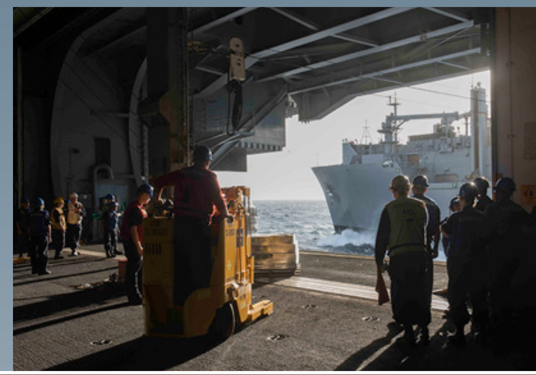
Naval Operational Supply System



ANALYSIS OF ALTERNATIVES

Bradley Wilson
Jessie Riposo
Thomas Goughnour
Mel Eisman
Angelena Bohman
Shane Tierney
Rachel M. Burns

RAND CORPORATION

For more information on this publication, visit www.rand.org/t/RR2403

Published by the RAND Corporation, Santa Monica, Calif.

Preface

The U.S. Navy's operational supply capability is currently supported by several information systems—systems that are antiquated, stovepiped, decentralized, and increasingly expensive to maintain. As a result, the Navy seeks to modernize the afloat and ashore operational supply capabilities to achieve a more-integrated supply system that can provide enterprise-level visibility of supply and minimize sustainment costs.

The Navy asked the RAND Corporation to assist with the Analysis of Alternatives for modernization of the future supply operations program, Naval Operational Supply System. This report discusses the results of that analysis, which was conducted from January 2017 to June 2017. This report should be of interest to those conducting naval operational fleet logistics, as well as analysts and managers of Defense Business Systems.

This research was sponsored by the Navy's Program Manager, Warfare 150, and conducted within the Acquisition and Technology Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

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

Contents

Figures

Tables

Summary

The U.S. Navy operates a 276-vessel battle force, in which each vessel requires a number of supplies for the care and feeding of the crew, the maintenance of the ship, shore-based operations, and operational effectiveness. The Navy uses 16 core information systems to help it manage afloat supply operations for the force. It has indicated that its disparate, antiquated systems have reliability, supportability, maintainability, and affordability problems. Other issues identified relate to the inability to have enterprise visibility into supply operations, cybersecurity demands, and challenges associated with meeting Financial Independent Auditability Review (FIAR) goals.

To address these capability gaps in the existing portfolio of systems and to assist in modernizing them, the Navy asked the RAND Corporation to help in conducting an Analysis of Alternatives (AoA) of its future supply operations program, known as Naval Operational Supply System (NOSS). Our study team relied on a series of qualitative and quantitative methods to evaluate the effectiveness, costs, and risks of proposed alternatives within a six-month period of performance (January to June 2017).

Approach

The AoA was conducted in accordance with the study guidance and the following standard practice for AoAs.[1] The costs and risks of the designated alternatives were each assessed using best practices for cost and risk analyses. Effectiveness was assessed by comparing vendor capabilities with the Navy's high-level requirements. The primary sources of data used for analyses were industry and government responses to a request for information, follow-up discussions with selected industry and government systems, interviews with stakeholders, literature review, study guidance, and study problem statement.

Results

Our results focus on how we identified and refined the alternatives for evaluation based on four alternative areas specified in the AoA. We then evaluated those refined alternatives in terms of effectiveness, costs, and risks.[2]

---

[1] Office of Aerospace Studies, *Analysis of Alternatives (AoA) Handbook: A Practical Guide to the Analysis of Alternatives*, Kirtland Air Force Base, N.M.: Headquarters, Air Force, July 6, 2016.

[2] The schedule is assessed in Chapter 5. There were not adequate data to conduct a full-schedule analysis.

Identified and Refined Alternatives for Evaluation

The AoA specified four alternative areas: Status Quo, Commercial-Off-the-Shelf (COTS), Government-Off-the-Shelf (GOTS), and Hybrid (some combination of the other three). The specified four alternative areas bounded the alternative solution space, but there were many possible variants within each area. The study team used the responses that came back from the Request for Information that was sent out to industry, as well as other discussions with the Navy's Program Manager, Warfare 150, to identify 30 variants of the first three alternatives. The alternative solution space was then refined down to seven alternatives that were studied in the analysis. The study team conducted a preliminary assessment of the level to which requirements could be met by all response offerors and proceeded to analyze only those that met more than half of the requirements. Also, although there were dozens of possible hybrid alternatives, we created two for the analysis. The hybrids were developed to provide additional capability or fill a gap in capability offered by COTS providers. Table S.1 shows the nine alternatives and provides a brief description of each. As shown by the shading, there were two Status Quo alternatives, one COTS alternative, four GOTS alternatives, and two Hybrid alternatives.

Table S.1. Alternatives for Evaluation

Alternative Area	Alternative Name	Alternative Descriptions
Status Quo	1. Status Quo—no modernization	• Baselines current Naval Tactical Command Supply System (NTCSS) • Removes Naval Aviation Logistics Command Management Information System pieces and incorporates others • A total of 16 programs or systems
	2. Status Quo + code modernization and refresh of 16 systems	• Government will continue modernizing Relational Supply • Will expand effort to modernize all 16 additional systems
COTS	3. COTS	• Use separate commercial integrator and software provider, each priced separately
GOTS	4. Leverage Navy Enterprise Resource Planning (ERP)	• Extend Navy ERP architecture to the operational fleet, leveraging existing Navy investments
	5. Leverage Military Sealift Command Logistics Engineering System (MSC LES)	• Extend Navy MSC LES architecture to operational fleet, leveraging existing Navy investments
	6. Leverage Global Combat Support System–Army (GCSS-A) or Global Combat Support System–Marine Corps (GCSS-MC)	• Use GCSS-MC or GCSS-A and extend or integrate into the Navy, leveraging existing U.S. Department of Defense (DoD) investments
	7. Leverage Defense Logistics Agency (DLA)—Defense Property Accountability System (DPAS)	• Extend DPAS to operational fleet, leveraging existing DoD investments
Hybrid	8. Optimize Commercial with Status Quo of Food Service Management (FSM) and Retail Operations Management (ROM) systems	• Keep current FSM and integrate with COTS to mitigate lack of off-the-shelf capability
	9. Forward Compatible Commercial	• Mitigate vendor lock-in by pursuing integration partially based on enterprise service bus, Application Programming Interface Management, or similar technology

Effectiveness Analysis

To assess the effectiveness of the alternatives, we assessed how well the vendor solutions could satisfy the 201 high-level business process requirements. The study team used the vendor self-scores, interviews, and product demonstrations—as well as industry reports—to conduct these assessments. The percentage of requirements that each alternative could satisfy was estimated, shown in Table S.2. As shown in the table, the COTS and Hybrid alternatives are the best performers, satisfying nearly all the high-level requirements. The Status Quo alternatives and the GOTS DPAS alternative meet up to half the requirements; the other GOTS alternatives can satisfy 70 percent to 80 percent of the requirements.

In addition to the high-level business requirements assessment, the study team derived several important quality objectives for NOSS from program documentation and stakeholder engagements. These objectives included the ability to be FIAR-compliant, the ability to pass a security assessment and achieve an Authority to Operate on DoD networks, the ability to operate in a disconnected environment, and the ability to provide an enterprise view of supply operations (the full list of measures is in Chapter 3).[3] Measures of effectiveness were then developed to assess the ability of each alternative to satisfy these quality objectives. Each alternative was scored, with a total possible score of 200.

Table S.2 shows that Alternative 3 and Alternative 9 have the highest scores for quality. Alternative 1 is the baseline and scores the lowest because it does not achieve any of the quality measures, such as enterprise visibility, auditability, cybersecurity, and others. The GOTS alternatives achieve scores from 85 to 126, which are better than the Status Quo alternatives but not as good as the COTS or Hybrid alternatives.

Table S.2. Effectiveness Analysis

	Effectiveness	
Alternative	**Requirements Score (% fully met) (*n* = 201)**	**Quality Score (out of 200)**
1. Status Quo—no modernization	40	0
2. Status Quo + code modernization and refresh of 16 systems	50	51
3. COTS	90–100	155–174
4. Leverage Navy ERP	80	85
5. Leverage MSC LES	70	119
6. Leverage GCSS-A or GCSS-MC	80	126
7. DLA—DPAS	50	92
8. Hybrid Optimize Commercial with Status Quo of FSM and ROM systems	90–100	120–142
9. Hybrid Forward Compatible Commercial	90–100	161–185

Cost Analysis

The risk-adjusted costs of the COTS and Hybrid alternatives are lower than most of the GOTS alternatives and the Status Quo, as shown in Table S.3. Continuing to maintain the current suite of systems or modernizing the current suite of systems—the Status Quo alternatives—are the costliest options. A COTS solution is more affordable than the Status Quo and most of the GOTS alternatives. The Hybrid alternatives are a bit costlier than the COTS alternative.

[3] An *Authority to Operate* is a formal certification granted under the Risk Management Framework process of DoD. The certification permits the Navy, other services, and agencies to operate computing and communications hardware and software systems within the government's enterprise environments.

Table S.3. Risk-Adjusted Costs Relative to the Status Quo

Alternative	Risk-Adjusted Cost: Average LCC Deviation from the Status Quo FYs 2018–2034 (FY 2016 M$)
1. Status Quo—no modernization	—
2. Status Quo + code modernization and refresh of 16 systems	$41
3. COTS	–$180
4. Leverage Navy ERP	–$103
5. Leverage MSC LES	–$219
6. Leverage GCSS-A or GCSS-MC	–$85
7. DLA—DPAS	$9
8. Hybrid Optimize Commercial with Status Quo of FSM and ROM systems	–$147
9. Hybrid Forward Compatible Commercial	–$129

NOTE: FY = fiscal year; LCC = life cycle cost.

Risk Analysis

The biggest source of risk to performance, cost, and schedule for all alternatives is customization of software. The risks associated with COTS and Hybrid alternatives are lower than they are for the Status Quo and GOTS alternatives, as shown in Table S.4. This is because these alternatives are expected to satisfy the requirements with the least amount of customization. The COTS and Hybrid alternatives can meet the majority of the high-level requirements out of the box. This is partly because of the new functionality offered by software vendors, which allows the integrator or user to more easily configure processes and data (as well as interface with other technologies) and have those configurations be more readily compatible with future versions of the software.

Table S.4. Risk Analysis

Alternative	Risk Analysis		
	Performance	Cost	Schedule
1. Status Quo—no modernization	7	1	1
2. Status Quo + code modernization and refresh of 16 systems	5	1	3
3. COTS	2	1	2
4. Leverage Navy ERP	3	2	3
5. Leverage MSC LES	4	1	3
6. Leverage GCSS-A or GCSS-MC	3	1	2
7. DLA—DPAS	3	1	3
8. Hybrid Optimize Commercial with Status Quo of FSM and ROM systems	2	1	2
9. Hybrid Forward Compatible Commercial	1	1	1

NOTE: Red = > 3 high risks; Yellow = 1–2 high risks.

The Status Quo alternatives will never be able to meet certain functional requirements or achieve certain levels of quality. For the Status Quo with code modernization (Alternative 2), there are performance risks and significant uncertainty with respect to the schedule.

The GOTS alternatives present higher risks than the commercial alternatives for a variety of reasons. All the GOTS solutions will require more configuration and customization than their commercial counterparts to fully meet NOSS requirements, which will increase performance and schedule risks. Many of the GOTS solutions would need to achieve the configuration and customization with architectures that are not amenable to forward compatibility, increasing the risk that the Navy would not achieve its objective of a more supportable and maintainable system. Some of the GOTS alternatives have been heavily customized, which can also present risks to performance and cost.

Evaluation of Alternatives

There are many viable alternatives for the Navy to pursue, but none performs as well as the COTS and Hybrid alternatives (Alternatives 3, 8, and 9 in Table S.5), which capture the key findings of the effectiveness, cost, and risk analyses. The COTS and Hybrid alternatives can satisfy the majority of the functional requirements (90 percent to 100 percent); achieve relatively high quality scores (120 to 185 out of 200) at a relatively low cost; and offer the lowest performance, cost, and schedule risks. Status Quo alternatives (Alternatives 1 and 2) and the GOTS DPAS alternative (Alternative 7) are the costliest. The Status Quo alternatives meet only 40 percent to 50 percent of the functional requirements and score very low in quality. The best-performing GOTS alternative (Alternative 6) meets up to 80 percent of the functional requirements and achieves a score of 126 out of 200 for quality, but this alternative is more expensive than the better-performing COTS and Hybrid alternatives.

Table S.5. Summary of Analysis Findings

	Effectiveness		Risk-Adjusted Cost	Risk Analysis		
Alternative	**Requirements Score (% fully met) (*n* = 201)**	**Quality Score (out of 200)**	**Average LCC Deviation From ALT 1 FYs 2018–2034 (FY 2016 M$)**	**Perf.**	**Cost**	**Sched.**
1. Status Quo—no modernization	40	0	–	7	1	1
2. Status Quo + code modernization and refresh of 16 systems	50	51	$41	5	1	3
3. COTS	90–100	155–174	–$180	2	1	2
4. Leverage Navy ERP	80	85	–$103	3	2	3
5. Leverage MSC LES	70	119	–$219	4	1	3
6. Leverage GCSS-A or GCSS-MC	80	126	–$85	3	1	2
7. DLA—DPAS	50	92	$9	3	1	3
8. Hybrid Optimize Commercial with Status Quo of FSM and ROM systems	90–100	120–142	–$147	2	1	2
9. Hybrid Forward Compatible Commercial	90–100	161–185	–$129	1	1	1

NOTE: Red = > 3 high risks; yellow = 1–2 high risks; green = 0 high risks.

Conclusions

The Navy has several viable options, with Alternatives 3, 8, and 9 offering the best performance and the lowest cost, schedule, and performance risks. Within the COTS alternative, there are many potential providers.

The recommendation of the AoA is to move forward with COTS, with a preference for Alternative 9. Both Hybrid alternatives are adaptations of COTS and should remain options for the Navy because their usefulness depends on the specific COTS vendor selected. Alternatives 3, 8, and 9 are not mutually exclusive. If, during source selection, the Navy likes a COTS alternative that assesses solidly in all categories except food service and retail, then the Navy can choose Alternative 8 and maintain support for government-supplied solutions in those areas until a vendor can subsume the food and retail capabilities. If the Navy wants to attempt to mitigate vendor lock-in and give itself flexibility down the road, it can identify a proposal that brings in third-party integration separate from the core functionality provided by the software, as is the case in Alternative 9.

Finally, the risk-adjusted cost estimates for the COTS alternatives (3, 8, and 9) vary significantly. The higher estimates are nearly twice the cost of the lower estimates, with a spread of more than $200 million. This cost range reflects risk and the variety of integrators and vendors available. The Navy has options to manage risk. For example, the Navy can minimize risk by prototyping. Furthermore, ensuring that the requirements are achievable without significant customization can also minimize risk. Ten thousand detailed-level requirements, with many of those functional in nature and lacking specification of quality attributes, could be problematic. Burdensome numbers of requirements and lack of specificity in quality attributes were two reasons why a previous attempt to modernize NTCSS had problems staying on budget and schedule and, ultimately, failed.

Acknowledgments

We would like to thank the Analysis of Alternatives team: Navy study director Kevin Geist of Naval Supply Systems Command (NAVSUP) Business Systems Center, Client Solutions Architects team members Greg John and Bryan Boggs, and Space and Naval Warfare Systems Command 1.6 team members Josh Frazier, Edward Monahan, and Jad Bishara.

We would also like to thank Baron Jolie, who provided thoughtful and focused guidance as the Navy's Program Manager, Warfare 150 sponsor, as well as his colleague, Ken Mackey, who guided us in both engineering and programmatic capacities. U.S. Fleet Forces Command acted as a responsive leader of functional requirements while also providing operational perspectives through Steve Reed, Jim Young, and Jack Norrid. Additionally, excellent operational perspectives were provided by Bill Cording and LCDR Noël Koenig from the NAVSUP Fleet Logistics Command, San Diego.

Thanks are also due to many industry and government representatives who shared time and insight into their systems. Additionally, we would like to thank Joseph Stossel of the Defense Logistics Agency, Mike O'Neill of the Military Sealift Command, and Layne Thompson and Sonja Mooney of Navy Enterprise Resource Planning.

Thank you to our RAND Corporation colleagues, past and present—specifically, Guy Weichenberg, who helped keep the team focused on quality through the duration of the project; Ken Girardini, who brought considerable wisdom and guidance on logistics and software systems in support of logistics commercially and within government; Paul DeLuca, who kept us thinking about improving software system acquisition long term for the Navy; and Carlo Morgano, who provided the team with industry perspective and beneficial reviews of the team's technical approaches and assessments. Finally, thank you to the RAND Corporation's Paul Steinberg, who provided the team with numerous ideas through many iterations of this report.

Abbreviations

ACAT	Acquisition Category
ACS	Agile Core Services
AIMS	Aviation Inventory Management System
AoA	Analysis of Alternatives
APB	Acquisition Program Baseline
APIM	Application Programming Interface Management
ATO	Authority to Operate
BCS	Bar Code Supply
BEA	Business Enterprise Architecture
BPR	business process re-engineering
BY	base year
CAC	Common Access Card
CANES	Consolidated Afloat Networks and Enterprise Services
CMP	Continuous Monitoring Program
COTS	Commercial-Off-the-Shelf
CY	constant year
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DoD	U.S. Department of Defense
DPAS	Defense Property Accountability System
EPS	Electronic Procurement System
E-PUK	Expeditionary Pack-Up Kit
ERP	Enterprise Resource Planning
ESB	enterprise service bus
FACET	Financial Audit Compliance and Enhancement Tool
FAR	Federal Acquisition Regulations
FIAR	Financial Independent Auditability Review
FIMS	Fleet Imaging System
FOC	Full Operational Capability
FSM	Food Service Management
FY	fiscal year
GCSS-A	Global Combat Support System–Army

GCSS-MC	Global Combat Support System–Marine Corps
GOTS	Government-Off-the-Shelf
HICSWIN	Hazardous Inventory Control System for Windows
IAVM	Information Assurance Vulnerability Management
IBS-ONE	Integrated Bar Code System-ONE
ID	identification number
IOC	initial operational capability
LCC	life cycle cost
LCCE	life cycle cost estimate
LOGFAM	logistics functional area manager
MSC LES	Military Sealift Command Logistics Engineering System
NAVAIR	Naval Air Systems Command
NAVSEA	Naval Sea Systems Command
NAVSUP	Naval Supply Systems Command
NOSS	Naval Operational Supply System
NTCSS	Naval Tactical Command Supply System
OIS	Ordnance Information System
PMW	Program Manager, Warfare
R-ADM	Relational Administration Data Management
RFI	Request for Information
RMF	Risk Management Framework
ROM	Retail Operations Management
R-SUPPLY	relational supply
SAMS	SNAP Automated Medical System
SAP	Systems, Applications, and Products in Data Processing
SCM	supply chain management
SHIMS	Submarine Hazardous Material Inventory and Management System
SME	subject-matter expert
SPAWAR	Space and Naval Warfare Systems Command
TY	then year
TYCOM	type command
UI	user interface
USFF	U.S. Fleet Forces Command

1. Introduction

Background

The U.S. Navy currently operates a 276-vessel battle force, in which each vessel requires supplies for the care and feeding of the crew, the maintenance of the ship, shore-based operations, and operational effectiveness. To support these ships and crew, the Navy requires hundreds of shore sites around the world. The procurement, distribution, and accounting of supplies required to operate the Navy are critical functions in supporting the fleet's operational effectiveness.

The Navy currently uses 16 core systems to help it manage afloat supply operations, as shown in Table 1.1. Some of these are no longer supported by commercial vendors or have government ownership. Many are owned and operated by different parts of the Navy. For example, each commodity type, such as food, ammunition, medical, retail, and other commodities, has its own system. Some of these systems support only supply management, while others, such as the Defense Property Accountability System (DPAS), have a supply component but primarily support other functions, such as finance. It is the supply portions of these 16 systems that the Navy would like to modernize and consolidate.

Table 1.1. Core Systems Currently Supporting Afloat Supply Functions

System or Application	Brief Description of System
Relational supply (R-SUPPLY)	Information management system that handles supply, inventory, and financial management for fleet operating forces[a]
Relational Administration Data Management (R-ADM)	Information management system that handles manpower management functions, such as personnel qualifications, watch bills, station assignments, lifeboats, awards, and others
Ordnance Information System (OIS)	Management system that handles supply of ordnance
SNAP Automated Medical System (SAMS)	Management of supply of medical equipment
Expeditionary Pack-Up Kit (E-PUK)	An application that provides the capability to execute detached and deployed expeditionary requisitioning
Aviation Inventory Management System (AIMS)	Management system that handles inventory for aviation
Food Service Management (FSM)	An automated information system for menus, recipes, food preparation, inventory management, procurement, and financial reports
Retail Operations Management (ROM)	Provides Navy Ship Store personnel with a means to maintain accountability of merchandise, track sales, determine profitability, and effectively manage a retail operation[b]
Bar Code Supply (BCS)	Interfaces with R-SUPPLY to extend capability

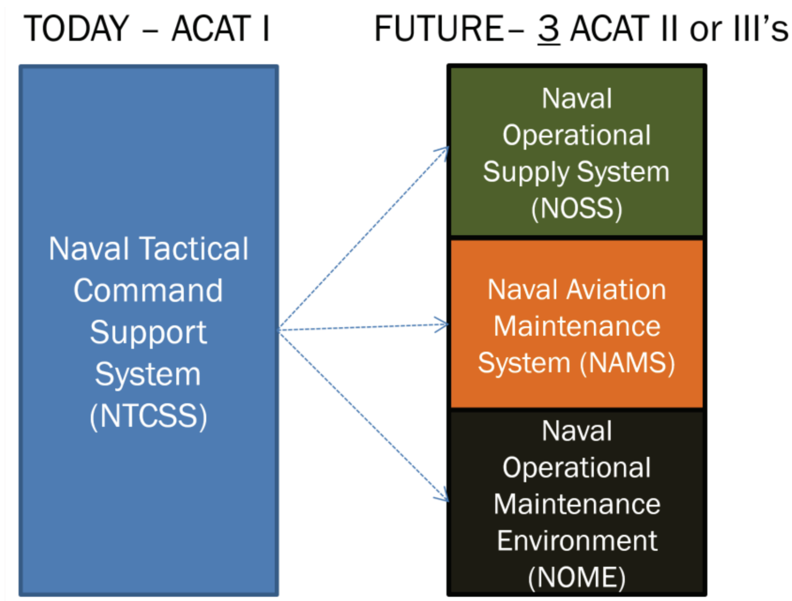
System or Application	Brief Description of System
Integrated Bar Code System ONE (IBS-ONE)	Work-station–based application that enables data collection using a bar code scanner and label printing for automated supply functions
Continuous Monitoring Program (CMP)	A web-based relational database system that provides logistic and financial support to type commands (TYCOMs) and shipboard users
Financial Audit Compliance Enhancement Tool (FACET)	System designed and configured to assist in the processing and archiving of supply-related documents
Hazardous Inventory Control System for Windows (HICSWIN)	Hazardous Inventory Control System used aboard U.S. naval warships
Submarine Hazardous Material Inventory and Management System (SHIMS)	System to help with the management and control of hazardous materials aboard submarines
Defense Property Accountability System (DPAS)	DPAS U.S. Department of Defense (DoD) property management system
Fleet Imaging System (FIMS)	Module of IBS-ONE and the part of the application responsible for automating the management of supply chain documents.

[a] See, for example, Naval Supply Systems Command, *RSupply Unit User's Guide*, NAVSUP P-732, Revision 3, March 31, 2005, p.1-1.
[b] See, for example, Assistant Program Manager–FSM3/ROM3, description of FSM and ROM capabilities emailed to study director, November 21, 2016.

To address challenges in operating the current systems, the Navy wants to restructure the current operational fleet supply system programs, the largest of which is referred to as the Naval Tactical Command Supply System (NTCSS). NTCSS is an Acquisition Category (ACAT) I logistics command-and-control support information system for managing ships, submarines, aviation squadrons, and intermediate maintenance activities (afloat and ashore). Not all of the systems shown in Table 1.1 are a part of NTCSS, but they are all part of the modernization effort for afloat supply operations.

The intent is to modernize NTCSS using an incremental approach (Figure 1.1). The first increment will be to modernize and consolidate operational supply systems into the Naval Operational Supply System (NOSS), which is the focus of this report. The second increment will be to modernize the Naval Aviation Maintenance System, and the third increment will be to modernize the Naval Operational Maintenance Environment. The three new systems have been collectively referred to as the Naval Operational Business Logistics Enterprise.

Figure 1.1. Future of NTCSS



To address these capability gaps, the Navy asked the RAND study team to help conduct an Analysis of Alternatives (AoA) of NOSS to evaluate the effectiveness, costs, and risks of four proposed alternative areas within a six-month period of performance—January 2017 to June 2017. The AoA was conducted in accordance with the study guidance and the standard practice for AoAs.[4] The study team consisted of the study director, Kevin Geist, from Naval Supply Systems Command (NAVSUP) Business Systems Center; our AoA analysis lead; Client Solutions Architects, providing subject-matter expertise, and Space and Naval Warfare Systems Command (SPAWAR) 1.6, providing supporting cost analysis. In addition to the core AoA study team, representatives from the U.S. Fleet Forces Command (USFF)—specifically, Fleet Forces Command Atlantic and Pacific—provided consultation.

Analytic Process

USFF (N41) was the functional lead for NOSS, and Program Manager, Warfare (PMW) 150 was the program manager. USFF conducted high-level business process re-engineering (BPR) exercises with stakeholders prior to the start of the AoA. These 201 high-level requirements were used in the AoA. Concurrent to the AoA, the fleet conducted detailed-level BPR exercises, arriving at approximately 10,000 detailed requirements.

High-level business processes were inputs to the AoA, which focused on analyzing materiel solutions that could best satisfy the process requirements. The study guidance dictated that four

[4] See Office of Aerospace Studies, *Analysis of Alternatives (AoA) Handbook: A Practical Guide to the Analysis of Alternatives*, Kirtland Air Force Base, N.M.: Headquarters, Air Force, July 6, 2016.

classes of material solutions be assessed: continued use of some form of existing systems, referred to as the Status Quo; Commercial-Off-the-Shelf (COTS) technology; Government-Off-the-Shelf (GOTS) technology; and Hybrid options.

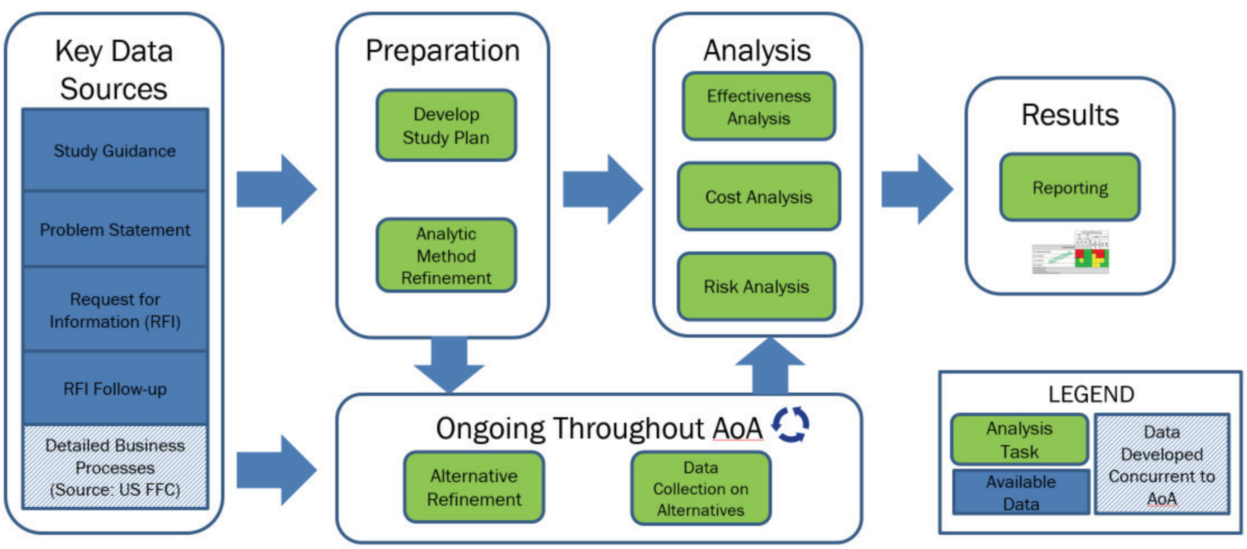
In December 2016, the Navy released a Request for Information (RFI) to help understand how well commercial technologies could meet NOSS requirements; the RFI drew a total of 30 responses. Most responses were from commercial providers, but some were from government program offices. In some cases, government program offices had their current information system contractors help respond to the RFI. The responses to the RFI are discussed in Chapter 2. To validate the responses, the study team met with offerors to discuss the responses and see demonstrations of certain capabilities (e.g., creating or modifying business processes and changing or adding a data field).

Responses to the RFI, the study guidance, and problem statement were primary sources of data for our study. The study guidance provided the ground rules, assumptions, and other guidelines and information necessary to conduct the study. Suggestions were provided on which GOTS to consider. The problem statement provided information on the desired performance measures, enterprise architecture, business process models, and cost-estimating assumptions that had to be adhered to, such as the fiscal year (FY) in which all costs should be presented.

The AoA refined alternatives; developed new data sources; and analyzed effectiveness, costs, and risks. Schedule was assessed as a risk.

Figure 1.2 shows the overall analytic process employed.

Figure 1.2. Analytic Approach



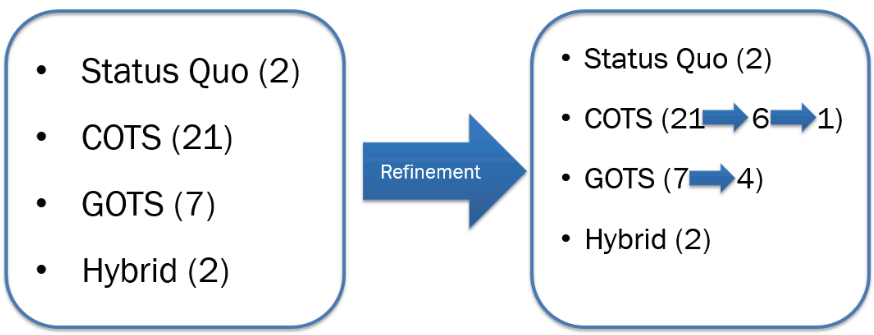
Organization of This Report

Chapter 2 describes the alternatives considered in the AoA. Chapter 3 discusses the effectiveness analyses methodology and results. Chapter 4 presents the cost methodology, assumptions, and rough-order-of-magnitude costs. Chapter 5 discusses the cost, schedule, and technical risks identified. Chapter 6 provides the findings and conclusions of the analyses and presents key considerations for the Navy that were discovered during the study but not directly tied to one of the defined tasks.

2. Alternatives Selected and the Process of Refining Them

As discussed in Chapter 1, the AoA specified four classes of alternatives: Status Quo, COTS, GOTS, and Hybrid (some combination of the other three). The specified four alternative areas bounded the AoA solution space, but there were many possible variants within each alternative area. We used the responses to the RFI that was sent out to industry, as well as material from discussions with PMW 150, to identify 30 variants of the first three alternatives. As shown in Figure 2.1, we used those 30 variants to refine the alternative space down to the first seven alternatives that were studied in the analysis. As also shown in the figure, there were several possible hybrid alternatives; ultimately, we created two for the analysis.

Figure 2.1. Number of Alternatives Considered Initially and After Refinement



The many variants were refined based on their capabilities, the quality of the response information from the RFI, and the relevance those variants had to the NOSS objectives. The solution spaces were refined in various ways. The remainder of this chapter describes the alternatives and the refinement process in more detail.

Status Quo

The Status Quo alternative represents the set of NOSS requirements that are provided within the NTCSS today. Therefore, the Status Quo option considers the afloat supply capabilities currently provided by the total of 16 existing systems, as shown in Chapter 1.[1]

[1] In the case of SAMS, AIMS, and DPAS, NOSS requirements consist only of the supply portion of those systems; therefore, any Status Quo analysis considers only the supply portion of those systems.

Status Quo Refinement

A second Status Quo alternative represents the subset of NTCSS systems but carries forward sunk costs for ongoing efforts to modernize the existing Power Builder base of R-SUPPLY into a more modern language and architecture, thus improving maintainability, cybersecurity, and extensibility. This would add needed capabilities that are not provided within the current system. This second Status Quo alternative also assumes that modernization efforts for the other 15 systems would also occur.[2]

COTS

COTS is defined in the Federal Acquisition Regulations (FAR) as:

> (1) Means any item or supply (including construction material) that is—
>
> (i) A commercial item (as defined in paragraph (1) of the definition in this section);
>
> (ii) Sold in substantial quantities in the commercial marketplace; and
>
> (iii) Offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace.[3]

From the RFI, the Navy received a total of 21 responses from commercial companies, as shown in Figure 2.1.[4] These responses varied widely in product type, functionality, and maturity; the responses are further discussed in the next subsection. However, the majority of responses fell into one of the two following categories:

1. software vendors: companies that develop and build software to be purchased.
2. software integrators: companies that take the purchased software and integrate the software into the Navy's business processes. This includes any configuration or customization needed for specific processes, any interfaces with other Navy systems, and any process improvement or reengineering efforts to align the Navy with built-in system processes.

COTS Refinement

To assess the COTS alternative area, we used data from the top COTS performers to provide a range for comparison. The top six COTS performers were selected based on each alternative's ability to meet the high-level requirements for NOSS.[5] The top performers were sufficiently

---

[2] A third Status Quo alternative was identified, but it was eliminated for lack of viability and therefore is not discussed here.

[3] FAR, Part 2, Definitions of Words and Terms, Subpart 2.101, Definitions, January 13, 2017.

[4] FAR, 2017.

[5] The COTS alternative is based on the COTS that meet the highest percentage of the requirements because, all else unchanged, the Navy would desire to have as many of the requirements as possible met.

similar to allow for aggregation. The COTS alternative offers a range of functionality, which is between the lowest and highest observed in the six. The alternative assumes there is a single systems integrator responsible for implementation and a single software provider that provides the majority or all the desired functionality.

The analysis focused on software systems and their capabilities. However, integration is a key component of the overall acquisition and the team engaged integrators to discuss experiences and risks in implementing some of the selected software vendor's systems. Additionally, the integrators provided cost and risk data, which is presented in subsequent chapters.

GOTS

GOTS is defined here as software products that are currently owned (through license or purchase) and used by the U.S. government. The software could have been developed by the U.S. government or a private company. Specifically, this alternative area evaluates the viability of whether an extension and/or enhancement to existing DoD programs can meet NOSS requirements. All the GOTS products considered provide some form of logistics and/or supply chain management support to the current users.

GOTS Refinement

A total of seven GOTS systems were considered. Only four of those systems performed well enough to be fully assessed for NOSS, as shown in Figure 2.1. Those four systems are Navy Enterprise Resource Planning (ERP), Military Sealift Command Logistics Engineering System (MSC LES), Global Combat Support System–Army (GCSS-A) and Global Combat Support System–Marine Corps (GCSS-MC), and the Defense Logistic Agency's DPAS. Unlike the COTS analysis, the four GOTS systems were considered as separate alternatives because each is unique; specifically, the costs, risks, and effectiveness of each system vary greatly.

Navy ERP

Navy ERP is being assessed to satisfy NOSS requirements for a number of reasons. To begin with, Navy ERP is the current

> Financial System of Record and Single Supply Solution for six Naval Systems Commands, including Naval Air Systems Command (NAVAIR), Naval Supply Systems Command (NAVSUP), Space and Naval Warfare Systems Command (SPAWAR), Naval Sea Systems Command (NAVSEA), Office of Naval Research (ONR), and Strategic Systems Programs (SSP).[6]

[6] Navy Enterprise Business Solutions, *Navy ERP Request for Information: COTS Solution to Meet Naval Operational Supply System (NOSS) Requirements*, January 31, 2017.

Navy ERP provides "financial, acquisition, supply chain, and workforce management capabilities via a single sign on utilizing [Public Key Infrastructure/Public Key Enabling] PKI/PKE technology.[7]" In other words, it provides an enterprise capability. The system supports some Navy logistics functions ashore and is the system through which the Navy plans to achieve auditability, a key requirement for NOSS. There are currently 62,000 users worldwide.

There are also several potential challenges to using Navy ERP. The system was developed on a Systems, Applications, and Products in Data Processing (SAP) COTS platform with Navy Program Executive Office, Enterprise Information Systems as the systems integrator using various contractors. Although the Navy ERP platform is SAP-based, it has undergone significant customization that makes it challenging to maintain and modernize. The Navy ERP also cannot currently meet some of the key requirements for NOSS. Specifically, Navy ERP does not currently offer a detached capability and cannot support cross-domain solutions. To add these capabilities would require an uncertain amount of development effort.

MSC LES

MSC LES is the logistics management program for the MSC. It is "an integrated application suite" of afloat and ashore systems that allow users to perform maintenance and logistics tasks to meet requirements.[8] MSC LES is a government-owned and government-developed system of systems with more than 14,000 users. Specifically, MSC LES's Shipboard Configuration Logistics Information Program (ShipCLIP) and Shipboard Automated Maintenance Management system are viable options for NOSS. ShipCLIP does supply chain management, including FSM, while Shipboard Automated Maintenance Management manages maintenance. MSC LES also offers a disconnected operations capability that is required for NOSS and is competitive on cost.

However, the platform cannot satisfy other NOSS requirements (e.g., forecasting and filtering demand data) and has had problems in the past with providing an accurate picture of spare parts. A DoD Inspector General report found challenges with management of spare parts because "MSC staff [did] not ensure the contractor complied with contract provisions on excess government property."[9] This resulted in an inaccurate count of excess spare parts.

---

[7] Navy Enterprise Business Solutions, 2017.

[8] Military Sealift Command, N4 Logistics, *Request for Information: COTS Solutions to Meet Naval Operational Supply System (NOSS) Requirements*, February 3, 2017.

[9] Inspector General, U.S. Department of Defense, *Military Sealift Command Oversight of Excess Spare-Parts Inventory and Purchases for Sealift Program Roll-On/Roll-Off Ships Needs Improvement*, DODIG-2014-106, September 9, 2014, p. i.

GCSS

GCSS-A is the program of record for management of supply operations for the Army. It is a web-based logistics and financial SAP ERP system.[10] It consists of two components, the first of which is the ERP, which "manages the flow of logistics, resources, and information to meet the Army's modernization requirements."[11] The second component, Army Enterprise Systems Integration Program, "integrates Army business functions by providing a single source for enterprise hub services, business intelligence and analytics, and centralized master data management across the business domain."[12] GCSS-A currently has 20,000 users, with the first group of users using the program in the first quarter of FY 2016.[13] Northrop Grumman is the prime contractor responsible for the integration of GCSS-A.[14]

GCSS-MC is the Marine Corps' program for management of logistics and supply operations. It is based on an Oracle web-based ERP system for logistics chain management (Oracle's 11i E-Business Suite). GCSS-MC "is a portfolio of systems that supports logistics elements of command and control, joint logistics interoperability, and secure access to and visibility of logistics data."[15] GCSS-MC Increment 1 achieved full deployment in December 2015, with approximately 36,000 users.[16]

Both GCSS-A and GCSS-MC are large global ERP systems with the similar functionality that NOSS requires. They are platforms that manage resources, logistics, and information from the theater level to headquarters, which is why they are assessed for NOSS. NOSS could attempt to integrate with the existing processes and hosting solutions, sit as a separate instance beside the existing solution in a common hosting environment, or exist as a clone within its own NOSS enclave. In any of these cases, the Navy can attempt to leverage existing investments within DoD. However, both GCSS-A and GCSS-MC are still being procured and have levels of customization (which the programs have indicated are necessary). It is unclear how much customization has been done, how many processes require customization, or how much remediation is necessary to make the process work "out of the box." Without further analysis, this AoA cannot determine the alignment of existing processes to those that are being proposed through the detailed BPR effort. What is known is that GCSS-A has opted against using the SAP

---

[10] Northrop Grumman, "Global Combat Support System–Army," webpage, undated.

[11] U.S. Army Acquisition Support Center, "Global Combat Support System-Army (GCSS–Army)," webpage, undated.

[12] U.S. Army Acquisition Support Center, undated.

[13] U.S. Army Acquisition Support Center, undated.

[14] Northrop Grumman, undated.

[15] Defense Acquisition Management Information Retrieval, *Major Automated Information System 2016 Annual Report, Global Combat Support System-Marine Corps Logistics Chain Management Increment 1*, Washington, D.C.: U.S. Department of Defense, March 2016, p. 5.

[16] Defense Acquisition Management Information Retrieval, 2016.

Supply Chain Management (SCM) module and has instead customized SAP's ERP Central Component material requirements planning module. However, not all of this code is necessarily applicable to NOSS and some might be duplication. GCSS-MC has customized in the areas of inventory tables, reports, and interfaces.

DPAS

DPAS is a DoD property management system that consists of four major modules: property accountability; maintenance and utilization; material management; and warehousing. DPAS has satisfied many of the security requirements of NOSS and provides logistics management functionality. It is a web-based, Common Access Card (CAC)-enabled system hosted by Defense Information Systems Agency (DISA) servers. The program is managed by the Defense Logistics Agency (DLA) and serves all military branches and more than 25 defense agencies. DPAS has more than 8,000 users and manages more than 2 million assets worth more than $672 billion.[17]

Although there are many potential benefits to using DPAS, the system is customized, which means that changes or modifications to the system require additional customization, not just configuration or formatting. This presents a risk to the Navy's supportability and maintainability goals. DPAS is owned and operated by the government but is currently managed by a contractor. The system has a customized data replication process used to transmit data between afloat and ashore units. Changing fields in the system to meet NOSS requirements would be a customization effort and this would likely introduce version compatibility issues.[18]

Other GOTS options that emerged in our study or were suggested in the study guidance were either deemed not viable or already covered by the COTS alternative. Although Navy ERP and GCSS are based on COTS technology, they were left as GOTS options because they carried customizations implemented for the government customer.

Hybrid

The Hybrid options emerged as the study progressed. They are based on the same COTS options that were assessed in the COTS alternative—and they did not result in point solutions but rather in a range of alternatives. We identified areas where the majority of providers identified shortfalls, such as with FSM and ROM, and where unique technical solutions could help mitigate some of the known risks.

---

[17] Defense Logistics Agency, *RFI Response: COTS Solutions to Meet Naval Operational Supply System (NOSS) Requirements*, February 17, 2017.

[18] Program Manager, Defense Property Accountability System, Defense Logistics Agency, interview with the authors, Arlington, Va., May 22, 2017.

Alternative 8 Concepts

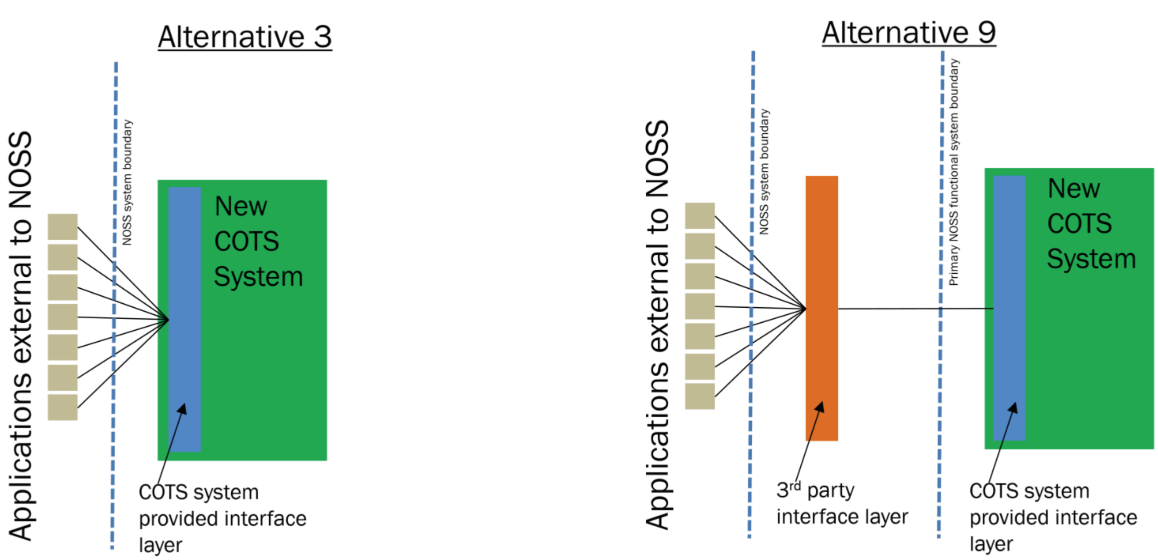
Alternative 8 was created as an optimized COTS option where selected requirements that seemed weakly met by COTS would be bolstered by existing (Status Quo) systems. Although some vendors indicated that they could meet the full range of NOSS requirements, most did not offer the full range of current FSM or ROM capabilities in the Navy. In this alternative, the FSM and ROM software currently employed by the Navy would remain in service. The existing software would be integrated with new software that provides the other functional capabilities desired by NOSS.

Alternative 9 Concepts

Alternative 9 was created as a way to mitigate prominent risks—the challenges of integrating 16 systems into NOSS until Full Operational Capability (FOC), the challenge of integrating across disparate fleet assets, and mitigating vendor lock-in. These options emerged as ways to mitigate some of the risks identified in other options.

The primary difference between the COTS alternative and Alternative 9 is the addition of a third-party interface layer designed to both mitigate challenges in integrating legacy applications and give the Navy flexibility in forward-compatibility. Figure 2.2 shows one way to view the difference.

Figure 2.2. Comparison of Alternative 3 (COTS) and Alternative 9 (Second Hybrid)



The two pieces of Alternative 9 are Application Programming Interface Management (APIM) [19] and enterprise service bus (ESB). APIM is not the same concept as ESB, although

---

[19] Paolo Malinverno and Mark O'Neill, *Magic Quadrant for Full Life Cycle API Management*, Stamford, Conn.: Gartner, October 27, 2016.

they do share features. APIM is primarily about exposing data and services through managed interfaces ready for consumption both internal and external to NOSS. ESB is primarily about exchanging data through defined adapters.

Our market research has shown that not all ESBs are the same. Historically, ESBs have been rigid and centralized concepts that are part of a top-down transformative organizational plan. These ESBs seem to be obsolescing. Modern ESBs seem to be evolving into lightweight solutions that run on nonspecialized hardware.

It would be useful to apply the ESB concept to help mitigate integration challenges with existing systems. However, the integration solution must be lightweight and easily deployed to realize a return on the investment, considering the legacy applications will be replaced by COTS options by the date of full deployment.

Some vendors will provide a service-oriented concept with an in-built ESB or APIM within their proposed solutions. Incorporating these technologies from a third party is likely to be a better long-term option for the Navy, for reasons discussed in the next section. Third parties might include open-source licensed options, as well as Navy Electronic Procurement System (EPS) and Consolidated Afloat Networks and Enterprise Services (CANES) Agile Core Services (ACS). However, it is unclear how much can be leveraged from EPS and CANES ACS. The NOSS source selection should consider a comparison of EPS, ACS, commercial specialists, and integrated solutions from the large vendors.

Mitigating Vendor Lock-In

An article in the journal of the Association for Computing Machinery discussing the shift away from custom development toward COTS solutions noted the most fundamental principle of software selection is that purchasing software means joining the software's network.[20] Software networks have pros and cons, but one particular con that has consistently challenged DoD is referred to as "the opportunistic actions of profit maximizing software producers"; the article reports that

> organizations should keep their options open by buying packaged software that is close to compatible standards; and if they are already using proprietary standard packages, they should keep their eyes open for gateway standards as a way to break an existing lock-in to a proprietary extension.[21]

The best time to consider an exit strategy for any software solution is before buying it.

The primary strategy within Alternative 9 is to give the Navy flexibility to mitigate potential lock-in, and leverage emerging gateway standards, such as those in APIM. The Navy could procure company A's software for business logic but also procure a third-party system to provide

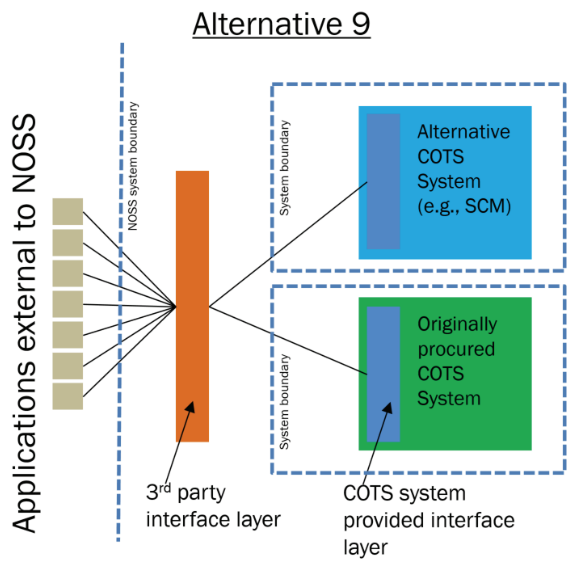
---

[20] Jan Damsgaard and Jan Karlsbjerg, "Seven Principles for Selecting Software Packages," *Communications of the ACM*, Vol. 53, No. 8, August 2010.

[21] Damsgaard and Karlsbjerg, 2010.

full life cycle API management. This provides flexibility to use company A's SCM module and company B's asset management module at some point in the future if company A engages in aggressive profit maximization. Maintaining the relationships within a layer outside the primary functional system boundary would better position NOSS for change. Figure 2.3 demonstrates this possible future.

Figure 2.3. Alternative 9 with Multiple System Components



This array of existing solutions is a benefit of going commercial. NOSS does not have to be locked into one vendor, as many previous customized solutions are. Because the system is designed for forward compatibility, it would also make a potential future transition easier.

Chapter Summary

In developing the alternatives to use in the AoA, we started with the four alternative areas specified for the AoA. We then used responses to the Navy's RFI to flesh out 30 variants in the first three alternative areas, followed by a process of refinement to get a viable set of alternatives within the four alternative areas. We developed the alternatives in the hybrid alternative area as we worked through the refinement process.

Table 2.1 summarizes the nine alternatives selected based on this process and that we evaluated going forward. This included two Status Quo alternatives (1 and 2); one COTS alternative (3); four GOTS alternatives (4 to 7); and two Hybrid alternatives (8 to 9).

Table 2.1. Summary of Nine Alternatives Identified

Alternative Area	Alternative Name	Alternative Descriptions
Status Quo	1. Status Quo—no modernization	• Baselines current NTCSS system • Removes Naval Aviation Logistics Command Management Information System pieces and incorporates others • A total of 16 programs or systems
	2. Status Quo + code modernization and refresh of 16 systems	• Government will continue modernizing R-SUPPLY • Will expand effort to modernize all 16 additional systems
COTS	3. COTS	• Use separate commercial integrator and software provider, each priced separately
GOTS	4. Leverage Navy ERP	• Extend Navy ERP architecture to the operational fleet, leveraging existing Navy investments
	5. Leverage MSC LES	• Extend Navy MSC LES architecture to operational fleet, leveraging existing Navy investments
	6. Leverage GCSS-A or GCSS-MC	• Use GCSS-MC or GCSS-A and extend or integrate into the Navy, leveraging existing DoD investments
	7. Leverage DLA—DPAS	• Extend DPAS to operational fleet, leveraging existing DoD investments
Hybrid	8. Optimize Commercial with Status Quo of FSM and ROM systems	• Keep current FSM and integrate with COTS to mitigate lack of off-the-shelf capability
	9. Forward Compatible Commercial	• Mitigate vendor lock-in by pursuing integration partially based on ESB, APIM, or similar technology

3. Effectiveness Analysis Results

We conducted the effectiveness analysis in two phases. First, we analyzed the responses to the RFI; these responses provided information about which functional requirements the software could meet. Second, we conducted a quality analysis where other data and information were collected to assess how well the software could perform along these other dimensions. As an example, to meet cybersecurity requirements, the study team looked at whether the system can be compliant with the Risk Management Framework (RMF) by the initial operational capability (IOC) date. This chapter describes these two phases of the effectiveness analysis, starting with a discussion of the key requirements and quality attributes, before turning to the two analyses and their results.

Requirements and Quality Attributes

USFF generated 201 high-level requirements during its high-level BPR effort. In discussions with USFF, it indicated that the requirements were primarily functional in nature, and an assessment of the requirements confirms this. The functional requirements were developed using the Office of the Chief of Naval Operations logistics functional area manager (LOGFAM) taxonomy.[1] The concurrently generated detailed requirements were generated using DoD's Business Enterprise Architecture (BEA) framework.[2] The number of functional requirements by LOGFAM functional area is shown in Table 3.1.

---

[1] Office of the Chief of Naval Operations, N414, Logistics and Readiness IT Executive Committee Operational Concept, draft, June 2016. Not available to the general public.

[2] For more information on DoD's BEA, see Office of the Chief Management Officer, U.S. Department of Defense, "Business Enterprise Architecture," webpage, undated.

Table 3.1. Summary of Functional Requirements

LOGFAM Functional Title (ID)	Number of Requirements
Management of Acquisition (A1)	3
Project Management (A2)	7
Manage Logistics Product Management (A3)	8
Supply Chain Management (A5)	112
Fleet Operations (A10)	4
Financial Management (A12)	11
Cross Functional Requirements (A14)	56
Total	201

ID = identification number.

Because quality was represented in a limited way in the BPR requirements and the quality of the system's performance is important, the study team synthesized quality attributes from other sources, such as the study guidance and problem statement. In doing so, other elements were identified as important that had limited representation in the BPR requirements, such as forward compatibility, enterprise capability, and maturity. The list of quality attributes was vetted with USFF and other stakeholders (NAVSUP, PMW 150) and weights were assigned to elevate the more important quality attributes. This analysis will be discussed later in the chapter.

Requirements Analysis

Overview of the RFI

As noted above, prior to the start of the AoA, the Navy released an RFI to industry and government providers. The providers were asked to score how well they could meet the 201 high-level BPR requirements and other areas of interest for the Navy (including some quality attributes).

The Navy's preference, and our approach, was for each of the 201 requirements to be treated equally in the RFI. Each responder was asked to evaluate the ability of its current software solution to meet each requirement according to the following scale:

- 0 indicated it could not meet the requirement.
- 1 indicated it could meet the requirement partially.
- 2 indicated it could meet the requirement fully.

The ability of the vendor to partially or fully meet a requirement could have been through configuration or customization or through existing functionality. The Navy asked whether a requirement could be met in the future through customization or configuration, but this was not asked about the current capability. Some vendors chose not to comment on future capabilities;

others indicated that they would be able to achieve functionality in the future through configuration or customization. Each survey was accompanied by a letter that described the offeror's company, capabilities, and approach to NOSS. Table 3.2 summarizes the responses to the RFI and options identified.

Table 3.2. Summary of RFI Response Data

Alternatives	Number of RFI Responses or Options Identified	Number of RFI Responses with Requirement Analysis Data
Status Quo	2	2
GOTS	7	5[a]
COTS	21	20[b]
Total	**30**	**27**

[a] Three GOTS did not score how well their software could meet NOSS requirements. Two GOTS responses indicated that the commercial vendors of the software they use would be better able to score the software. GCSS-A was scored by RAND subject-matter experts (SMEs).
[b] One vendor did not reply with a score because it is a system integrator.

To collect data on the Status Quo, we engaged the current NTCSS program and government entities to identify options and document them according to the RFI. One option would be to continue the functionality currently provided by the 16 systems supporting afloat supply. The other option would be continuing to support the 16 systems, plus modernizing to meet NOSS requirements. The two options correspond to Alternatives 1 and 2 in Table 2.2 in the previous chapter.

We reviewed the documentation provided and verified and validated the response data through interviews with providers and industry literature. There are pros and cons to relying on self-reported data. Vendors know their software and can best provide information about what the software can and cannot do. However, vendors may also be optimistic in their current or future capabilities. The following sections summarize the written responses and describe the requirements scoring.

Analysis of RFI Responses

As shown in Table 3.2, the Navy received scores from 27 of the 30 respondents. Twenty were from COTS providers, five were from GOTS, and two were from Status Quo. The response data were not consistent because the respondents had differing interpretations of the questions. Some respondents left requirements blank because they did not believe their systems could satisfy the requirement (instead of scoring 0); others left requirements blank because they did not understand or had questions about the requirement. Still others were uncertain how to interpret a partial requirement.

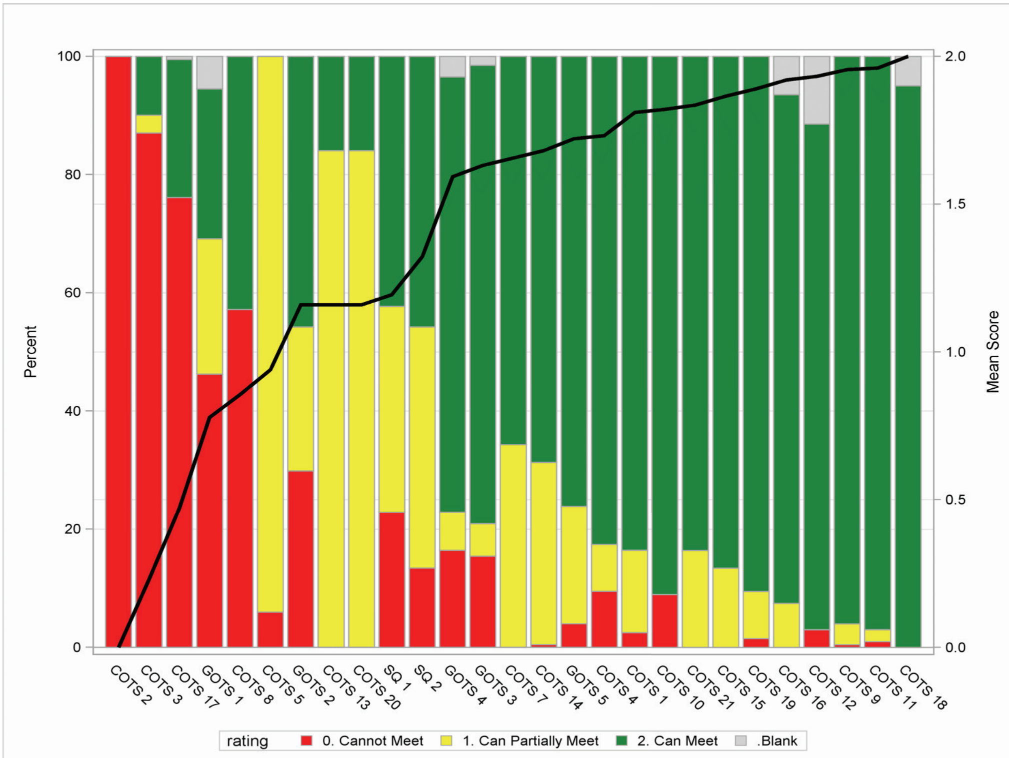
To validate and normalize the responses, we completed various activities. Half-day sessions were held with nearly all of the software providers and some of the system integrators. In the sessions, responses to the RFI were discussed and limited demonstrations were provided. Several discussions with PMW 150 and the program offices that manage GOTS helped to clarify the capabilities and limitations of the current systems and GOTS alternatives. We reviewed industry literature to identify what is in the realm of the possible today, and what capabilities might be expected in the future. Cost and schedule performance of similar projects were reviewed. From these assessments, we concluded that the self-reported scores were not unreasonable. The responses, at a high level of review, appear to be a reasonable representation of the vendors' capabilities and expected costs.

Many respondents indicated that they could satisfy the majority of the NOSS requirements with their current solutions.[3] Figure 3.1 shows how each of the 27 respondents in the Status Quo, COTS, and GOTS areas scored in the RFI analysis. The right vertical axis highlights the mean score across all requirements.[4] A score of 2 would imply that they can fully meet all the requirements. The left vertical axis shows the percentage of the requirements that are fully met (2 or colored green), partially met (1 or colored yellow), or not met (0 or colored red). The mean score is shown by the line in the figure. The vendors that can meet the highest percentage of the requirements are shown on the right side of the figure. On the far right of the figure, COTS 18 indicates that it can fully meet all the requirements for which it provided a response. COTS 11 indicates that it can fully meet about 98 percent of the requirements. Moving from the right of the figure to the left, the percentage of requirements that are fully met diminishes. COTS 2, on the far left, indicates that it could not satisfy any of the requirements (but was planning to in a future version). Some of the vendors did not score all the requirements. If the requirement was still unclear after conversations with the vendor, then the requirement remained unscored. In these cases, the total score would not reach 100 percent.

[3] The commercial vendor responses have been anonymized.

[4] A mean score can be useful for comparison. However, it does not provide all of the information that could be of interest. For example, response A could score half of the requirements as 2 and the other half as 0, while response B could score everything as 1; in the two cases, both responses would have an equal mean score of 1.

Figure 3.1. Clustered RFI Responses



Additional analyses were performed to understand the vendors' abilities to satisfy requirements; these additional analyses were used to develop hybrid alternatives. For example, *high-level requirement 144*—defined as "the system will maintain auditable financial records associated with managing Retail Operations"—was the worst-performing in the LOGFAM financial management group, with 40 percent of responses saying they could not meet the requirement and 20 percent saying they could partially meet it. This is compounded by the detailed-level requirements analysis that showed more than 1,000 detailed requirements were mapped to high-level requirement 144, making audit-enabled retail operations an area of risk. The Navy should consider selecting a vendor that is robust in this area or leverage Alternative 8 and maintain the current ROM capability as needed.

Table 3.3 shows the percentage of the high-level BPR requirements that each alternative is able to meet out of the box. The clear message from the table is that the COTS alternative and the two hybrid alternatives can meet 90 percent to 100 percent of the 201 BPR requirements.

Table 3.3. Percentage of BPR Requirements Met by As-Is Solution (cleaned data)

Alternative (values are rounded to the nearest 10th)	% Fully Met (*n* = 201)
1. Status Quo—no modernization	40
2. Status Quo + code modernization and refresh of 16 systems	50
3. COTS	90–100
4. Leverage Navy ERP	80
5. Leverage MSC LES	70
6. Leverage GCSS-A or GCSS-MC	80
7. DLA—DPAS	50
8. Hybrid Optimize Commercial with Status Quo of FSM and ROM systems	90–100
9. Hybrid Forward Compatible Commercial	90–100

NOTE: Alternatives 3, 8, and 9 are ranges because they represent multiple software solutions. *Cleaned data* are data adjusted for inconsistencies in response; the procedure was applied across all responses.

The response to the RFI indicated that there are many vendors that believe they can meet the majority of the high-level requirements of NOSS with their out-of-the box solutions or through configuration. At least one vendor indicated it could meet all the requirements out of the box. The responses were received from integrators, software providers, and government organizations currently using commercial software products. In some cases, the government organization responded with the help of the contractor who supports the software being evaluated.

Some of the high-level requirements' language left room for interpretation by vendors, leading to assessments that were overly conservative or overly optimistic. In the case of the cross-domain solution, several vendors indicated that the requirement could be met, but only one integrator offered a solution that enabled machine-to-machine reconciliation.[5] For the majority of the financial management requirements, the respondents were conservative, indicating that many of the requirements could not be met. Clarifying the language used for key requirements will be an important step to ensuring that the Navy receives the desired capabilities.

Quality Attribute Analysis

As noted earlier in this chapter, quality measures were not fully captured in the high-level BPR requirements, but quality was an important component of other guiding documents. The study guidance, study plan, and other NOSS program documentation revealed a number of important quality and performance attributes for NOSS, in addition to the functional requirements. We refined the qualities into a more meaningful set of quality attributes. Each alternative was assessed against each attribute to come up with an overall assessment of quality.

[5] This would allow machines to transfer the classified information between domains without a human in the loop.

Unfortunately, quality areas and measures are not one-to-one. The measures are assigned to the group of qualities to which they pertain, if they pertain to more than one. Table 3.4 describes the 24 quality areas and the set of measures for each evaluated area. It also shows the weight for all measures in the quality area, which is discussed next.

Table 3.4. Quality Areas and Measures of Effectiveness

Quality Area	Measure	Total Weight for All Measures in the Quality Area
Enterprise capability (auditability, supportability, interoperability)	• Enterprise database • One Authority to Operate (ATO) • Single sign-on • Well-defined interfaces	22
Usability or configurability	• Configurable user interface (UI) • Configurable business processes	16
Cybersecurity or supportability	• Cloud capable or enabled • Lightweight Information Assurance Vulnerability Management (IAVM) patching • Sustainable third-party dependencies	11
Availability	• In-place disconnected technology • Distributed authoritativeness	11
Supportability	• Thin client afloat or ashore • Lightweight updates • Rapid release cycles	11
Cybersecurity	• RMF ATO by objective IOC	9
Forward compatibility (open architecture)	• Open standards • Application modularity • Data modularity • Automated BEA alignment	9
Auditability	• Successful audits • Support separation of duties and extensive logging	7
Mobility	• Support for mobile supply devices	2
Interoperability	• Automated process for moving data between domains	1
Maturity	• Large and diverse customer base	1
Total		100

The desired solution should be more easily supported and maintainable than the current system and, to the extent possible, agile enough to prevent vendor lock-in and allow for more-rapid technological improvements. The solution needs to enable an enterprise business architecture, support disconnected and mobile operations, and seamlessly transfer data between classified and unclassified domains. Because of the nature of operations and allocation of bandwidth on the ship, the amount of bandwidth required by any solution must be limited.

As part of the RFI follow-up during the AoA, the team engaged vendors and system owners to understand how their system architectures might be capable of achieving the desired qualities.

We developed a set of three criteria for each of the 24 measures shown in Table 3.4 and an associated score, whereby a zero indicated that the alternative did not meet the measure, a 1 indicated that it partially met the measure, and a 2 meant that the alternative fully satisfied the condition. Furthermore, each measure was assigned a weight from a total score of 100 (as shown in Table 3.4). The higher the weight, the more important the measure. The maximum weight for an individual measure is 10. Therefore, a perfect score is 200 (a total weight of 100 * score of 2 for each measure). The weights were assigned based on the team's assessment of the relative importance of the individual factors, which was gained through interviews with stakeholders, interactions with stakeholders at the detailed BPR validation sessions, and assessment of the mapping between detailed BPR requirements and high-level BPR requirements. In addition, the weights were discussed with USFF and agreed upon, with the exception of mobile computing. However, an excursion was run where each attribute was treated as equally important (or unimportant) and Alternatives 3, 8, and 9 were still the preferred alternatives.

The Status Quo alternative with no modernization was the baseline and scored poorly because it did not have any of the quality attributes identified for NOSS. Table 3.5 summarizes the quality attribute scores for each alternative and shows that the COTS solution and the two Hybrid ones rank highest in terms of quality scores.

Table 3.5. Summary of Quality Scores by Alternative

Alternatives	Score (out of 200)
1. Status Quo—no modernization	0
2. Status Quo + code modernization and refresh of 16 systems	51
3. COTS	155–174
4. Leverage Navy ERP	85
5. Leverage MSC LES	119
6. Leverage GCSS-A or GCSS-MC	126
7. DLA—DPAS	92
8. Hybrid Optimize Commercial with Status Quo of FSM and ROM systems	120–142
9. Hybrid Forward Compatible Commercial	161–185

NOTE: Alternatives 3, 8, and 9 have score ranges because they represent multiple software solutions.

Chapter Summary

After reviewing both the functional requirements and the quality and performance attributes, the COTS and Hybrid solutions provide the most capability. The GOTS alternatives perform next best, and the Status Quo alternatives perform worst of all. Table 3.6 summarizes the requirements and quality scores.

Table 3.6. Summary of Functional Requirements and Quality Scores by Alternative

Alternative (values are rounded to the nearest 10th)	Requirements Score (% fully met (n = 201)	Quality Score (out of 200)
1. Status Quo—no modernization	40	0
2. Status Quo + code modernization and refresh of 16 systems	50	51
3. COTS	90–100	155–174
4. Leverage Navy ERP	80	85
5. Leverage MSC LES	70	119
6. Leverage GCSS-A or GCSS-MC	80	126
7. DLA—DPAS	50	92
8. Hybrid Optimize Commercial with Status Quo of FSM and ROM systems	90–100	120–142
9. Hybrid Forward Compatible Commercial	90–100	161–185

4. Cost Analysis Results

In this chapter, we discuss the cost analysis results for each alternative (starting with the cost-estimating ground rules and assumptions that underlie that analysis). We discuss the risk analysis results in Chapter 5.

Ground Rules and Assumptions

This section describes some of our key ground rules and assumptions made by developing the rough-order-of-magnitude cost estimates. We note that the cost estimates will be of sufficient quality to support acquisition and investment decisions—however, the estimates are not of budget quality. The cost-estimating ground rules and assumptions are overarching in nature and applicable to all the alternatives estimated, unless noted otherwise.

All costs in the report are presented in constant year (CY) or base year (BY) 2016 dollars. Then year (TY) costs or costs collected in other CY dollars were normalized to 2016 BY dollars using the latest published Naval Center for Cost Analysis inflation indexes. In instances where labor rates were used, these data are based on SPAWAR 1.6–approved labor rates and PMW 150 spend-plan rates.

The Work Breakdown Structure (WBS) used for the estimates is loosely based on the top-down SPAWAR 1.6 cost estimate WBS template (of SPAWAR Global WBS Mod E). This template was used as a guide for which general cost elements to consider and the template for presenting cost estimates. However, the granularity of the cost estimates is at a higher level than in the SPAWAR Global WBS Mod E because of the level of available data for the rough-order-of-magnitude cost estimates.

The *life cycle cost estimate* (LCCE) is defined as ten years beyond the deployment of all Increment I builds or, alternatively, ten years beyond FOC. FOC has been defined as the deployment of NOSS Increment I to all sites by the end of FY 2024. Therefore, the LCCE time frame is from FY 2018 through FY 2034. Another key date assumed in the estimate is the IOC date of FY 2021, which is defined as the deployment of Increment I to one shore site (i.e., enterprise) installation and one unit-level ship installation.

Additionally, the cost estimates include costs of a hosting solution properly sized to handle all data requirements and support implementation during development, production, and deployment phases.

In addition to the investment costs for the various alternatives, the sustainment cost estimates of the Status Quo legacy systems and applications will be included until their capabilities have been fully replaced or until FOC is achieved.

As discussed in Chapter 3, each of the alternatives fails to fully meet all the specified requirements. Using this analysis, additional development costs were calculated to fill the capability gaps for each alternative. In areas where known gaps exist, especially for ensuring backward compatibility for GOTS or COTS alternatives, we are factoring in transition cost estimates for the necessary system's customization efforts and any updated training costs needed.

Cost Summaries

Table 4.1 presents the costs for all alternatives prior to adjustments for risk. The two cost columns present a low and high LCCE relative to the status quo, including both NOSS costs and legacy system costs as they phase out.

Table 4.1. Unadjusted Costs Relative to the Status Quo

	LCC Deviation from the Status Quo FY 2018–2034 (BY 2016 $M)	
Alternative	**Low**	**High**
1. Status Quo—no modernization	—	—
2. Status Quo + code modernization and refresh of 16 systems	$29	$12
3. COTS	–$263	–$131
4. Leverage Navy ERP	–$164	–$128
5. Leverage MSC LES	–$258	–$294
6. Leverage GCSS-A or GCSS-MC	–$102	–$141
7. DLA—DPAS	$30	–$37
8. Hybrid Optimize Commercial with Status Quo of FSM and ROM systems	–$225	–$96
9. Hybrid Forward Compatible Commercial	–$260	–$56

NOTE: LCC = life cycle cost.

Risk-Adjusted Cost Summary

Table 4.2 is a summary of the risk-adjusted costs for all the alternatives. The two cost columns present a low and high LCCE relative to the status quo, including both NOSS costs and legacy system costs as they phase out.

The following three areas have been adjusted for risk:

1. **Code modernization failure or schedule slip.** The code modernization effort for R-SUPPLY has failed in past attempts. Based on our risk analysis, the probability of schedule slips for the code modernization effort is 75 percent. As documented in the Alternative 2 cost estimate, a high estimate was calculated using this probability of occurrence.

2. **Custom development for gap requirements.** A 75-percent risk factor was applied to custom development because of the uncertainty in the complexity of gap requirements. This means that the cost was increased by 75 percent for the requirements that were customized. This method was used in the 2014 RFI results to do business process improvements.
3. **Integration/implementation effort.** A 50-percent cost growth factor was applied to the integration/implementation effort for GOTS alternatives to account for schedule risk, while a 50-percent cost growth factor was applied to the integration/implementation effort for the low estimate of COTS alternatives to account for cost risk.

Table 4.2. Risk-Adjusted Costs Relative to the Status Quo

	LCC Deviation from the Status Quo FYs 2018–2034 (BY 2016 $M)	
Alternative	**Low**	**High**
1. Status Quo—no modernization	—	—
2. Status Quo + code modernization and refresh of 16 systems	$42	$40
3. COTS	–$248	–$112
4. Leverage Navy ERP	–$130	–$76
5. Leverage MSC LES	–$229	–$210
6. Leverage GCSS-A or GCSS-MC	–$85	–$85
7. DLA—DPAS	$30	–$11
8. Hybrid Optimize Commercial with Status Quo of FSM and ROM systems	–$212	–$82
9. Hybrid Forward Compatible Commercial	–$242	–$36

5. Risk Analysis Results

In this chapter, we present the risk analysis results. Risk analysis is a core component of any AoA. Each alternative is assessed on a number of risk areas and scored as either low, medium, or high risk in alignment with risk-scoring practices in DoD's *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*.[1] The assessed risk categories included performance, cost, and schedule. This chapter describes the risk analysis and the results of that analysis conducted for the NOSS AoA, starting with the methods we used.

Risk Analysis Element Definitions

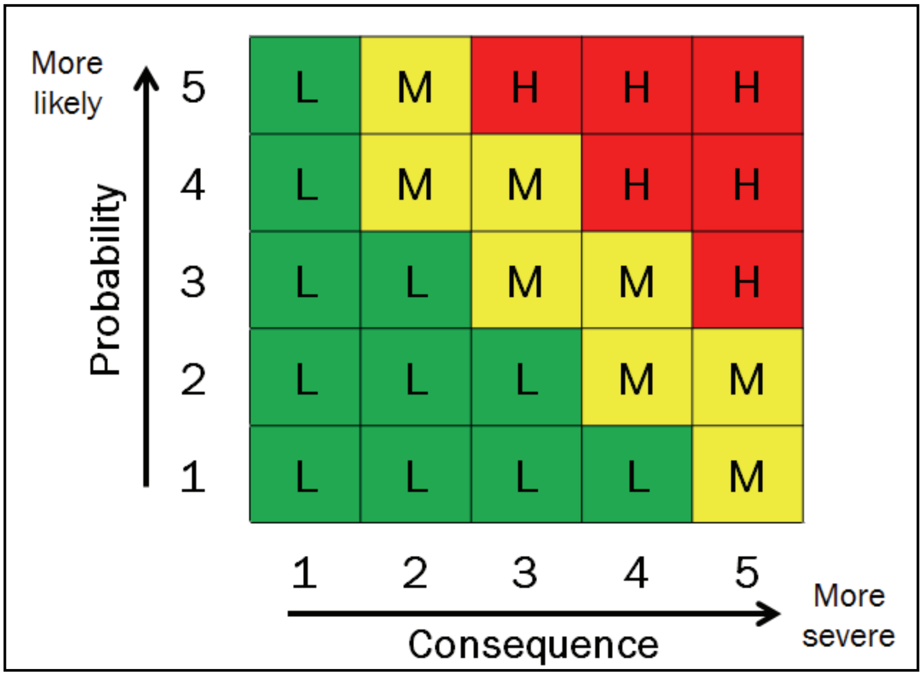
For this study, *risk* is defined as the probability that something adverse will occur and the consequence should that adverse event occur. This means that a high-risk score for a risk item, such as the ability to achieve compliance with the Financial Independent Auditability Review (FIAR), indicates a high likelihood and/or severity of failure on that item's part.

Our method for assessing risk for the NOSS AoA follows guidelines laid out in DoD's *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*.[2] Risk is calculated on a matrix of likelihood and consequence and falls into regions of low, moderate, and high risk, shown in Figure 5.1. The matrix is not quite symmetric: Items with very low likelihood but high consequence are deemed moderate risks, while items with a very high likelihood but very low consequence are deemed low risk. Outside these two blocks, the risk matrix is symmetric along the diagonal.

[1] Office of the Deputy Assistant Secretary of Defense for Systems Engineering, *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*, Washington, D.C.: U.S. Department of Defense, January 2017.

[2] Office of the Deputy Assistant Secretary of Defense for Systems Engineering, 2017.

Figure 5.1. Risk Matrix as Defined in DoD's *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*



SOURCE: Office of the Deputy Assistant Secretary of Defense for Systems Engineering, 2017, p. 28.

The DoD risk guidance offers further clarity on what the various levels of likelihood and consequence represent, shown in Table 5.1. A level-5 likelihood score indicates that the system component being examined will almost certainly fail in its intended use or not meet its intended cost or schedule. Although the guidance is clear, estimating a probability of occurrence for a given event can be very challenging.

Table 5.1. Risk Likelihood Levels

Level	Likelihood	Probability of Occurrence
5	Near certainty	>80% to ≤ 99%
4	Highly likely	>60% to ≤ 80%
3	Likely	>40% to ≤ 60%
2	Low likelihood	>20% to ≤ 40%
1	Not likely	>1% to ≤ 20%

SOURCE: Office of the Deputy Assistant Secretary of Defense for Systems Engineering, 2017, p. 26.

Risk likelihood is evaluated in the same way for all risk types, but risk consequence has slightly different meanings for the three different areas of risk— cost, schedule, and performance. Table 5.2 describes how consequence is assessed for cost, schedule, and performance.

Table 5.2. Risk Consequence Levels

Level	Cost	Schedule	Performance
5 Critical impact	• 10% or greater increase over the Acquisition Program Baseline (APB) objective values for research, development, test, and evaluation (RDT&E), Program Acquisition Unit Cost (PAUC), or Average Procurement Unit Cost (APUC) • Cost increase causes program to exceed affordability caps	• Schedule slip will require a major schedule rebaselining • Precludes program from meeting threshold dates	• Degradation precludes system from meeting a key performance parameter or key technical/supportability threshold; will jeopardize program success • Unable to meet mission objectives (defined as mission threads, concept of operations, Operational Mode Summary/Mission Profile)
4 Significant impact	• 5%–<10% over the APB objective values for RDT&E, PAUC, or APUC • Costs exceed life cycle ownership of Key System Attribute	• Schedule deviations will slip program to within 2 months of the approved APB threshold schedule date • Schedule slip puts funding at risk • Fielding of capability to operation units delayed by more than 6 months	• Degradation impairs ability to meet a Key System Attribute. Technical design or supportability margin exhausted in key areas. • Significant performance impact affecting system-of-system interdependencies. Work-arounds required to meet mission objectives
3 Moderate impact	• 1%–< 5% over the APB objective values for RDT&E, PAUC, or APUC • Manageable with Program Executive Officer or Service assistance	• Can meet APB objective schedule dates, but other APB key events (e.g., system engineering technical reviews or other Tier 1 Schedule events) may slip • Schedule slip affects synchronization with interdependent programs by greater than 2 months	• Unable to meet lower-tier attributes, Technical Performance Measures, or Critical Technical Parameters • Design or supportability margins reduced • Minor performance impact affecting system-of-system interdependencies. Work-arounds required to meet mission tasks
2 Minor impact	• Costs that drive unit production cost (e.g., APUC) increase of <1% over budget • Cost increase, but can be managed internally	• Some schedule slip, but can meet APB objective dates and non-APB key event dates	• Reduced technical performance or supportability; can be tolerated with little impact on program objectives • Design margins reduced with trade space
1 Minimal impact	• Minimal impact; costs expected to meet approved funding levels	• Minimal schedule impact	• Minimal consequences to meeting technical performance or supportability requirements. • Design margins will be met; margin to planned tripwires

SOURCE: Office of the Deputy Assistant Secretary of Defense for Systems Engineering, 2017, p. 25.

Risk consequence indicates the severity of the impact on the NOSS system if the risk item under discussion fails in its intended use or does not meet its intended schedule or expected cost.

Cost risk is the uncertainty associated with costs related to each alternative. Cost risk measures the uncertainty as a function of the absolute cost.

Schedule risk is relative to an alternative's ability to meet the IOC and FOC dates laid out in the NOSS program objectives. These are (objective) IOC by second quarter 2020, (threshold) by first quarter 2021, and FOC by fourth quarter 2024. *IOC* is defined as the deployment of build I to a unit level ship and one enterprise/shore installation.

Performance risk is typically based on critical technology elements associated with each alternative. These are not yet defined for NOSS, so we derived critical areas of performance based on the NOSS high-level business process requirements and supplemented these with discussions with stakeholders, internal SME discussions, and sponsor guidance.

Risk Analysis Approach

The risk assessment followed the study plan guidance, which calls for the definitions and types of risk in DoD's *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*.[3] The overall approach consisted of synthesis of risk elements, and scoring probability and consequence of risks. Each will be described in detail next.

Risk Element Synthesis

We enumerated risks from multiple sources. The NOSS high-level business process requirements were a primary source and were supplemented by discussions with stakeholders, internal SME discussions, and sponsor guidance. Nearly 300 detailed risk elements were derived for NOSS. Through a process of clustering, we combined similar risks to arrive at a total of 23 high-level risk elements (Table 5.3). A realized risk may affect cost, schedule, performance, or any combination of the three. For example, if a solution is delivered that does not support auditability, then it is likely that cost and schedule will be affected. Here, we assess the risk of a solution not meeting the performance requirements associated with auditability. Where an "X" is placed in the performance column only in Table 5.3, we assess the risk of a solution not meeting certain performance requirements, but we do not assess the cost and schedule implications of the event. The same is true for the columns where an "X" is placed in only the cost or schedule column.

[3] DoD, 2017.

Table 5.3. NOSS AoA Risk Elements

ID	Risk	Cost	Schedule	Performance
1	Not ready for FIAR audit, audit of materials			X
2	Does not provide sufficient or required financial and materiel management			X
3	Slow response to vulnerability patching			X
4	Inefficient work processes derived from lack of single sign-on solution (enhanced afloat because of personnel reductions)			X
5	Users cannot conduct near-real-time supply functions, while transitioning and synchronizing between connected and disconnected environments			X
6	Cannot perform desired analytics	X		
7	Cannot interface machine-to-machine with required external applications (including varying versions of Defense Logistics Management Standards implementations)			X
8	Cannot meet selected shore-side NOSS implementation at IOC by second quarter 2020 (objective) or first quarter 2021 (threshold)		X	
9	Cannot meet selected shore-side and afloat NOSS implementation FOC by fourth quarter 2024		X	
10	Cannot perform food services or subsistence tasks			X
11	Cannot handle retail operations			X
12	Unable to interface legacy systems to the enterprise during IOC to FOC changeover	X	X	
13	Unable to migrate legacy systems data to the enterprise during IOC to FOC changeover	X	X	
14	Unclear required level of integrator effort between IOC and FOC (e.g., to meet requirements gaps not met out of the box)	X		
15	Level of effort to integrate applications from different providers.	X	X	
16	System is cumbersome and time-consuming to learn, requiring extensive training (e.g., inefficient or unintuitive UI)	X		
17	Lack of a coherent training or change management program hurts adoption		X	
18	Too much customization, which prevents agility or maintainability	X		X
19	Inaccurate NOSS user and site numbers	X		X
20	Fails to deliver a secure system (RMF compliance, ATO compliance or waiver)		X	
21	Users cannot conduct near-real-time supply functions while operating in a reduced communications environment			X
22	Across the board, costs are significantly higher than projected	X		
23	Cannot achieve enterprise capability by FOC		X	X

Assessing Likelihood and Consequence

Determining the likelihood that a particular alternative will incur one of the identified risks required the synthesis of a number of documents from multiple sources. Each of the study team members used the information available in the form of responses to the RFI, engagements with vendors, demonstrations of capability, and commercial and industry reports to score the likelihood of occurrence. Through a nominal-group technique,[4] the study team worked to arrive at a final score for the likelihood of risk occurrence. The same process was employed to assess consequences. In addition to the documentation above, the study team also synthesized program information on capability gaps, goals, and objectives of NOSS to determine the magnitude of consequence should a risk occur.

Risk Analysis Results

Table 5.4 shows the number of high risks identified for each of the nine alternatives out of the 23 risk elements in Table 5.3. NOSS risks were broken into three categories: performance, cost, and schedule. We used a multitude of sources, including the NOSS high-level BPRs, internal discussions, external discussion, and SME input, with an iterative process to determine what these risks should be. We then used a second iterative process to score the probability and consequence of these risks in relation to the nine NOSS alternatives under consideration in this study.

---

[4] The nominal group technique is a social science methodology used to help groups of stakeholders arrive at a consensus. Three team members independently scored the risks and then met to review and discuss scores. During the review of individual risks, each member described their assumptions and reasons for their score until consensus was reached. For more information on the nominal group technique, see A. L. Delbecq, A. H. Van de Ven, and D. H. Gustafson, *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes*, Glenview, Ill.: Scott, Foresman and Company, 1975.

Table 5.4. Summary of Risk Analysis by Alternative

	Number of High Risks		
Alternative	**Performance**	**Cost**	**Schedule**
1. Status Quo—no modernization	7	1	1
2. Status Quo + code modernization and refresh of 16 systems	5	1	3
3. COTS	2	1	2
4. Leverage Navy ERP	3	2	3
5. Leverage MSC LES	4	1	3
6. Leverage GCSS-A or GCSS-MC	3	1	2
7. DLA—DPAS	3	1	3
8. Hybrid Optimize Commercial with Status Quo of FSM and ROM systems	2	1	2
9. Hybrid Forward Compatible Commercial	1	1	1

NOTE: red = greater than or equal to 3 high risks; yellow = 1–2 high risks.

As shown in the table, no alternative has zero high-level risks in performance, cost, and schedule. The Status Quo alternative (Alternative 1) cannot meet the performance requirements and has cost risk because of its reliance on customization. Alternative 2 is the riskiest alternative. Performing a code modernization improves performance, but it increases schedule risk and many performance risks still remain. Additionally, cost risk is higher for Alternative 2 than for Alternative 1 because of the need for additional integration work.

Using a COTS product and commercial integrator is a low-risk solution. High configurability reduces risk in all categories. Only the potential for some required customization for a food services or retail module introduces high risk to this alternative.

The three Navy GOTS extensions—Navy ERP, MSC LES, and DPAS—all have similar risk profiles. They carry noticeable performance risk because they lack performance out of the box and because they are highly customized applications. Because of this high level of customization and a need for additional customization to meet NOSS requirements, schedule slip is likely and cost overruns may result. In all cases, the number of high-risk items is similar to that for the code modernization alternative, and DPAS is the riskiest choice of the three. The best-of-breed non-Navy alternative fares slightly better because it would be based on a COTS solution, as GCCS-A and GCCS-MC are. It still has some high risks, but fewer than the other GOTS alternatives.

Alternative 9 is the least risky, with Alternatives 3 and 8 having slightly higher risk than 9 but less risk than the other alternatives. Alternative 8 handles the risk of needing customized modules by using already in-use solutions, while otherwise adapting the advantages of a COTS solution. Alternative 9 takes this concept to an even more robust point: It need not be just integration of legacy pieces with a COTS baseline but rather a combination of any software parts to make the solution. Both cases eliminate or reduce risk.

Chapter Summary

The COTS and Hybrid alternatives have the lowest overall risk, with low risk across all three categories. The alternatives for Navy ERP, MSC LES, DPAS, and a best-of-breed non-Navy GOTS system are moderately risky alternatives, having some areas of lower or higher risk but falling between the highest- and lowest-risk alternatives. Among these, Navy ERP and DPAS hold the highest risk of the GOTS alternatives, with the non-Navy alternative carrying the lowest risk of a GOTS system. The Status Quo alternatives carry high risk. Code modernization mitigates some of the many performance and schedule risks associated with the Status Quo alternative but is itself still a high-risk alternative, certainly no less risky than the GOTS alternatives.

6. Conclusions

Sixteen information systems support the Navy's afloat and ashore supply operations. The systems vary in their level of visibility of the data, thus making it difficult for the Navy to easily obtain an enterprise view of supply operations that can better respond to audits. The current set of systems also suffers from cybersecurity and supportability challenges. Many of the systems are antiquated, and some are no longer supported by the vendor. For these reasons, the Navy would like to modernize the afloat supply operations capability. As part of this, the Navy has developed a number of high-level functional requirements for the future supply system, referred to as the NOSS.

The Navy asked RAND to assist with an AoA for NOSS. Specifically, our study team was asked to assess the ability of the alternatives to satisfy the functional requirements, costs, and risks of four classes of alternatives:

- Status Quo, defined as the current set of systems
- COTS
- GOTS
- a Hybrid, defined as some combination of COTS, GOTS, and Status Quo.

The remainder of this chapter discusses our conclusions, starting with the alternatives we identified within the four alternative areas and then turning to the results of the assessment of those alternatives in terms of effectiveness (including quality), cost, and risk (performance, cost, and schedule risks).

Nine Alternatives Identified for Assessment

The study team defined nine specific alternatives, falling within the four alternative areas, as shown in Table 2.2.

Results of Assessment of the Nine Alternatives

There are many viable alternatives for the Navy to pursue, but none perform as well as the COTS and Hybrid alternatives (Alternative 3 and Alternatives 8 and 9). The COTS and Hybrid alternatives can satisfy the majority of the functional requirements (90 percent to 100 percent) and achieve relatively high-quality scores (149 to 174 out of 200) at a relatively low cost, and they offer the lowest performance, cost, and schedule risks. Status Quo alternatives (Alternatives 1 and 2) and DPAS (Alternative 7) are the costliest alternatives. The Status Quo alternatives meet only 40 percent to 50 percent of the functional requirements and score very low in quality. The best-performing GOTS alternative (Alternative 6) meets up to 80 percent of the functional requirements and achieves a score of 126 out of 200 for quality, but this alternative is more expensive than the better-performing COTS alternative.

Table 6.1 summarizes the effectiveness, cost, and risk of each alternative, highlighting the two best choices' rows in gray shading and in bold text—the COTS alternative and two Hybrid alternatives. The following paragraphs discuss the results in more detail, referring back to the table.

Table 6.1. Summary of Analysis Findings

	Effectiveness		Cost	Risk Analysis		
Alternative (values are rounded to the nearest 10th)	**Requirements Score (% fully met) (*n* = 201)**	**Quality Score (out of 200)**	**Average LCC Deviation from Status Quo FYs 2018–2034 (FY 2016 M$)**	**Perf.**	**Cost.**	**Sched.**
1. Status Quo—no modernization	40	0	—	7	1	1
2. Status Quo + code modernization and refresh of 16 systems	50	51	$41	5	1	3
3. COTS	**90–100**	**155–174**	**–$180**	**2**	**1**	**2**
4. Leverage Navy ERP	80	85	–$103	3	2	3
5. Leverage MSC LES	70	119	–$219	4	1	3
6. Leverage GCSS-A or GCSS-MC	80	126	–$85	3	1	2
7. DLA—DPAS	50	92	$9	3	1	3
8. Hybrid Optimize Commercial with Status Quo of FSM and ROM systems	**90–100**	**149**	**–$147**	**2**	**1**	**2**
9. Hybrid Forward Compatible Commercial	**90–100**	**165**	**–$129**	**1**	**1**	**1**

Effectiveness

To assess the effectiveness of the alternatives, the study team assessed how well the vendor solutions could satisfy the 201 high-level business process requirements. The study team used the vendors' self-scores, interviews, and product demonstrations, as well as industry reports, to conduct these assessments. The percentage of requirements that each alternative could satisfy was estimated as shown in Table 6.1. COTS and Hybrid are the best performers, satisfying nearly all the high-level requirements. The Status Quo alternatives and DPAS GOTS alternative meet up to half the requirements; the other GOTS alternatives can satisfy between 70 percent and 80 percent of the requirements.

In addition to the high-level business requirements assessment, the study team derived a number of important quality objectives for NOSS from program documentation and stakeholder engagements. These included the ability to be FIAR compliant, the ability to achieve an ATO,[35] the ability to operate in a disconnected environment, and the ability to provide an enterprise view of supply operations. Measures of effectiveness were then developed to assess the ability of each alternative to satisfy these quality objectives. Each alternative was scored, with a total possible score of 200.

Alternatives 3 and 9 have the highest scores for quality. Status Quo alternatives score the lowest, because they do not achieve any of the quality measures, such as enterprise visibility, auditability, or cybersecurity. The GOTS alternatives achieve scores between 85 and 126, which is better than the Status Quo alternative but not as good as Alternative 3.

Cost

The costs of the COTS and Hybrid alternatives are lower than most of the GOTS alternatives and the Status Quo, as shown in Table 6.1. Continuing to maintain the current suite of systems or modernizing the current suite of systems—the Status Quo alternatives—are the costliest options. A COTS solution is more affordable than the Status Quo ones, and most of the GOTS alternatives. The Hybrid alternatives are a bit costlier than the COTS alternative. MSC LES has the lowest average cost.

Risk

Customization of commercial software is the biggest source of risk to cost, schedule, and performance for all of the alternatives. The risks associated with the COTS and Hybrid alternatives are lower than they are for the Status Quo and GOTS alternatives, as shown in Table 6.1. This is because these alternatives are expected to satisfy the requirements with the least amount of customization. The COTS and Hybrid alternatives can meet the majority of the requirements out of the box. This is partly because of the new functionality being offered by software vendors, which allows the integrator or user to more easily manipulate processes and data, as well as interface with other technologies.

The Status Quo alternatives will never be able to meet certain functional requirements or achieve certain levels of quality. For the Status Quo with code modernization (Alternative 2), the performance risks are somewhat mitigated, but there is significant uncertainty with respect to the schedule.

The GOTS alternatives have a higher risk than the commercial alternatives for a variety of reasons. All the GOTS solutions will require more customization than their commercial

[35] An ATO is a formal declaration by a Designated Approving Authority that authorizes operation of a business product and explicitly accepts the risk to agency operations (see Centers of Disease Control and Prevention, "Authority to Operate," webpage, undated).

counterparts to fully meet NOSS requirements, which increases performance and schedule risk. Some of the GOTS alternatives have been heavily customized, which can also present risks to performance and cost.

Conclusion

Given the findings above, the recommendation of the AoA is to move forward with COTS, with a preference for Alternative 9. Alternative 3 is COTS, which could be provided by any number of vendors. Alternatives 8 and 9 are simply adaptations of Alternative 3. If the Navy likes a COTS option that assesses solidly in all categories except food service and retail, then the Navy can choose Hybrid Alternative 8 and maintain support for government-supplied solutions in those areas until a vendor can subsume the food and retail capabilities. If the Navy wants to attempt to mitigate vendor lock-in down the road, then it can identify a proposal that brings in third-party integration separate from the core functionality provided by the software, as is the case in Alternative 9. Moreover, there is no reason the Navy cannot choose a combination of Alternatives 8 and 9.

References

Assistant Program Manager–FSM3/ROM3, description of FSM/ROM capabilities emailed to study director, November 21, 2016.

Centers for Disease Control and Prevention, "Authority to Operate," webpage, undated. As of May 7, 2018: https://www2a.cdc.gov/cdcup/library/pmg/implementation/ato_description.htm

Damsgaard, Jan, and Jan Karlsbjerg, "Seven Principles for Selecting Software Packages," *Communications of the ACM*, Vol. 53, No. 8, August 2010.

Defense Acquisition Management Information Retrieval, *Major Automated Information System 2016 Annual Report, Global Combat Support System-Marine Corps Logistics Chain Management Increment 1*, Washington, D.C.: U.S. Department of Defense, March 2016. As of August 14, 2017: http://www.dtic.mil/dtic/tr/fulltext/u2/1019806.pdf

Defense Logistics Agency, *RFI Response: COTS Solutions to Meet Naval Operational Supply System (NOSS) Requirements*, February 17, 2017.

Delbecq, A. L., A. H. Van de Ven, and D. H. Gustafson, *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes*, Glenview, Ill.: Scott, Foresman and Company, 1975.

FAR—*See* Federal Acquisition Regulations.

Federal Acquisition Regulations, Part 2, Definitions of Words and Terms, Subpart 2.101, Definitions, January 13, 2017. As of July 13, 2017: http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/02.htm

Inspector General, U.S. Department of Defense, *Military Sealift Command Oversight of Excess Spare-Parts Inventory and Purchases for Sealift Program Roll-On/Roll-Off Ships Needs Improvement*, Washington, D.C., No. DODIG-2014-106, September 9, 2014. As of August 28, 2017: https://media.defense.gov/2014/Sep/09/2001713398/-1/-1/1/DODIG-2014-106.pdf

Malinverno, Paolo, and Mark O'Neill, *Magic Quadrant for Full Life Cycle API Management*, Stamford, Conn.: Gartner, October 27, 2016. As of May 5, 2018: https://www.gartner.com/doc/3488151/magic-quadrant-life-cycle-api

Military Sealift Command, *N4 Logistics, Request for Information: COTS Solutions to Meet Naval Operational Supply System (NOSS) Requirements*, February 3, 2017.

Naval Supply Systems Command, *RSupply Unit User's Guide*, NAVSUP P-732, Revision 3, March 31, 2005.

Navy Enterprise Business Solutions, *Navy ERP Request for Information: COTS Solution to Meet Naval Operational Supply System (NOSS) Requirements*, January 31, 2017.

Northrop Grumman, "Global Combat Support System–Army," webpage, undated. As of August 14, 2017:
http://www.northropgrumman.com/Capabilities/GCSS/Pages/default.aspx

Office of Aerospace Studies, *Analysis of Alternatives (AoA) Handbook: A Practical Guide to the Analysis of Alternatives*, Kirtland Air Force Base, N.M.: Headquarters, Air Force, July 6, 2016. As of May 4, 2018:
http://afacpo.com/AQDocs/AoAHandbook.pdf

Office of the Chief Management Officer, U.S. Department of Defense, "Business Enterprise Architecture," webpage, undated. As of May 5, 2018:
http://cmo.defense.gov/Products-and-Services/Business-Enterprise-Architecture

Office of the Chief of Naval Operations, N414, Logistics and Readiness IT Executive Committee Operational Concept, draft, June 2016. Not available to the general public.

Office of the Deputy Assistant Secretary of Defense for Systems Engineering, *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*, Washington, D.C.: U.S. Department of Defense, January 2017.

U.S. Army Acquisition Support Center, "Global Combat Support System–Army (GCSS-Army)," webpage, undated. As of August 6, 2018:
https://asc.army.mil/web/portfolio-item/eis-gcss-army/