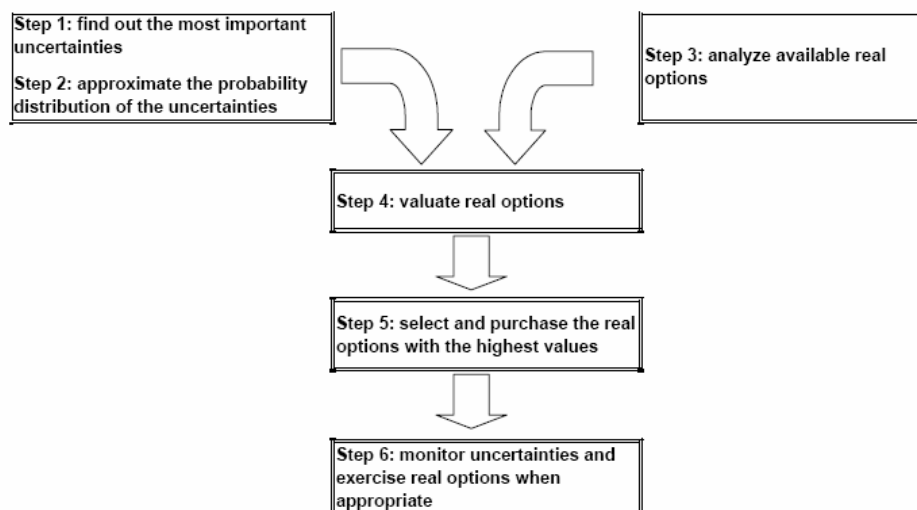


Figure 23. Framework of Real Options On Projects (Wang 2005)

Much like the first step in any framework, the background information is discovered in the first step. This is where the projects drivers and uncertainties should be identified. Uncertainties usually include market risks, such as market demand, price of the product, and what stage of the economic cycle is the market currently in. Technical

risks; can the project be finished on time and if the project can achieve its technical objectives are also researched at this point. Once the uncertainties have been discovered, it is possible to assign approximate probability distribution, which is step two. Step three should identify possible options on the project, such as those listed above. In step four, the appropriate valuation method is chosen and applied to obtain the value of the project options. Options are selected and purchased in step five. This is done by comparing the value of the options and the cost to obtain those options. The final step is to monitor uncertainties and exercise the purchased options when appropriate.

2. Real Options in Projects

While real options on projects treat the system as an entire physical system, real options in projects are created by changing the design of the technical features built into the project or system. In other words, real options in projects provide flexibility to the design and engineering processes. The benefit to using options in projects is evident when a “go” or “no go” decision needs to be made and accurate values are less important. The exact value of the options is not necessary during design and engineering, but it is important to know what options should be designed into the system. One of the difficult aspects when using options in projects is to decide what design variable should be an option. In many systems, there are a great number of design variables, each of which is not necessarily an option in the project. It is difficult to decide where enough flexibility exists in the project and where the options should be designed into the project.

Real options in projects is a newer concept which needs to be further developed. Real options in projects expands the options thinking into the design process for systems, adding flexibility by providing insight into uncertainty. This methodology has the potential to improve engineering and design to better meet customer demands while increasing economical feasibility and profitability.

E. APPLYING REAL OPTIONS TO INFORMATION TECHNOLOGY INVESTMENTS

Unlike traditional valuation methods, real options capture the value created by IT investments that deliver flexibility to an organization in a disciplined manner. Employing options on IT investments can provide an organization with systems that are easily modified or extended in response to changes in that organization. That flexibility

provides insight into value that may be less obvious when using traditional tools that focus on incremental cost reductions or incremental increases in capacity. Many organizations, including the Department of Defense, have begun to take an architectural view of their information systems and supporting technologies in an attempt to measure the business value of their investments. Enterprise architecture development can be viewed as a process of decision making under uncertainty and incomplete knowledge. Embedded in a portion of the value of an enterprise architecture initiative are real options that provide architects with the flexibility to change plans as uncertainties are resolved throughout the life of the project.

The economic value of an enterprise is often influenced by the structure and methodology that is used during the engineering phase. It is often necessary, however, to incorporate flexibility into a project due to changing and uncertain business conditions. Flexibility provides great value to architects and is a desirable characteristic that can both minimize risk and expose the project to opportunities that may arise. Architectures that are designed with flexibility are also in line with the EA Management Maturity Framework published by the General Accounting Office. The fifth stage of maturity in that framework is the capability of being able to leverage EA to manage change. (GAO, 2003) An organization should weigh the cost of incorporating flexibility against the value to make value-maximizing decisions. That cost, however, is difficult to quantify due to potential payoffs occur in the future and are contingent on uncertain and unknown conditions. In order to accurately value flexibility, an organization needs a valuation method that allows comparison of real costs to real value by making the present value of flexibility tangible. This is what traditional methodologies such as net present value fail to accomplish. In order to fully analyze and value flexibility, an organization should employ a real options methodology.

When an IT project allows management to make decisions about the project in response to changing conditions, the projects are embedded with real options and the benefits provided by those options play a critical role in the use of options theory to analyze IT investments. IT system development and implementation often requires mid-course corrections to incorporate new information. Each phase of a project, especially

enterprise architecture projects, is a step at which a decision is required. By allowing for flexibility, an organization is better prepared to address uncertainties in the proposed enterprise architecture. An organization can drastically reduce costs incurred by altering a strategy by making an initial investment in flexibility. Real options analysis is particularly suited for programs and projects characterized by large investments, extended timeframes, significant uncertainties, and a large number of intangible benefits that are subject to rapid deterioration if timing is wrong. IT programs are natural candidates for the real options approach, as they often display all or some of the above characteristics.

F. CONCLUSION

This chapter discussed the Real Options method of assigning value to IT programs. The Real Options methodology as it applies to financial options was provided as a background on what Real Options are. A discussion of methodologies such as the Black-Scholes method and the binomial method was also provided. The chapter concluded by discussing how Real Options can be applied to IT projects.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CASE STUDY OF MARINE CORPS AIR STATION, YUMA ARIZONA

A. INTRODUCTION

This chapter will consist of a case study of the Marine Corps Air Station (MCAS) Yuma, Arizona. It will prepare a business case analysis, similar to the one prepared in 2002, which will compare the costs associated with provision of network services, both pre-NMCI and in an NMCI environment. This case study will not analyze network performance, nor will it include tenant commands of MCAS Yuma, only users directly supported by the MCAS Yuma IT department.

B. MARINE CORPS AIR STATION YUMA, ARIZONA

MCAS Yuma is one of the Marine Corps' premier aviation training bases. Units training at MCAS Yuma have access to over 2.8 million acres of bombing and aviation training ranges, as well as ground training ranges. The weather in Yuma provides for year-round flying, enabling MCAS Yuma to support 80 percent of the Marine Corps' air-to-ground aviation training. Each year, numerous units and aircraft from U.S. and Allied forces travel to MCAS Yuma to conduct training. MCAS Yuma is home to several commands including; Marine Aviation Weapons and Tactics Squadron-1, Marine Aircraft Group-13, Marine Wing Support Squadron-371, Marine Fighter Training Squadron-401, Marine Air Control Squadron-1, and Combat Service Support Detachment-16. (MCAS Yuma 2006)

C. PRE-NMCI ENVIRONMENT

The IT environment at MCAS Yuma supports over 5000 users that are assigned to the following commands:

- Marine Corps Air Station Yuma
- Headquarters and Headquarters Squadron
- Marine Corps Community Services
- Marine Aviation Weapons and Tactic Squadron-1
- Marine Aircraft Group-13
- Marine Wing Support Squadron-371
- Marine Fighter Training Squadron-401
- Marine Air Control Squadron-1
- Combat Service Support Detachment-16

The commands have their own IT departments that are responsible for service provision, user management, computer troubleshooting and repair.

The IT department provides the point of presence and network troubleshooting and assistance for all commands aboard MCAS Yuma. For MCAS Yuma users, including H&HS and MCCS employees, the IT department provides computer and printer repair services. The IT department is responsible for maintaining all outside plant cabling, including fiber optics and copper wire; and the inside plant, from the building entry point to the wall jack. (MCAS Yuma, 2006)

1. IT Infrastructure

The following sections provide a description of the MCAS Yuma network environment.

a. Desktop Computing Environment

The user desktop-computing environment at MCAS Yuma consisted of Intel based processor PC desktops and laptop systems with Microsoft (MS) Windows based operating systems. The standard MS Office package was used as a standard application package on the computers. Specialized software, such as CAD programs, Adobe Acrobat, etc. was purchased as needed according to mission requirements. See Table 2 for a breakdown of operating systems in use during 2002.

Desktop Computing Environment	
Number of PCs	767
Desktop Operating System (% of total PCs)	
- Windows NT v4.0, 2000	68 %
- Windows 95, 98	32 %
Number of Laptops	14
Laptop Operating System (OS) (% of total Laptops)	
- Windows NT v 4.0, 2000	100 %
- Windows 95, 98	-

Table 3. MCAS Yuma Desktop Computing Environment

Among the PCs in use, the majority of which were between three and six years old, there was a mix of manufacturers and capabilities. There was a wide range of processor speeds (between 333 Mhz and 2.0 Ghz), memory (between 64 Mb and 256

Mb), and hard drive size. Personnel that required higher powered machines with greater capabilities, (i.e., increased memory, video capabilities, hard drive, etc) were considered on a case by case basis and most of the upgrades were performed as after-market upgrades. The laptop computers were not utilized as “seats”, they were utilized as needed for temporary use while users departed on official travel.

b. Server Environment

The primary server network operating system aboard MCAS Yuma was Windows NT 4.0. The NT servers hosted all user profiles, file services, a MS-Exchange e-mail system, and application services. There was one Unix based server in operation. Table 3 summarizes the server environment.

Server Environment	
Number of Servers	34
Network Operating System (% of total servers)	
- Windows NT v 4.0	97%
- Other (UNIX, Apple)	3%

Table 4. MCAS Yuma Server Environment

Many of the servers had less processing power than some of the higher-end desktop PCs and the age of the servers varied between two and five years. Servers were upgraded piece by piece, with some being built from the ground up. As with the desktop PCs, there was a mix of manufacturers in operation aboard MCAS. Some of the servers were provided by contractors in support of specific programs, such as the Defense Messaging System and the Hewlett-Packard Openview application. The servers that were provided by contractors tended to be more up-to-date than the servers owned by the Marine Corps.

c. Base Area Network Infrastructure

The MCAS Yuma Base Area Network (BAN) infrastructure was in good condition. A complete renovation of MCAS’s outside plant cabling, inside plant cabling, and upgrade to an ATM protocol had been completed in 2002. The BAN provided services to over 100 buildings located on MCAS Yuma and on a remote site that was provided service by a microwave transmitter and receiver. The outside plant cabling renovation provided 144 strands of fiber optic cabling that connected four nodes that

provided services to nearby buildings, with at least twelve pairs of fiber optic cabling connecting each building and the node. The inside plant cabling renovation provided category 5 twisted-pair cabling and fiber optic cabling to the desktop. The ATM backbone was provided by Enterasys switches, located in newly renovated equipment rooms provided service to the buildings and between nodes.

d. *Peripheral Items and Supplies*

MCAS Yuma maintained a wide range of peripheral items by a multitude of manufacturers. In total, there were over 2,500 peripheral items. There was a central contract that provided networked multi-function devices in each building; however, many personnel retained printers directly connected to their PCs. Consumable supplies were purchased through the Serv-Mart system or open purchase at Office Depot or Staples. These purchases were approved by the individual sections and not assigned as costs to the IT department.

2. IT Support Practices

The IT department consisted of three branches that perform separate activities and duties, however, all branches interface and support one another. The branches, as depicted in Figure 24 below are: Network Services Provision and Repair, Computer Repair, Information Assurance, and the Communications Center.

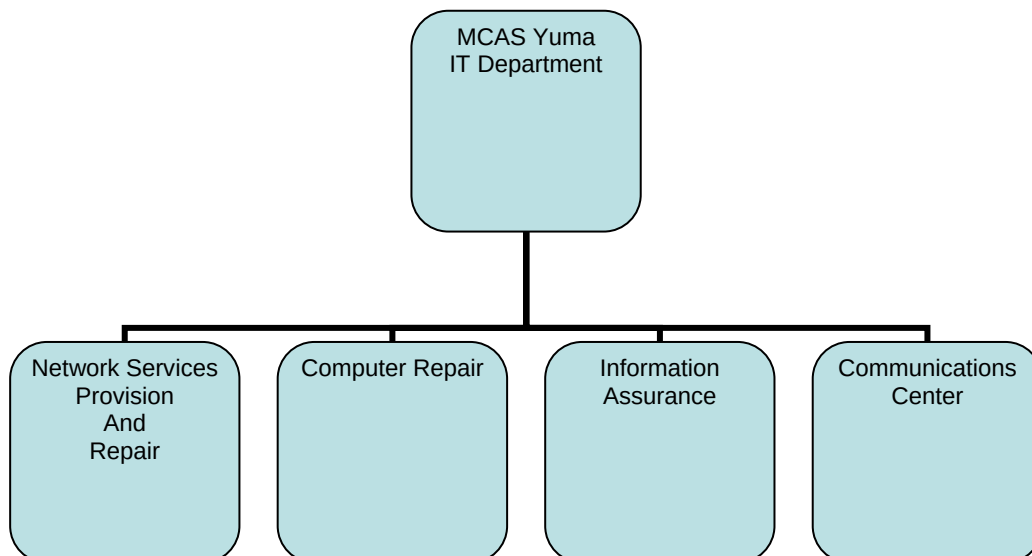


Figure 24. MCAS Yuma IT Department Organizational Structure

The Network Services Provision and Repair Branch performed all network services. This includes ensuring connectivity for global networking services including the USMC intranets [NT and Marine Corps Data Network (MCDN)], DoD intranets, other Federal intranets (e.g., FBI), and the Internet (e.g., WWW and e-mail). The Network Branch monitored and optimized network performance and performed network/circuit quality control testing and evaluation. At MCAS Yuma, the IT Department was responsible for network wiring of buildings (i.e., not phones), complete LAN setup, and LAN administration. Aside from MCAS Yuma units and personnel, IT also provided network support for visiting squadrons through the networks wired into the transient hangars.

The Repair and Software Support Branch conducted personal computer (PC) support functions. This consisted of the management of all information technology assets on the Air Station, with the exception of the tenant organizations. Currently, tenant units obtain repair support from either their parent organizations at Miramar, or their own repair shop. IT support, however, is available on a cost reimbursable basis. Cost reimbursement includes parts only, not labor. Managing Station assets included budgeting, assigning, maintaining and configuring systems, tracking (i.e., licenses, warranties, and inventory), life-cycle management, and customer support. The Repair Branch also performed all troubleshooting and repair of Station PCs.

The Communications Center was responsible for the receipt, processing, distribution and transmission of all classified and unclassified message traffic for all Station and visiting units. Duties include the maintenance of classified material related to message traffic. The Communications Center also maintained the Naval Telecommunications Publications Library. At the time, the Communications Center operated on a 24-hour basis. The Communications Center had begun to convert its message system to the Defense Messaging System (DMS). Upon conversion to DMS and as AUTODIN is phased out the message traffic will become more automated, reducing the need for personnel to be on-site 24 hours a day, seven days a week. The

Communications Center is the only branch within IT affected by wartime activities, during which message traffic can increase as much as three-fold due to the number of classified messages processed.

The Information Assurance branch was responsible for developing and maintaining secure information systems that are effective, interoperable, integrated, and affordable. The Information Assurance branch served as the central point of contact for all matters pertaining to the security and accreditation of the MCAS Yuma non-secure Internet protocol routed network (NIPRNET). Branch personnel were responsible for determining what security controls needed to be in place to protect NIPRNET data and service availability. Other duties included implementing user security awareness training, enforcing security policies and safeguards on all personnel having access to information systems, and verifying that appropriate security tests were conducted and documented.

As of February 2002, there were 32 military personnel devoted to the IT Department. Of the 32, thirteen personnel devoted a majority of their time to Communications Center activities (There were sixteen people assigned to the Communications Center. Thirteen performed Communication Center duties full-time; the remainder supported other IT activities as required). Also included in the 32 total personnel were six Fleet Assistance Program (FAP) personnel, all of whom performed Communications Center activities. The remaining nineteen performed IT business activities as well as administration and overhead activities. Most of the personnel cross-perform in many of the processes identified. Six civilian full time employees, ranging in grade from GS-09 to GS-12 performed IT business activities as well.

3. Pre-NMCI Financial Analysis

The financial analysis consisted of calculating the cost per seat for the 2002 MCAS Yuma computing architecture. For the purposes of this study, a “seat” is defined as either a desktop or laptop computer. All cost amounts are in FY2002 dollars.

a. *Distributed Computing*

The cost for distributed computing was calculated by dividing total annual costs for each element by the total number of end-user seats. MCAS Yuma utilizes a total of 767 desktop PCs, or seats, for which the cost is broken down as follows:

- **Hardware.** Hardware includes all desktops, laptops, servers, peripherals, and network connectivity equipment. The cost per seat for hardware was estimated to be \$1244. This cost reflects the cost to both acquire end-user and support staff desktops and laptops, which were depreciated over a five-year period. The cost per seat of desktops and laptops is \$742. The cost of peripheral items is also included in the hardware category. MCAS Yuma has contracted network printing services to a local vendor, as well as having printers, scanners, and other devices connected to individual workstations. The assorted peripherals add \$139 to the cost per seat. Servers and network connection devices, such as switches and routers, are included in this category and add \$345 to the cost per seat. Consumable supplies include diskettes, CD-RWs, backup tapes, and other supplies for clients, servers, network devices, and peripheral items. The per seat cost for this element is approximately \$15.
- **Software.** Software comprises Commercial Off the Shelf (COTS) client software that supports standard business applications. Client software does not include licensing for client operating systems, as they are included in the purchase price of the client hardware. The cost per seat for software is estimated at \$110.
- **MCAS Yuma annual IT budget.** The annual IT operations budget is almost \$420,000, adding \$547 to the cost of each seat. This budget is used for maintenance of existing systems and training costs.
- **Manpower.** MCAS Yuma has six full time civilian employees assigned to the IT department. There are 32 military personnel that provide IT services. There are also two civilian personnel that provide budgetary and clerical support for the IT department. It is estimated that the six civilian employees spend 75% of their time working on MCAS Yuma related IT projects, accordingly, 75% of their

salaries has been assigned to the per seat cost of MCAS Yuma seats. The two support personnel estimate spending 30% of their time in IT related tasks; therefore, 30% of their salaries are distributed to the 767 MCAS Yuma seats. Manpower costs', including military and civilian employees, adds \$1,886 to the cost of each seat.

b. Wide Area Data Transport

The cost estimates for WAN assume the Defense Systems Information Agency (DISA) provides all wide area services through the life of the contract. DISA employs a two-tiered pricing system for wide area networking. Tier 1 is an amount paid by each Service to support DISA's basic operations. Tier 2 is the actual cost of usage. The June 2000 NMCI DISN/Commercial WAN Service Analysis concluded that the average per seat cost of Tier 2 WAN usage in the pre-NMCI environment was \$129 per seat (in FY01 dollars). This encompassed all costs incurred to transport data between sites, and included DISN and FTS2000 data transport services. Tier 1 cost estimates add an additional \$162 per seat. When elevated to 2002 dollars, the WAN transport costs add a total of \$295 per seat.

c. Cable Plant

The MCAS Yuma outside plant and inside plant wiring had just completed a complete overhaul in 2002. In earlier business case analyses, there was no accurate method available to estimate the cost of the DON cable plant. In this case, since the renovation had just been completed, an accurate measure of cost was provided. The renovation of the cable plant cost approximately \$7M, in FY2002 dollars. Using a 10 year depreciation, which is industry standard for cable plant, the cost of the cable plant adds \$384 per seat.

d. Mandated Requirements

Mandatory requirements, such as Public Key Infrastructure implementation, Federal Records Management, and Defense Information Technology Security Certification and Accreditation Process (DITSCAP) testing are based on DoD and statutory requirements and are included in the price of an NMCI seat. The mandated requirements pre-dated the NMCI initiative and would have been required regardless of the decision to outsource the infrastructure. As a result of some of the costs associated

with the requirements being already budgeted, the value of the mandates is expressed as a range. The low end of the range includes costs that were already budgeted for and the high end being the actual budgeted costs plus estimates of the cost to comply with requirements that were not budgeted for. The cost per seat varies between \$19 and \$750.

4. Pre-NMCI Annual Per-Seat Cost

By adding the four cost elements, an initial estimate of annual pre-NMCI IT environment costs can be made. Dependent upon the cost of providing mandated services, the pre-NMCI per seat costs for MCAS Yuma range between \$4,486 and \$5,217. The cost per seat is higher than the cost identified in the 2002 NMCI Business Case Analysis, which identified an average cost per seat of \$3,545 in the pre-NMCI environment. One of the reasons for the discrepancy is that an accurate estimate of the cable plant was not available for the 2002 NMCI BCA. MCAS Yuma has an accurate cost for the cable plant. As a result, the 2002 NMC BCA identified the cost of the cable plant as \$38 per seat. MCAS Yuma, with an accurate estimate of the cost, has a cost of \$384 per seat.

D. POST-NMCI ENVIRONMENT

The cost data in this case study is based on the actual MCAS Yuma NMCI seat order placed in 2005. There are also additional costs that must be included for an appropriate comparison with the pre-NMCI environment: amortized transition costs, non-contract operating costs, and DISN costs for WAN services. This report will also examine the costs that are still being incurred by MCAS Yuma for maintenance of the legacy network and manpower.

1. The NMCI IT Infrastructure

The NMCI team is responsible for 679 workstations and laptops that are in use throughout MCAS Yuma. Support is provided through the use of a 24x7 help desk that is accessible by a toll free phone number. Remote assistance is provided, if the problem is not solved over the phone, a trouble ticket is sent to MCAS Yuma for NMCI personnel to respond to.

When the NMCI concept was first developed, MCAS Yuma was to have a “micro” server farm that would provide all user management, e-mail, file, and print

services. During the implementation of NMCI, it was decided that a regional server farm, located aboard Camp Pendleton, would provide those services to MCAS Yuma and other sites throughout the Southwestern U.S. After monitoring the traffic and usage of the print server, it has been decided that a print server would be installed aboard MCAS Yuma in an effort to speed up the response time for print requests.

There are 21 support personnel aboard MCAS Yuma; however, the Site Manager and the Information Assurance team also provide support to the logistics base in Barstow California. The MCAS Yuma team provides remote support to Barstow, with occasional trips to Barstow for additional support. No data was provided regarding the percentage of time personnel spend at each site.

MCAS Yuma retains a small legacy network for computers that have not transitioned to the NMCI environment. The current legacy network consists of twenty workstations and sixteen servers. All of the servers are over five years old. The IT department is currently transitioning from the ATM equipment installed in 2002 to a backbone that is capable of gigabyte transport speeds.

There are four civilian personnel and twelve military personnel in direct support of the MCAS Yuma IT department. There are two civilian personnel that provide support as a portion of their duties, which are centered on budgeting and administrative assistance. The communications center has ended 24x7 operations and now provides assistance with the Defense Messaging Service to MCAS Yuma personnel and tenant commands.

2. NMCI Cost Elements

NMCI cost elements include contract costs, such as seat orders and additional Contract Line Item Number (CLIN) orders, and performance incentives.

The NMCI contract specifies prices that include hardware, software, operations, and administration services that are included in the pre-NMCI environment, but at a specified price that is the same for all commands. Also included in the seat price is the cost of meeting the Federal Records Management requirements, DoD PKI security upgrades, DITSCAP testing, 24-hour a day help desks, and required performance

parameters. The total seat order for MCAS Yuma is for 679 PCs at a cost of \$1.95M. Included in this price is the maintenance of servers, peripheral items, and software that comprised a large amount of the cost in the pre-NMCI environment. The cost per seat under the NMCI environment is \$2,870. Currently not included in the cost is a deficiency of nineteen additional seats at a cost of over \$205,000, for which there is no funding at this time. (USMC, February 2006)

An additional cost is the performance incentives that may be received for meeting specific performance and contracting objectives, including: customer satisfaction, information assurance, and small business participation. These costs could amount to an additional \$427 per seat per year if all the criteria are met. To obtain the maximum customer satisfaction incentive, the customer satisfaction rating must be 95% or greater, across the enterprise. If customer satisfaction falls below 85%, no incentive is received. To date, the satisfaction level throughout the Marine Corps has remained around 73%. (NMCI, 2006) To that end, this analysis will not add the possible bonus payments to the NMCI costs.

An estimate is also required for WAN connectivity costs. This report will use the same estimate that was used in the pre-NMCI WAN cost calculations. This will add an additional \$295 per seat, when adjusted for FY05 dollars.

3. MCAS Yuma Site Specific Cost Elements

MCAS Yuma continues to require the services of civilian and military personnel, as well as an Operations and Maintenance (O&M) budget to maintain a legacy network of computers and servers that will not be transitioning to NMCI for various reasons.

MCAS Yuma retains four civilians and twelve military members in direct support roles and two civilians in partial support roles. The costs associated with the military members and civilian employees add an additional \$1151 per seat. This is calculated with the understanding that the civilian employees and military members in direct support can allocate 100% of their time to support the MCAS Yuma network. The two civilians in partial support spend 33% of their time supporting the MCAS Yuma network.

MCAS Yuma is required to maintain a legacy network in order to support allied and U.S. visiting units that are not part of the NMCI network. In order to accomplish this, the IT department is allocated an Operations and Maintenance (O&M) budget of \$132,000, which is equivalent to \$194 per seat. This includes the operation of 16 legacy servers, all of which are over five years old and twenty non-NMCI seats. It is unknown when or if the seats that are not part of NMCI will transition to the intranet.

4. Cost Summary

After adding the NMCI cost elements and the MCAS Yuma cost elements, the total cost to MCAS Yuma in support of IT services is approximately \$4,510 per seat per year. This cost is subject to several items including performance bonuses, which could potentially add an additional \$427 per seat per year to the cost. Another pending issue is the deficiency of 19 seats at a cost of \$205,310 per year. If the performance level increases to the point where the full performance incentive is awarded and the seat deficiency is funded, the total cost per seat becomes approximately \$5,161

E. PRE-NMCI AND POST-NMCI COST COMPARISON

The purpose of this analysis was to compare the costs associated with providing IT services in a pre-NMCI environment with the costs incurred while operating in a NMCI environment. This analysis will compare the costs with those calculated in a 2002 business case analysis, which used seven sites that were operating in an NMCI environment.

The pre-NMCI costs associated with delivery of IT services for MCAS Yuma presented in this analysis are estimated to be between \$4,486 and \$5,217, dependent upon the actual cost of mandated requirements, per seat per year. This estimate is consistent with the pre-NMCI cost estimate developed by the 2002 business case analysis, which identified the pre-NMCI seat cost to be within a range varying from \$2,859 to \$4,620. MCAS Yuma's cost per seat was higher due to an increased value of outside and inside plant cabling, for which the value was known, and higher distributed computing costs.

This analysis found the cost per NMCI seat to be \$3,165 per seat, which is lower than the cost per seat calculated in the 2002 business case analysis. The cost per seat in this analysis does not include incentive payments, which could increase the cost per seat

to \$3,592. This analysis did consider the remaining costs associated with operation and maintenance of the legacy network, which is necessary due to restrictions in the NMCI contract. Operation and maintenance of the MCAS Yuma legacy network requires an additional \$1,345 per seat. This brings the total cost of providing both NMCI and legacy IT services for MCAS Yuma to \$4,510 per seat. There is potential for that cost to increase should customer satisfaction increase and incentive payments begin. The Table below presents a summary of the Pre-NMCI and the Post-NMCI IT environment at MCAS Yuma.

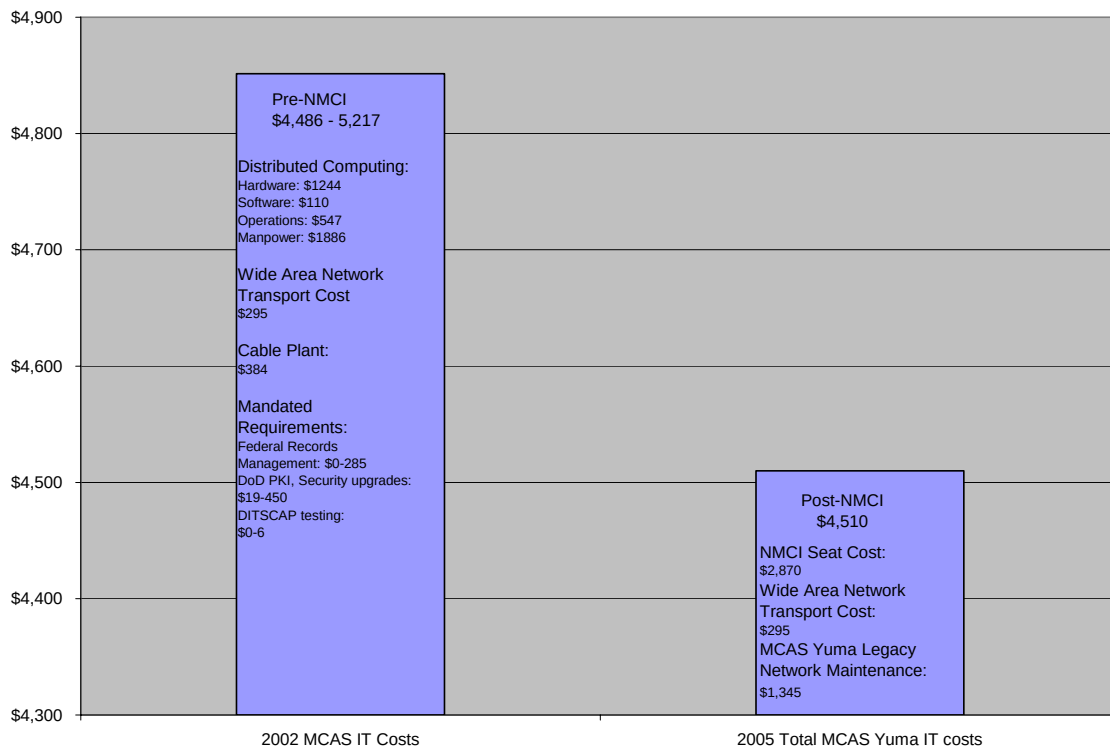


Table 5. Comparison of Pre-NMCI and Post-NMCI Costs

While this thesis did not discuss the subject, the NMCI environment provides additional benefits such as a dedicated 24x7 help desk, increased security, increased reliability, measurable performance, periodic hardware refreshment, and enterprise software upgrades.

F. CHAPTER SUMMARY

It is important to remember that one of the fundamental reasons for contracting IT services throughout the DON was the inability to determine the actual costs for IT

services. Based on the information presented in this analysis, the lower seat costs found in an NMCI environment provide justification that the contract is a financially sound method of obtaining IT services.

VIII. CONCLUSIONS AND RECOMMENDATIONS

A. INTRODUCTION

This thesis explored the efforts of the Marine Corps related to creating an enterprise architecture (EA) to assist in meeting the goals and objectives of the Department of Defense's strategy of transformation, specifically the implementation of the Navy Marine Corps Intranet (NMCI) as a part of the EA. The research conducted for this thesis examined management techniques, such as the use of Real Options methodology to assign value to project flexibility; and management frameworks that are associated with the effective provision of Information Technology services. This thesis also researched the theory and application of Business Process Reengineering (BPR), specifically how IT can enable BPR efforts and how Knowledge Value Added (KVA) provides a methodology of measuring the success of those BPR efforts.

The purpose of this Chapter is to present conclusions and recommendations based on the research effort. The answers to the primary and secondary research questions will be summarized.

B. RESEARCH QUESTIONS

This thesis explored a wide range of issues that are facing current managers of IT. The answers to the research questions will provide a summary of the findings.

1. Creation of the Marine Corps Enterprise Network

How does NMCI facilitate the creation of the Marine Corps Enterprise Network?

In an article that created one of the biggest controversies in years, Nicholas Carr stated that the core functions of IT, data storage, processing and transport, can no longer provide an advantage over an organizations rivals since the capabilities have become available and affordable by all. (Carr, 11 June 2003). The challenge facing organizations today is to create a strategic advantage from a commodity that everyone can possess. By utilizing strong management techniques and tightly controlling costs, that advantage can be created. This is the focus of the efforts associated with the creation of the USMC enterprise architecture.

The Marine Corps recognizes that the efficient management of Command, Control, Communications, and Computers is critical to operational success in the 21st Century. The focus of the Marine Corps Enterprise Network (MCEN) is to create an advantage over its rivals by leveraging IT capabilities to ensure that the right information is available at the right time and place in support of global operations. In other words, the mission of the Marine Corps requires a flexible IT environment that provides the ability to quickly change. An architecture based approach can allow organizations to focus on information needs and business processes by promoting an understanding of how the enterprise operates, which enables better decision making and rapid deployment of changes. NMCI is the solution for providing IT services in a garrison environment and serves as an integral part of the MCEN.

The garrison environment is often overlooked or shortchanged when competing for funds with operational requirements. The USMC created the beginnings of an enterprise architecture, however, the efforts fell short, largely due to funding deficiencies and the “just make it work” attitude. This research has shown that NMCI can provide a cost effective solution to a significant problem, the garrison IT environment, helping to control IT complexity and costs. The pre-NMCI environment consisted largely of individual efforts that did not follow the enterprise effort. This, along with a lack of funding led to an outdated infrastructure that was not prepared to transition to a network centric architecture. In the NMCI environment, costs are tightly controlled, there is standardization of equipment and software, and single purpose, stove piped systems are being replaced. These efforts are aiding the USMC in creating a force that is prepared for the transition to a network centric environment.

IT is only considered successful if it helps an organization to achieve its goals and objectives. NMCI serves several purposes for the Marine Corps. Some of the key benefits of an enterprise architecture include reduced cost of ownership, standardization, and the reduction of investments in duplicative products and services. NMCI, as part of the USMC’s enterprise architecture provides these benefits to the garrison environment.

2. The Information Technology Infrastructure Library

How should the principles of the Information Technology Infrastructure Library management framework be implemented within the MCEN?

The ITIL is probably the most widely accepted approach to IT service management in use today. It provides a comprehensive, consistent and coherent set of best practices for IT service management that promotes a quality approach to achieving effectiveness and efficiency in the use of information systems. Once an organization has decided to adopt ITIL practices, they have to be implemented, which can be a complex project. A common approach to implementing ITIL principles is to take a phased approach. This approach takes into consideration the limitations of resources that can be allocated to the project, while maintaining normal activities. One of the benefits of taking an ITIL approach to IT service management is that standard practices can be implemented throughout the components of the MCEN; including the expeditionary network (eXNET), NMCI, and the Marine Corps Enterprise Information Technology Services (MCEITS).

The steps of a phased approach are as follows:

- Planning and Initiation; This is where the project planning takes place, to include basic steps such as developing a communications strategy and conducting ITIL awareness training. Organizations that are considering implementing ITIL realize that there are procedural problems existing in their IT service management. During this step, the current problems that require resolution are identified, baselined, and prioritized. The Marine Corps is currently in this phase of implementation.
- Implementation; ITIL processes identified in the first step are implemented, according to their priority.
- Integration; Internal procedures should be documented and aligned with the ITIL framework. After that has been accomplished, they should be reengineered for greater effectiveness and efficiency.
- Quality review and continuous assessment; Regular quality reviews of changed processes and continual assessment of relevant performance metrics are conducted to ensure ITIL activities achieve their goal.

3. Outsourcing Best Practices

What outsourcing best practices did the Navy and Marine Corps use when preparing to outsource network services?

This research has determined that when preparing to outsource services, the DON did follow common best practices.

The DON recognized that outsourcing network services would be the largest outsourcing contract to date, thus, use of best practices would be critical to the success of the project. Following industry best practices will help to ensure that the organization achieves cost savings, while at the same time improving service. The DON utilized many of today's best practices during different phases of the NMCI contract.

The DON recognized their lack of experience related to outsourcing contracts of this magnitude and hired an outside contractor that had experience in a variety of sourcing arrangements, specifically related to government contracts. This helped formulate the sourcing strategy that was used to contract NMCI services. In addition to receiving outside help, the DON also contacted other organizations that had made similar sourcing decisions. Due to the size of the project, however, many organizations had undertaken only limited outsourcing efforts when compared to NMCI.

Developing strong relationships between personnel is critical to a project's success. The DON created a NMCI task force that helped to create and define management structure and relationships. Even following a pre-contract communications plan, in many cases members of the NMCI team were viewed as outsiders that were not needed. The NMCI team attempted to remedy this by hiring former DON and USMC members that were knowledgeable of business practices and processes shortly after the contract was awarded.

When preparing to outsource services, it is also important to create a baseline of current services. The Navy attempted to benchmark the current environment but found it difficult to do so. Determining the actual operational costs associated with current operations was difficult due to a lack of centralized control over IT expenditures. The non-standardized environment also created difficulties when attempting to use programs

such as Belarc to discover equipment and software that was in operation aboard many installations. This led to a baseline that was not accurate and caused many problems when attempting to transition to the NMCI environment, eventually requiring a reassessment of the project schedule and Service Level Agreements.

4. Business Process Reengineering

How can the NMCI platform enable the Marine Corps to improve business processes?

Business Process Reengineering (BPR) efforts should not be focused around any specific technology, however, successful BPR requires a stable and consistent IT environment. The pre-NMCI IT environment could be considered a detriment to effective BPR. Legacy systems, non-standard equipment, and different software applications in use throughout the USMC did not provide the consistent environment that allows for BPR. This research has determined that NMCI provides that environment by standardizing hardware and software.

This thesis has shown that under a standardized IT environment, it is possible to begin to reengineer processes that, until now, have not been reviewed. The example of the morning report submission process is evidence of this. In the pre-NMCI environment, there was no standard method of performing this task. One of the main reasons for this was that there was no standard application suite that was available to each user that was took part in this task. In the NMCI environment, there is a standard application suite that is available to all users, regardless of the capabilities of the system hardware capabilities. This standardization enables users to reengineer a process that can be used across the enterprise.

The use of Knowledge Value Added (KVA) to measure the effectiveness of the process enables practitioners of BPR to determine if their efforts are effective. As shown in the morning report example, as a result of a standard IT environment, the effectiveness of the process was greatly improved. KVA is a valuable tool that should be employed during BPR projects.

5. Real Options Analysis

Could Real Options Analysis provide useful insight to the value of IT projects?

This research has shown that the use of Real Options Analysis could prove useful to IT projects.

The development of an enterprise architecture, like the Marine Corps Enterprise Network (MCEN) requires the flexibility to adapt to changing conditions. Real Options on projects provides managers with such options as abandonment, expansion, delay, and temporary suspension. In other words, management has the flexibility to alter decisions as further information becomes available. If future conditions are favorable, a project can be expanded. If conditions are unfavorable, the project can be curtailed or even cancelled to prevent loss.

C. RECOMMENDATIONS

1. Involve NMCI Personnel in Business Process Reengineering Projects

Essential to the success of BPR projects is the involvement of IT personnel. The current contract does not provide for NMCI personnel to be assigned to BPR project teams and the on-site team does not have the amount of staff required to perform this function, however, this should be reconsidered. NMCI team members have extensive IT experience that could prove very useful when reengineering business processes. Creating a team of IT professionals that can work with the different business units throughout the USMC can greatly assist in BPR projects.

2. Develop Standard Information Technology Infrastructure Library Practices to be Used Throughout the Marine Corps Enterprise Network

ITIL can provide repeatable, documented processes that are essential to improving the service delivery and management of IT. Employing standardized practices throughout the MCEN could increase customer satisfaction, while reducing costs for development of procedures and practices throughout the organization.

3. Investigate the Use of Real Options as a Method of Evaluating Strategic Investments in Information Technology Projects

Real Options is a tool that can be used when evaluating strategic investments that involve uncertainty. When combined with an approach such as IT Portfolio Management, it creates a disciplined approach to evaluation of investments without significantly expanding requirements.

LIST OF REFERENCES

1. Association for Federal Information Resources Management, (July 1998). Seat Management: A Federal IRM Perspective.
2. Carr, N. (11 June 2003). Why IT doesn't Matter Anymore. Harvard Business Review.
3. Chief Information Officer Council. (February 2001). A Practical Guide to Federal Enterprise Architecture Version 1.0.
4. Computer Associates International. (June 2004). Federal Enterprise Architecture: Realigning IT to Efficiently Achieve Agency Goals.
5. Devaraj, S. and Rajiv, K. 2002. *The IT Payoff: Measuring the Business Value of Information Technology Investments*. New Jersey, Prentice-Hall, Inc. 2002.
6. Diamond Cluster. (Spring 2005), 2005 Global IT Outsourcing Study.
7. DoD Pamphlet, (October 2005). Business Enterprise Priorities. Retrieved on 15 February 2006 from www.defenselink.mil/dbt/priorities_beps.html
8. DoD. (30 September 2005). Enterprise Transition Plan, Volume I.
9. DON, 2002. "Naval Power 21". *Proceedings*, October 2002. <http://www.chinfo.navy.mil/navpalib/cno/proceedings.html>. Retrieved on 17 October 2005.
10. Furey, T., 1993. A Six Step Guide to Process Reengineering. *Planning Review* 21 (2), 20-23.
11. GAO, (3 March 2004). GAO-04-478T. Information Technology: Improvements Needed in Strategic Planning, Performance Measurement, and Investment Management Governmentwide. Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives.
12. GAO, (April 2003). GAO-03-584G. Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1).
13. Gaynor, M. & Bradner, S. (2001). *The Real Options Approach to Standardization*.
14. Hammer, M. and Champy, J. 2001. *Reengineering the Corporation*. New York, Harper Collins Publishing.

15. Harrison, B. and Pratt, M., 1993. A Methodology for Reengineering Business., Planning Review 21 (2), 6-11.
16. Housel, T. and Bell, A. 2001 *Measuring and Managing Knowledge*. McGraw Hill/Irwin: New York.
17. Housel, T. and Kanevsky, V. 1995. "Reengineering Business Processes: A Complexity Theory Approach to Value Added." INFOR 33(4):251
18. Manganelli, R. and Klein, M., 1994. The Reengineering Handbook: A Step by Step Guide to Business Transformation. New York. American Management Association.
19. Mauboussin, M. (June 1999). Get Real: Using Real Options in Security Analysis
20. Mayer, R. and Dewitte, P., 1998. Delivering Results: Evolving BPR from Art to Engineering.
21. MCAS Yuma, 2006. MCAS Yuma Official Webpage. www.yuma.usmc.mil.
22. Myers, S. and Turnbull, S. 1977 "Capital Budgeting and the Capital Asset Pricing Model: Good News and Bad News," Journal of Finance, Volume 32, 1977, pp. 321-333.
23. NMCI, (April 2002). Interim Updated Business Case Analysis; Cost Analysis.
24. NMCI, (April 2006). NMCI Conformed Contract, Awarded in October 2002.
25. NMCI, 2006. Assessment – SLA's/Customer Satisfaction. NMCI Winter 2006 Enterprise Conference.
26. Onley, D. and Wait, P. 2005. "NMCI Goes for the Save". GCN, June 20, 2005. http://www.gcn.com/print/24_15/36065-1.html Retrieved on March 24, 2006.
27. Public Law 107-347, (2002). The E-Government Act of 2002
28. Ranvijay, S. (August 2005). An ITIL Primer
29. Smit, H. & Trigeorgis, L. (April 2004). Quantifying the Strategic Option Value of Technology Investments.
30. The IT Service Management Forum, (July 2004). An Introductory Overview of ITIL.
31. U.S. Code, Title 40, Section 1401. Clinger-Cohen Act of 1996
32. Underdown, D., 1977. Transform Enterprise Methodology. Unpublished Paper. www.mrc.twsy.edu/enteng/tem.html. Retrieved on February 5, 2006.

33. USMC (May 2004). MARADMIN 226/04. Marine Corps Enterprise Software Portfolio.
34. USMC Briefing, (24 February 2004). Marine Corps Architecture. Retrieved on 10 August 2005 from www.usmc.mil.
35. USMC, (2003). Information Technology: Enabling Transformation For the U. S. Marine Corps.
36. USMC, (2004). C4 Campaign Plan
37. USMC, (25 March 2005). Marine Corps Enterprise Information Technology Services (MCEITS) Strategic Plan
38. USMC, (February 2006). MARFORPAC NMCI Monthly Report.
39. USMC, (January 2006). C4 Strategic CONOPS. Prepared for Brigadier General George Allen, Director C4.
40. USMC, (November 2005). Fiscal Year 2006 Major Command NMCI Budget Allocation.
41. Wang, T. (May 2005). Real Options “in” Projects and Systems Design – Identification of Options and Solution for Path Dependency.
42. Worthen, B. (September 2005). ITIL Power. CIO Magazine.
43. Zachman, J.A., (1987), “A Framework for Information Systems Architecture,” *IBM Systems Journal* 26, no. 3
44. Zittle, Robert. 2006. Interview by Charles Buckley, February 25. Yuma, Az.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

1. Alberts, D., et al, (August 2001). Understanding Information Age Warfare.
2. Alberts, D., et al, (September 2001). Network Centric Warfare; Developing and Leveraging Information Superiority.
3. Alesii, G. (December 2003). Rules of Thumb in Real Options Analysis.
4. Allen, J. (January 2002). Real Options, Real Opportunities; Treating IT Investments Like Stock Options Can Lead to Better Product Valuation, Capital Budgeting, and Strategic Planning. Optimize
5. Booz, Allen, & Hamilton, Inc, (June 1999). Lease versus Buy Analysis for the Marine Corps Systems Command Information Technology Utility Study.
6. Borison, A. (May 2003). Real Options Analysis: Where are the Emperor's Clothes?
7. Boyer, M. et al. (May 2004). Real Options and Strategic Competition: A survey.
8. Bullock, K.F. (June 2003). Navy Marine Corps Intranet: An Analysis of its Approach to the Challenges Associated with Seat Management Contracting (Master's Thesis, Naval Postgraduate School, 2003).
9. Carnegie Mellon Software Engineering Institute, (February 2002). Capability Maturity Model Integration (CMMI), Version 1.1
10. Cebrowski, A. & Garstka, J., (January 1998). Network-Centric Warfare: Its Origin and Future. Proceedings.
11. CIO (September 2005). The Power of Processes. CIO Magazine Retrieved on 2 September 2005 from www.cio.com
12. Cook, G. & Dyer J., (September 2003). Business Process Reengineering with Knowledge Value Added in Support of the Department of the Navy Chief Information Officer. (Master's Thesis, Naval Postgraduate School, 2003)
13. Covert, M., (October 1999). Successfully Performing BPR
14. Dalaklis, D., (March 2004). Monitoring the Progress of the Navy Marine Corps Intranet (NMCI): Implementation, Performance, and Impact. (Master's Thesis, Naval Postgraduate School, March 2004).
15. Damodaran, A. (September 1999). The Promise and Peril of Real Options.

16. Davis, J. (December 2003). Information Technology Portfolio Management and the Real Options Method (ROM): Managing the Risks of IT Investments in the Department of the Navy (DON). (Master's Thesis, Naval Postgraduate School, 2003).
17. DoD Directive 8115.aa, (7 January 2005). Information Technology Portfolio Management
18. DoD Memorandum, (22 March 2004). Information Technology Portfolio Management
19. DoD Memorandum, (3 February 2006). Organization of the Defense Business Transformation Agency
20. DoD Pamphlet, (December 2003). Network-Centric Warfare; Creating a Decisive Warfighting Advantage.
21. DoD, (7 April 2005). Net-Centric Environment, Joint Functional Concept
22. DoD, (December 2004). The Implementation of Network-Centric Warfare.
23. DoD, (March 2001). Report on Network Centric Warfare, Sense of the Report.
24. DoD, (November 2003). Military Transformation, A Strategic Approach
25. DoD, (September 2005). Elements of Defense Transformation.
26. DoD. (15 March 2006). Annual Report to the Congressional Defense Committees, Status of the Department of Defense's Business Transformation Efforts.
27. DON (December 2005). SECNAV Instruction 5000.36A. Department of the Navy Information Technology Applications and Data Management.
28. DON, (2003). FORCEnet Campaign Plan, 2003
29. DON, (2004), Vision Presence Power
30. DON, (February 2005). FORCEnet: A Functional Concept for the 21st Century
31. DON, (January 2003). Naval Transformation Roadmap; Power and Access...From the Sea
32. DON, (June 2005). FORCEnet Campaign Plan.
33. DON, (May 2003). Report to Congress on FORCEnet

34. Evidence Based Research Inc, (November 2003). Network Centric Operations Conceptual Framework, Version 1.0
35. Flatto, J. (Unknown). The Role of Real Options in Valuing Information Technology Projects.
36. GAO, (August 2004). GAO-04-702. Department of Homeland Security; Formidable Information and Technology Management Challenge Requires Institutional Approach.
37. GAO, (February 2003). Contracting for Information Technology Services.
38. GAO, (July 2005). GAO-05-702, DoD Business Systems Modernization, Long-Standing Weaknesses in Enterprise Architecture Development Need to Be Addressed. Report to Congressional Committees.
39. GAO, (April 2003). GAO-03-371. Information Technology: DoD Needs to Leverage Lessons Learned From Its Outsourcing Projects. Report to the Subcommittee on Readiness and Management Support, Committee on Armed Services, U.S. Senate.
40. GAO, (January 2004). GAO-04-49. Information Technology: Governmentwide Strategic Planning, Performance Measurement, and Investment Can Be Improved.
41. GAO, (November 2001). GAO-02-214. Information Technology: Leading Commercial Practices for Outsourcing of Services. Report to the Chairman and Ranking Minority Member, Subcommittee on Readiness and Management Support, Committee on Armed Services, U.S. Senate.
42. GAO, (November 2003). GAO-04-40. Information Technology: Leadership Remains Key to Agencies Making Progress on Enterprise Architecture Efforts.
43. GAO, (8 June 2005). GAO-05-723T. DoD Business Transformation: Sustained Leadership Needed to Address Long-standing Financial and Business Management Problems. GAO Testimony before the Subcommittee on Government Management Finance, and Accountability, Committee on Government Reform, House of Representatives.
44. Graves, G., (September 2005). The United States Navy Reserve Components Account Management Challenge in a Navy Marine Corps Intranet Environment. (Master's Thesis, Naval Postgraduate School, September 2005).
45. Grieser, T., (June 2005). Optimizing Data Center Performance and Building ROI: The TeamQuest Approach.
46. Hagel, J. & Brown, J. (September 2005). The Joy of Flex. CIO Magazine.

47. Hammer, M., (February 1990). Reengineering Work: Don't Automate, Obliterate Harvard Business Review.
48. Holden, T. et al, (1995). KNOVA: Modelling the Knowledge Value-Added Factors that Influence Business Process Performance in Organizations
49. Housel, T. and Bell, A. (2001) Measuring and Managing Knowledge. McGraw Hill/Irwin: New York.
50. Industry Advisory Council. (January 2005). Advancing Enterprise Architecture Maturity, Version 2.0.
51. InterProm USA. (15 December 2002). What is ITIL?. Retrieved 15 September 2005 from <http://www.interpromusa.com>.
52. Joint Staff, (31 October 2005). Net-Centric Operational Environment Joint Integrating Concept.
53. Keppo, J. & Pak, D. (February 2004). A Real Option Approach to Telecommunications Network Optimization.
54. Kulatilaka, N. & Lin, L. (May 2004). Strategic Investment in Technology Standards.
55. Lam, K. A Study of Business Process Reengineering. Retrieved on 13 January 2006 from www.doc.uc.ac.uk
56. Litten, K., (January 2005). Five Steps to Implementing ITIL.
57. Luddy, J., (February 2005). The Challenge and Promise of Network-Centric Warfare.
58. Mayer, R. & deWitte, P., (May 2000). Delivering Results: Evolving BPR From Art to Engineering
59. Municipal Information Systems Association of British Columbia, (September 2004). Best Practices When Implementing ITIL
60. Muthu, S., Whitman, L., & Cheraghi, S., (November 1999). Business Process Reengineering: A Consolidated Methodology
61. NASCIO, (August 2005). IT Management Frameworks: A Foundation for Success. Retrieved on 19 October 2005 from www.nascio.org
62. Niessink, F. (January 2003). IT Service CMM. Retrieved 7 October 2005 from www.itservicecmm.org
63. NMCI, (October 2000). NMCI Contract N00024-00-D-6000.

64. Pink Elephant, (May 2002). The Benefits of ITIL. Retrieved on 11 November 2005 from www.techrepublic.com
65. Rozier, J., (December 2002). An Analysis of Current and Proposed Oversight Processes for the Acquisition of Large Scale Services as Seen Through the Eyes of the Navy Marine Corps Intranet Program. (Master's Thesis, Naval Postgraduate School, December 2002).
66. Saha, P. (Unknown). A Real Options Perspective to Enterprise Architecture as an Investment Activity.
67. Sledgianowski, D & Luftman, J. (April 2005). IT-Business Strategic Alignment Maturity: A Case Study. Journal of Cases on Information Technology.
68. Symons, C. (29 March 2005). IT Governance Framework. Retrieved on 17 October 2005 from www.forrester.com
69. Tech Republic, (January 2005). The Adoption of ITIL in Large Enterprises. Retrieved on 11 November 2005 from www.techrepublic.com
70. The Centre For IT Service Management, (August 2004). Introducing ITIL
71. The Centre For IT Service Management, (August 2004). The ITIL Story
72. The International Engineering Consortium, (October 2002). Business Process Revolution. Retrieved on 13 January 2006 from www.iec.org
73. The International Engineering Consortium, (September 2000). Knowledge Value Added (KVA) Methodology. Retrieved on 17 September 2005 from www.iec.org
74. USMC (April 1999). MARADMIN 146/99. Information Technology Advisory 99-02 USMC Common Component Configurations
75. USMC (March 1998). GENADMIN Message. United States Marine Corps Network Operations Center Interim Concept of Operations.
76. USMC (March 2005). Marine Corps Enterprise Information Technology Services Strategic Plan.
77. USMC (May 2000). MARADMIN 263/00. Information Technology Advisory 00-01 USMC Common Component Configurations
78. USMC (May 2000). MARADMIN 267/00. Information Technology Advisory 00-03 Marine Corps Information Technology Requirements and Acquisitions Policy.

79. USMC (October 2001). MARADMIN 473/01. Revised Information Technology Procurement Approval Process.
80. USMC (September 2000). GENADMIN Message. MCHS Modernization Project/ FY00 Summary and FY01 Objectives.
81. USMC (September 2002). Headquarters, United States Marine Corps Charter For the Information Technology Steering Group.
82. USMC Briefing (20 February 2004). Marine Corps Enterprise IT Services. Retrieved on 10 August 2004 from www.usmc.mil
83. USMC Briefing (2003). Information Technology: Enabling Transformation for the U.S. Marine Corps. Retrieved on 10 August 2005 from www.usmc.mil
84. USMC, (18 November 2004). Marine Corps Enterprise IT Services, Book 1, Introduction to MCEITS
85. USMC, (April 2005). Transformation of C4 Manpower, Equipment, and Structure to Support the 21st Century Marine Corps Study. Prepared by Northrop Grumman Mission Systems.
86. USMC, (February 2003). Business Plan, FY03-04.
87. USMC, (February 2004). Statement by Lieutenant General Edward Hanlon Jr., Deputy Commandant Combat Development United States Marine Corps. Before the Committee on Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, United States House of Representatives. Regarding Transformation.
88. USMC, (March 1999). MARADMIN 123/99. Information Technology Advisory 99-01 USMC Data Management Program.
89. USMC, (March 2004). Testimony of Brigadier General John Thomas, Director, Command, Control, Communications, and Computers, Headquarters, United States Marine Corps and Department of the Navy Deputy CIO for the United States Marine Corps. Before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats, and Capabilities. United States House of Representatives. Regarding DoD Business Transformation Efforts.
90. Violino, B. (21 February 2005). IT Frameworks Demystified. [Network World](#).
91. Violino, B. (25 July 2005). Best-Practices Library Gains Fans. [Information Week](#).
92. Wang, T. & de Neufville, R. (June 2005). Real Options “in” Projects.

93. Weicher, M. et al, (December 1995). Business Process Reengineering Analysis and Recommendations.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Fort Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Marine Corps Representative
Naval Postgraduate School
Monterey, California
4. Director, Training and Education, MCCDC, Code C46
Quantico, Virginia
5. Director, Marine Corps Research Center, MCCDC, Code C40RC
Quantico, Virginia
6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
Camp Pendleton, California