IDA

INSTITUTE FOR DEFENSE ANALYSES

Beyond Enterprise Resource Planning (ERP): The Next Generation Enterprise Resource Planning Environment

Laura A. Odell, Project Leader

Brendan T. Farrar-Foley
John R. Kinkel
Rama S. Moorthy
Jennifer A. Schultz

February 2012
IDA Paper P-4852
Log: H 12-000323
Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract DASW01-04-C-0003,Task AO-5-3446, "Beyond Enterprise Resource Planning (ERP)," for the Office of the Under Secretary of Defense for Acquisition and Technology. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Paul K. Ketrick, Elizabeth A. McDaniel, Robert M. Rolfe

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper P-4852

Beyond Enterprise Resource Planning (ERP): The Next Generation Enterprise Resource Planning Environment

Laura A. Odell, Project Leader

Brendan T. Farrar-Foley
John R. Kinkel
Rama S. Moorthy
Jennifer A. Schultz

Executive Summary

Introduction

The Department of Defense (DoD) has invested billions of dollars in business, logistics, and financially focused enterprise resource planning (ERP) systems that are not meeting their schedules, are over cost, and are under-performing. Billions of dollars more are needed to implement them fully and achieve expectations; and the need to implement these ERP systems successfully and within budget is now more pressing than ever. Meanwhile, information technology (IT) has continued to evolve in the 20 years since ERPs were first introduced.

The Institute for Defense Analyses (IDA) evaluated eight of DoD's ERPs to identify the best way to leverage those ERPs that have met their objectives and explore alternatives that might better support DoD business processes in the future.

IDA analyzed historical and planned cost and schedule data, capabilities, performance, financial and budget information, and future planning documentation for the Department's major ERP implementations, which include the following:

- Army—Global Combat Support System-Army (GCSS-Army), General Fund Enterprise Business System (GFEBS), and Logistics Modernization Program (LMP);
- Navy/Marine Corps—Global Combat Support System-Marine Corps (GCSS-MC) and Navy Enterprise Resource Planning Program (Navy ERP);
- Air Force—Defense Enterprise Accounting and Management System (DEAMS) and Expeditionary Combat Support System (ECSS); and
- Defense Logistics Agency (DLA)—Enterprise Business System (EBS).

IDA reviewed DoD documentation regarding the underlying causes of cost overruns, the organizational structure used for the ERP systems' strategic and operational decision-making, acquisition-related and architectural material, including the Business Enterprise Architecture (BEA), and auditability requirements and plans. The team considered the maturity and effectiveness of the ERP systems and several ancillary systems implemented by the Departments of the Army, Navy, and Air Force, and the DLA.

As part of the data collection on the ERPs and evolving software technologies, the IDA team interviewed current and former DoD, Military Department, and Defense Agency leaders and program managers, and industry leaders. To promote candor, interviewees' comments were for background information and without attribution.

Next, the IDA team conducted trade-space analyses of feasible solutions, such as Business Process Modeling/Management, Software as a Service, and available open source tools for modeling business rules and for building and operating systems around those rules. The solutions included commercially available services, other federal agency solutions, and hybrid solutions using a combination of native DoD services and commercial services. These analyses are documented in populated risk cubes with risks, drivers, and recommendations. All risks were examined for cost, schedule, and performance impact, and each of the criteria was examined as a trade between likelihood and consequence. Building on the recommendations developed from the trade-space analyses, IDA derived several overarching findings and recommendations.

Overarching Findings

The need to streamline processes and gain efficiencies through the use of IT is complicated by the evolving nature of IT. More than ever, commercial consumers—not DoD's buying power—influence technology developments.

While return on investment (ROI) is the basic industry measure of success or failure, the Department focuses on total cost of ownership of IT investments. A better indicator of value to an organization would be to take into consideration the economic characteristic of the investment and the ROI evidence by adoption rates (e.g., number of users and the ease of use).

Portfolio management forces an enterprise perspective of requirements, investments, and priorities instead of treating requirements as distinct and unrelated. With this approach, portfolio managers must exercise extreme discipline to achieve situational agility by assessing performance against expectations of each segment of their portfolio. Situational agility involves dynamic understanding and leveraging of financial, logistics, human capital management, and other business functions using portfolio management as an enabler of innovation to fulfill needed capabilities.

If the DoD continues at the high investment rate required to deploy the business ERP systems fully, the following fundamental changes to the strategic segments of the portfolio management profile must be addressed:

- The reliance on system integrators and software vendors to implement ERP systems must be minimized to the greatest extent practicable. To undo this reliance requires an investment in the recruitment and retention of key government personnel who are knowledgeable about ERPs and systems.
- ERP program compliance with the Defense Acquisition System (including administrative and oversight activities) must not be confused with achieving results. Whenever possible, performance and technical reviews and evaluations should carry more weight than compliance and oversight briefing reviews in determining whether a program should continue.

- Each ERP system must become much more than a single-focused platform (e.g., financials and logistics). These ERP system investments must provide the foundation for integrating other technologies (e.g., cloud computing initiatives, mobile applications, customer relationship management, and business intelligence). The Department's heavy dependence on only two software vendors will result in vendor lock-in, potentially leading to a single point of failure.

Overarching Recommendations

DoD can better manage its investments in legacy and ERP systems and the next-generation enterprise resource planning environment by:

- Taking advantage of emerging technologies and approaches, such as the increasing shift from products to services as tools, to accomplish business transformation goals as alternatives to ERPs.
- Initiating an objective assessment of what the ERP systems can realistically deliver and the effects of customization. An ERP system cannot and should not be used as a forcing function for organizational change management; rather the ability and willingness of an organization to change behavior, cultural norms, and processes is a prerequisite for a successful ERP implementation.
- Creating an environment where decisions to cancel under-performing programs are as routine as decisions to continue performing programs.
- Establishing incentives for enterprise leadership and stewardship for managing the Department's IT investments. Every investment should meet a common purpose that achieves an outcome beyond just one Military Department or Agency.
- Using aggregate data methods to the greatest extent practical. As Defense business systems become increasingly linked and are hosted in dynamic commodity computing environments, data ownership will evolve into a data stewardship model. Hence, data aggregation concepts and methods become increasingly important to allow decision makers and system architects to build effective and efficient systems with minimal duplication of effort across DoD.
- Recognizing organizational constraints—both mission and political—and focusing on high performance, not just high compliance, when making IT investments.
- Implementing enterprise IT solutions that address the entire doctrine, organization, training, materiel, leadership and education, personnel, and facilities spectrum.
- Controlling the business logic across financial, logistics, human capital management, and other business functions, thereby preventing lock-in to particular vendors, products, or business models.

THIS PAGE INTENTIONALLY LEFT BLANK

Contents

Appendixes

Illustrations

Tables

THIS PAGE INTENTIONALLY LEFT BLANK

1. Introduction

A. Background

The Department of Defense (DoD) has invested billions of dollars in business, logistics, and financially focused enterprise resource planning (ERP) systems. An investment of billions of dollars more is required to implement these systems fully and to make them achieve expectations. It has become clear, however, that ERP systems are not meeting their schedules, are over budget, and are under-performing. The current economic environment demands high impact, low cost solutions in which high performance trumps all other factors.

The "all in" ERP strategy of the 1990s is undergoing a reevaluation as new, more agile technology options become available. Industry is balancing the ongoing conflict between staying the course and realizing benefits from sunk costs totaling billions of dollars against continuing with under-performing and immature systems. Given a constrained economic environment, the Department must learn from the experiences of large global companies that are taking a fresh look at their business models and realigning their enterprise software for congruency with operational realities.

The ability to implement the DoD ERP systems successfully and within budget is now more pressing than ever. In a November 3, 2010 memorandum, Dr. Ashton B. Carter, who was then serving as the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), directed that the Department should obtain greater efficiency and productivity in defense spending by pursuing initiatives in the following five areas:

1) Target affordability and control cost growth;
2) Incentivize productivity and innovation in industry;
3) Promote real competition;
4) Improve tradecraft and services acquisition; and
5) Reduce nonproductive processes and bureaucracy.[1]

More recently, the National Defense Authorization Act (NDAA) for Fiscal Year 2012 took aim at DoD's redundant systems for accounting and business operations. The NDAA directed the

[1] Ashton B. Carter, Under Secretary of Defense for Acquisition, Technology and Logistics, DoD, *Implementation Directive for Better Buying Power—Obtaining Greater Efficiency and Productivity in Defense Spending*, Memorandum, November 3, 2010, http://www.ndia.org/Advocacy/Resources/Documents/LegislativeAlerts/Implementation_Directive_6Nov2010.pdf.

DoD Deputy Chief Management Officer (DCMO) to establish an investment review board by March 15, 2012, to conduct trade-space evaluations of business systems and management processes from a number of perspectives, including scope, complexity, and cost. The board's goal is to aggressively streamline systems across DoD's business management communities.[2]

Senior Defense leaders are increasingly aware that the current U.S. and world economic environments demand that the DoD move from *readiness at any cost* to *readiness at the best value*. While DoD sees the potential of ERP systems to lead to a clean financial audit, the issues delaying successful deployment of these business information technology (IT) capabilities go beyond the challenges of system acquisition.

B. Scope and Methodology

The Institute for Defense Analyses (IDA) was asked to:

- Evaluate current government ERP implementations to assess ways to leverage the DoD systems that are meeting objectives. The evaluation focused on financial systems but included logistics and business systems that IDA deemed appropriate for this evaluation.
- Explore potential alternatives or add-ons to ERPs to improve support for DoD business processes. Potential alternatives include:
  - Business Process Modeling/Management (BPM) solutions—BPM and BPM Notation (BPMN) based solutions allow for the extraction of business processes from legacy and non-legacy systems;
  - Software as a Service (SaaS)—SaaS solutions involve conforming an organization's business processes to an existing set of business process providers that are provided as a software service; and
  - Open source—Open source software tools are available both for modeling business rules and for building and operating software systems around those rules.

IDA analyzed historical and planned cost and schedule data, capabilities, performance, financial and budget information, and future planning documentation for the Department's major ERP implementations, which include the following:

- Army—Global Combat Support System-Army (GCSS-Army), General Fund Enterprise Business System (GFEBS), and Logistics Modernization Program (LMP);

[2] National Defense Authorization Act for Fiscal Year 2012, Sec. 901. REVISION OF DEFENSE BUSINESS SYSTEMS REQUIREMENTS. Public Law 112-81, December 31, 2011.

- Navy/Marine Corps—Global Combat Support System-Marine Corps (GCSS-MC) and Navy Enterprise Resource Planning Program (Navy ERP);
- Air Force—Defense Enterprise Accounting and Management System (DEAMS) and Expeditionary Combat Support System (ECSS); and
- Defense Logistics Agency (DLA)—Enterprise Business System (EBS).

IDA reviewed DoD documentation regarding the following: (1) underlying causes of cost overruns; (2) the organizational structure used for the ERP systems' strategic and operational decision-making; (3) acquisition-related and architectural material, including the Business Enterprise Architecture (BEA); and (4) auditability requirements and plans. In addition, the IDA team considered the maturity and effectiveness of the ERP systems and several ancillary systems implemented by the Departments of the Army, Navy, and Air Force, and the DLA.

The IDA team also interviewed current and former DoD, Military Department (MILDEP), and Defense Agency leaders and program managers, and industry leaders on ERP systems and other software technologies. To promote candor, interviewees' comments were for background information and without attribution.

Based on what was learned, the IDA team conducted trade-space analyses of feasible solutions including:

- Commercially available services;
- Solutions other federal agencies are leveraging; and
- Hybrid solutions using a combination of native DoD services and commercial services.

These analyses are documented in populated risk cubes for solutions that are available beyond the traditional ERP models. Each risk cube includes risks, drivers, and recommendations. All risks were examined for cost, schedule, and performance impact. Each of the criteria was examined as a trade between likelihood and consequence. This top-down design view was tailored to the DoD with ancillary examples of other global footprint companies that require similar privacy, security, and magnitude of volume of transactions considerations.

C. Organization of Report

Chapter 2 provides a history and current status of DoD business systems—ERP and legacy—and the risks associated with the legacy systems and ERP system environments within the Department. Chapter 3 describes the imperatives and opportunities of the next-generation enterprise resource planning environment. Chapter 4 explores technology and standards for the next-generation ERP environment. Moving beyond the narrower system focus of the preceding chapters, Chapter 5 examines the business IT portfolio by addressing the risks associated with the Department's reliance on system integrators and recommending portfolio management

solutions, including consolidation. Finally, drawing from the trade-space analyses, Chapter 6 concludes with the findings and recommendations.

There are four appendices. Appendix A contains full-page views of the trade-space analyses contained in the report. Appendix B provides two cases studies on the uses of industry consortia's success in developing standards, building common vocabularies, and establishing trust agreements. Appendix C is a list of acronyms. Appendix D is the list of references.

2. History and Current Status of ERP Systems in DoD

A. Terminology

The findings and recommendations in this report are dependent upon an understanding of ERP systems in DoD. For this reason, the following definitions are offered:

- **Enterprise resource planning environment:** a set of business functions that are consolidated for the purposes of data exchange, data transaction, and reporting. These business functions tie directly to daily operations delivering optimization to mission requirements. An integrated set of commercial (e.g., ERPs) and custom systems can provide these business functions.
- **ERP system:** an enterprise-wide commercial off-the-shelf (COTS) software product (e.g., SAP and Oracle) that integrates and automates various business functions (i.e., financial management, human capital management, and logistics management), including any added customizations, being pursued by a MILDEP or Agency.
- **Information Technology (IT):** "any system or subsystem of hardware and/or software whose purpose is acquiring, processing, storing, or communicating information or data."[3]
- **Legacy system:** a non-ERP business system that is fully implemented within a MILDEP or Agency. Fully implemented means the system achieved a Full Deployment Decision (FDD) or Full Operational Capability (FOC) from its Milestone Decision Authority and is currently in sustainment.

B. Background

After more than a decade of striving to implement ERP systems, the current environment reveals mixed implementation results. This statement is applicable to both government and commercial entities. In the private sector and at the state government level, project failures and resulting lawsuits (e.g., City of New York, Lumber Liquidators, and Tesco Bank) are described openly in business journals and publications. Although there are successful implementations of ERP systems, including within DoD, the results were realized at much higher costs and over longer implementation timeframes than first predicted at the inception of these large projects.

[3] Defense Science Board, *Department of Defense Policies and Procedures for the Acquisition of Information Technology*, Report, March 2009, 1, http://www.acq.osd.mil/dsb/reports/ADA498375.pdf (this definition was developed by the Defense Science Board for the purpose of clarity because the "DOD has a very long definition of IT which is too complicated to be useful").

There is a growing realization that results rather than activities must be the focus of any evaluation when declaring an ERP effort a success. Central to these evaluations is the tenet that the degree the system users' benefit from the ERP solution should be *the* critical indicator of success. In the past, the administrative aspects—including schedule and cost milestones—were the focus of program success rather than performance. While this approach benefits the contractors involved in these large efforts, it is a detriment for the communities of interest that the original requirements were supposed to serve. There are many reasons for this. First, cost and schedule are easy to measure; therefore, the Department measures them. Second, DoD's acquisition requirements demand compliance to administrative checklists. These checklists do not reflect satisfactory performance from a user perspective. Finally, in the March 2009 *Final Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for Acquisition of Information Technology*, the Board highlighted the fact that DoD managers lacked the necessary skills to manage IT programs.[4] Specifically, the Board noted: "[s]kills in program administration are confused with skills in operational process design and/or skills in IT. Contracting, budgetary, and organizational design debates crowd out concepts of operations and system engineering debates."[5]

To understand better how the ERP systems evolved as the primary methodology for business transformation during the late 1990s in the Department, it is instructive to chronicle the iterative steps from the brick-and-mortar IT infrastructure days of the 1980s to the IT solutions now available, including cloud computing (see Figure 1).

It is worth mentioning that the issues of today are similar to the systematic management problems faced by the Department several decades ago. These issues include: (1) cultural barriers that limit opportunities for change; (2) the lack of incentives for implementing change; (3) the lack of comprehensive and reliable management data for making decisions and measuring program cost and performance; (4) the lack of clear results-oriented goals; and (5) inconsistent management accountability and follow through.

[4] Defense Science Board, *Final Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for Acquisition of Information Technology*, March 2009, 67, http://www.acq.osd.mil/dsb/reports/ADA498375.pdf.

[5] Ibid.

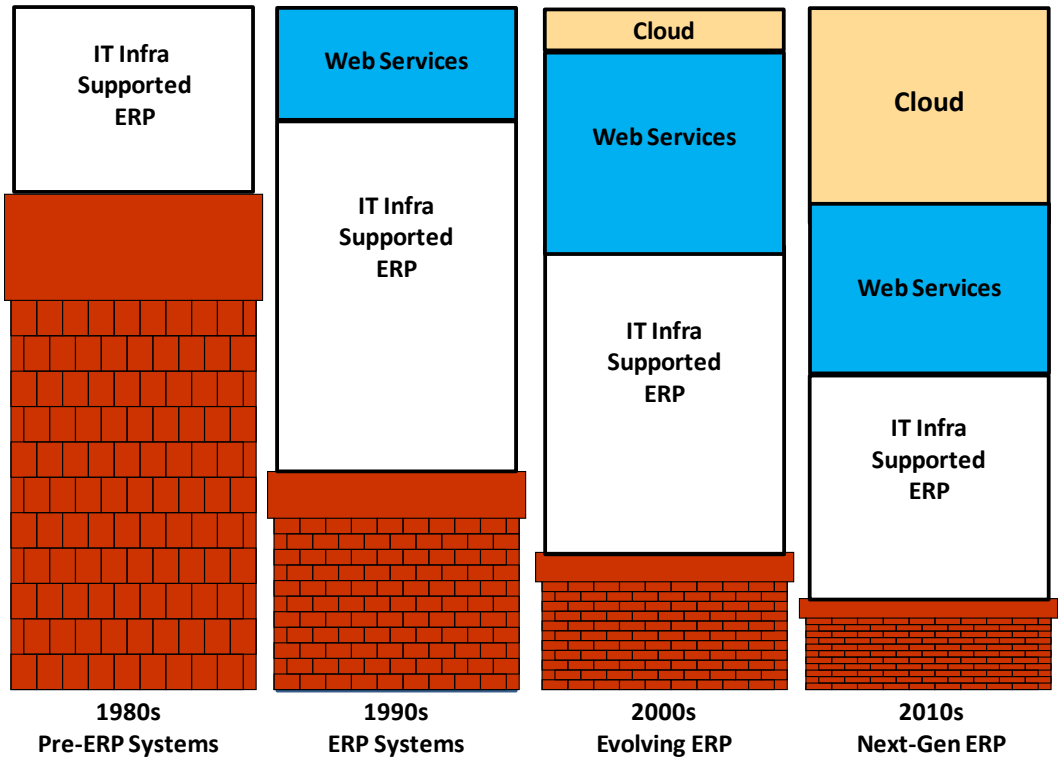


Figure 1. Business System Technology Progression: Brick and Mortar to Cloud

In the decades preceding and during the 1980s, most of the Department's emerging or deployed high technology systems were primarily mission- and warfighting-related. Business systems were considered *back office* and were highly localized to a specific geographic region with a singular function. During the mid- to late-1990s, many business systems were developed in response to the Secretary of Defense's *paperless initiatives*.[6] The paperless initiatives were intended to reduce the costs of DoD business and support activities so that operations and maintenance funds could be freed up to be used in support of weapons modernization and readiness needs. When the House of Representatives' Subcommittee on Military Readiness of the Committee on National Security met for its hearing on "FY 1999 Infrastructure Reduction and Military Readiness" on March 13, 1998, the General Accounting Office noted in its testimony that "significant opportunities remain to further streamline operations, consolidate

[6] Under Secretary of Defense (Comptroller), *Management Reform Memorandum #2— Moving to a Paper-free Contracting Process by January 1, 2000*, Memorandum, May 21, 1997, http://www.defense.gov/dodreform/mrms/mrm2.html; Deputy Secretary of Defense, *Department of Defense Reform Initiative Directive #46—Paperless Contracting*, December 9, 1998, http://www.defense.gov/dodreform/drids/drid46.html; Deputy Secretary of Defense, *Department of Defense Reform Initiative Directive #47—End-to-End Procurement Process*, December 9, 1998, http://www.defense.gov/dodreform/drids/drid47.html.

functions, eliminate duplication of effort, and improve efficiency in DOD's business activities."[7] Even though the Chief Financial Officers Act of 1990[8] had been in effect for over seven years, there was no mention during the hearing of the concept or goal of a clean audit or audit readiness for the DoD.[9] Rather, the hearing's focus was on the goal of decreasing infrastructure costs—through the reduction of paper-intensive, manual processes, and administrative burdens or through outsourcing or privatizing government activities via A-76 competitions—to fund modernization initiatives.[10] In early 1998, the Department started down the road with its first ERP system—Army's LMP—to resolve longstanding logistics troubles.[11] Shortly thereafter, the Department of the Navy initiated four logistics ERP pilots. Again, the focus was not on financials.

By late 2001, the emphasis shifted from a paperless to a decidedly more business-focused initiative of financial statement reliability. With the passage of specific provisions of the National Defense Authorization Act for Fiscal Year 2002, Congress was no longer interested in infrastructure cost reductions; instead, it was on a quest for audit readiness and a clean audit for the Department and its components.[12] Specifically, the Department was required to report annually on its financial statements as to "whether the policies and procedures of the Department of Defense, and the systems used within the Department of Defense, for the preparation of financial statements allow the achievement of reliability in those financial statements."[13] To achieve reliable financial statements, Congress also established the Financial Management Modernization Executive Committee chaired by the Under Secretary of Defense (Comptroller)/Chief Financial Officer (USD(C)), USD(AT&L), USD(Personnel and Readiness), and the DoD Chief Information Officer.[14] Congress directed the committee:

> (1) To establish a process that ensures that each critical accounting system, financial management system, and data feeder system of the Department of

[7] GAO, *Defense Management: Challenges Facing DOD in Implementing Defense Reform Initiatives*, (Testimony, Statement of David R. Warren, Director, Defense Management Issues, National Security and International Affairs Division, GAO/T-NSIAD/AIMD-98-122), March 13, 1998, 1, http://www.gao.gov/assets/110/107264.pdf.

[8] Title II of Public Law 101-576, November 15, 1990.

[9] Hearing of the Military Readiness Subcommittee of the House National Security Committee, SUBJECT: FY 1999 Infrastructure Reduction and Military Readiness, 2212 Rayburn Building, Washington, DC, March 13, 1998, http://commdocs.house.gov/committees/security/has065030.000/has065030_3.HTM.

[10] Ibid.

[11] GAO, *DOD Business Systems Modernization: Billions Continue to Be Invested with Inadequate Management Oversight and Accountability* (GAO-04-615), May, 2004, 14, http://www.gao.gov/assets/250/242540.pdf.

[12] Sections 1008-1009, Public Law 107-107, December 28, 2001.

[13] Section 1008(a), Public Law 107-107, December 28, 2001.

[14] Section 1009(a), Public Law 107-107, December 28, 2001.

Defense is compliant with applicable Federal financial management and reporting requirements.

(2) To develop a management plan for the implementation of the financial and data feeder systems compliance process established pursuant to paragraph (1).

(3) To supervise and monitor the actions that are necessary to implement the management plan developed pursuant to paragraph (2), as approved by the Secretary of Defense.

(4) To ensure that a Department of Defense financial management enterprise architecture is developed and maintained in accordance with--

(A) the overall business process transformation strategy of the Department; and

(B) the architecture framework of the Department for command, control, communications, computers, intelligence, surveillance, and reconnaissance functions.

(5) To ensure that investments in existing or proposed financial management systems for the Department comply with the overall business practice transformation strategy of the Department and the financial management enterprise architecture under paragraph (4).

(6) To provide an annual accounting of each financial and data feeder system investment technology project to ensure that each such project is being implemented at acceptable cost and within a reasonable schedule and is contributing to tangible, observable improvements in mission performance.[15]

To achieve this new Congressional mandate, the functional community within the Offices of the Secretary of Defense (OSD) and the MILDEPs—flowing from the members of the new Financial Management Modernization Executive Committee—decoupled various business activities from mission activities, creating stovepipes rather than integrated business and mission processes. This evolution of these stovepipes stemmed from the need for specific information at the enterprise and headquarters levels that historically was thought not to be available, accurate, consistent, timely, nor, in many cases, trusted. As a result, in order to obtain and trust the data, many in the OSD and MILDEP leadership ranks believed that they needed a hand in controlling the data sources and the processes and systems that produced the data.

Instead of focusing on issuing data standards in support of enterprise information needs, the functional communities chose to meet the need through control of the data via ownership of enterprise-level ERP system solutions. Because of this ownership, the functional stovepipe

[15] Section 1009(b), Public Law 107-107, December 28, 2001.

owners could now dictate the details of process execution across all of the operating units with the assumption that it is efficient for all units to do business exactly the same way, regardless of mission, customers, and span of the authority of the operational commanders.

In the early to mid-2000s, the DoD began investing billions of dollars in ERP systems. While the deployment of ERP systems helped to focus the Department-wide efforts at eliminating hundreds of unconnected and non-enterprise-level systems, more system consolidation still needs to be accomplished. Cutoff and cutover plans for migration away from legacy systems to end-to-end transactions contained within the ERP systems is being achieved at a much slower pace than originally anticipated. This failure to migrate legacy systems gets somewhat disguised by the re-baselining, re-planning, and re-programming activities associated with the various ERP system initiatives. For these reasons, even the most successful renderings of the MILDEPs' and Agencies' ERP systems are orders of magnitude higher in cost and schedule than anticipated at program inception. In addition, maintaining the legacy systems while continuing development and deployment of the ERP systems is another factor in the added overall implementation costs that are minimizing the efficiencies anticipated.

Thus far, the majority of the DoD's ERP system investments are with two Tier 1 ERP software vendors: Oracle and SAP.[16] Moreover, the implementation contracts for these larger ERP system investments were only awarded to a handful of system integrators (SIs). The government did not incentivize this group of SIs to work directly with the ERP software vendors so as to minimize customization of interfaces and extensions by leveraging the ERP system's native features.

Moving forward, there is a need for situational agility in DoD's ERP system investments. Changes—including software upgrades and added functionality—contained in emerging technology are a reality and must be accommodated in the Department's legacy and ERP systems environment. This reality is driven by the accelerated developmental rates of commercial IT, supportability of hardware (viewed as a commodity), and software applications. Consequently, the pace of technology change is adding pressure to acquisition timelines in the trade-off to ensure relevancy.

The lifecycle of technology, particularly software, is rapid and commercial software is now considered a significant cost investment for any public or private sector organization. The Federal Accounting Standards Advisory Board (FASAB) no longer considers software an intangible asset. Software is now categorized as a fixed asset, like property, plant, and

[16] Industry analysts also consider Microsoft Dynamics a Tier 1 ERP vendor. See Chris Shaul, "Top 10 ERP Solutions," *ERP Selection Help*, May 30, 2011, http://erpselectionhelp.com/top-10-erp-solutions/ ("Tier 1 is the largest systems which support the largest companies. Tier 2 is the middle market solutions serving companies of about $50 Million in revenue up to $500 Million. Often these solutions are scaled so that they roll out individual installations on a plant by plant basis. Tier 3 is for those companies under $50 Million in revenue and is designed for the smaller companies.")

equipment.[17] Furthermore, the design phase of software development is capitalized as well.[18] While the pace of technology continues to accelerate, business processes, organizational alignment, and business objectives are more constant. Therefore, logic indicates that software and technology should be integrated into the culture and into the business areas with the greatest chances of adoption to achieve success. Often, the exact opposite is occurring in the Department; thus, the need for situational agility.

C. Characteristics of the Legacy Systems Environment

Legacy systems continue to play a key role in the integration of both financial and logistics management data for current Defense business operations. The way in which legacy systems are managed (cutover/cutoff planning) requires significant improvement. Legacy systems plague the ERP system implementations across both the MILDEPs and Agencies well beyond their projected expiration dates.

> Stewardship is "the careful and responsible management of something entrusted to one's care."—*Merriam-Webster Dictionary*, m-w.com, January 4, 2011.

Legacy systems were built as bespoke or custom-made systems separate from each other. By design, there was a lack of congruency or standardization between systems. In addition, systems communicated in a variety of non-standard and often proprietary ways. As recent as the late 1990s, these processes sometimes consisted of transferring paper documents—via paper copies—from organization to organization for manual input from one system into another. Due to the manual rekeying of data, keypunch error rates were high, resulting in mismatches that caused late payment of invoices and inability to reconcile accounts.

When systems were able to communicate in the legacy systems environment, rarely were these interactions between systems bi-directional. More often than not, these interfaces were one directional even when interfaces existed between two systems. Systems were producers or consumers of data but not both.

[17] FASAB, "Statement of Federal Financial Accounting Standards 6: Accounting for Property, Plant, and Equipment," *FASAB Handbook, Version 10*, June 2011, page 16, Footnote 27, http://www.fasab.gov/pdffiles/2011_fasab_handbook.pdf ("Software and land [See SFFAS 10 for standard regarding internally developed software] rights, while associated with tangible assets, may be classified as intangible assets by some entities. In this event, they would be subject to amortization rather than depreciation. 'Amortization' is applied to intangible assets in the same manner that depreciation is applied to general PP&E—tangible assets.").

[18] FASAB, "Statement of Federal Financial Accounting Standards 10: Accounting for Internal Use Software," *FASAB Handbook, Version 10*, June 2011, page 2, http://www.fasab.gov/pdffiles/2011_fasab_handbook.pdf ("This standard requires the capitalization of the cost of internal use software whether it is COTS, contractor-developed, or internally developed. Such software serves the same purposes as other general PP&E and functions as a long-lived operating asset. This standard provides guidance regarding the types of cost elements to capitalize, the timing and thresholds of capitalization, amortization periods, accounting for impairment, and other guidance.).

The non-standard interfaces and data exchange formats made communications between these legacy systems difficult and error prone. Over time, some of these systems were retired or subsumed into larger ERP systems; but many still exist as data feeders to or data recipients of the ERP systems. The legacy systems generally accomplished only one function or set of functions and did not interoperate with other systems.

There are several factors associated with legacy systems that cause issues in an enterprise resource planning environment:

- The stakeholders who own the legacy systems are not always the same as those who own the ERP system implementations, resulting in mission objective conflicts (i.e., financial and logistics systems).
- The duty of legacy system owners is NOT to produce data for another system to consume that data.
- Legacy systems developed by the specific stakeholder organization may meet more than one need and thus include multiple operational functions, not just those required for financial or logistics management. The legacy system must be fully documented (architecture and code) to accommodate financial and logistics functions prior to moving relevant functions into the enterprise resource planning environment. Without automation and standards innovation, these efforts will continue to be high cost, predictably fail, and reduce the incentives to migrate.
- The priorities for budgeting to maintain and upgrade [e.g., service-oriented architecture (SOA)[19] enablement or modernization] legacy systems are driven by the stakeholder organization's mission priorities and not the ERP stakeholder's priorities. More than likely, any push from the ERP stakeholder will result in little impact on either resource allocation or movement of data.

By leveraging standards-based automated extraction and analysis solutions, the means and methodology exist to improve the current state of legacy systems for ERP system needs. If budgets could be put in place, the cost of addressing these legacy system issues could be reduced to 10 to 50 percent of any previous cost estimates. Additionally, all non-ERP system-related business processes can remain intact while all ERP-enabled functions migrate to the ERP systems. Some of the specific risks associated with continuing to use pre-ERP legacy systems in an enterprise resource planning environment are shown in Figure 2. The recommendations and potential solutions are explored later in this report.

[19] A SOA is "[a] collection of services. These services communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some activity." Anoop Singh et al., NIST, *Guide to Secure Web Services: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-9, August 2007, C-5, http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf.

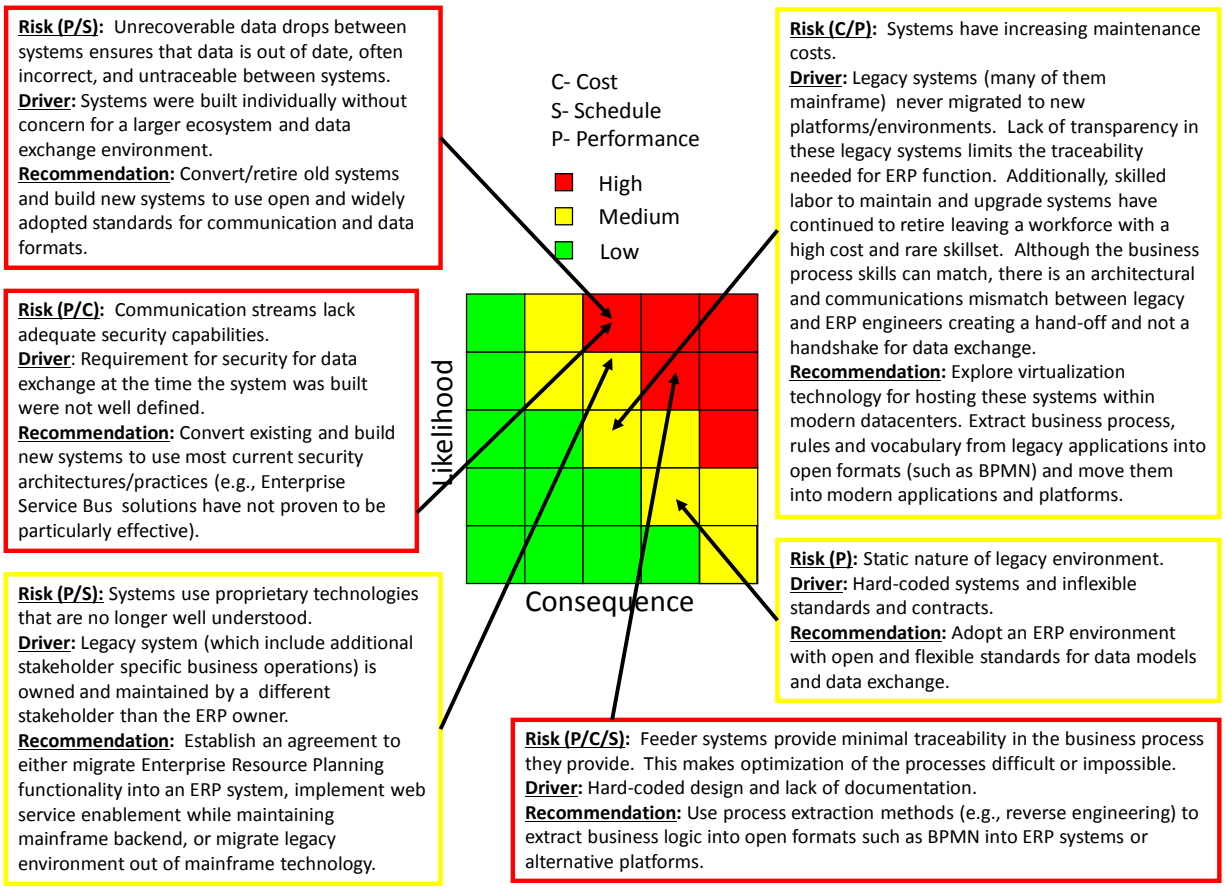


Figure 2. Risks and Issues with Legacy Systems in an Enterprise Resource Planning Environment

D. ERP Systems Environment—Today

The Department's ERP systems are expected to deliver integrated solutions across many aspects of business operations, including financial management, logistics management, human capital management, procurement, supply chains, and value chains. Prior to deployment, the ERP software vendor incorporates various functional modules (pre-integration), thereby minimizing the requirement for the customer to connect to disparate systems.

The MILDEPs and Agencies implemented ERP systems in anticipation of the following benefits:

- Seamless integration across and between functional areas and business processes, such as "Procure-to-Pay" and "Acquire-to-Retire" that, at a minimum, cross both logistics and financial domains;
- Enforcement of referential integrity across all dependent data elements;
- Transaction traceability and integrity;
- Typical business processes proven across thousands of implementations;

- Visibility of key information required for the effective and efficient management of the enterprise (i.e., progress of budget execution and asset visibility);
- Shared data models across the entire ERP system enabling functional modules to utilize complex data efficiently without building complex communications between the modules;
- Improved operational control of the enterprise;
- Incorporated leading practices for internal controls;
- Integrated cost accounting (limited by other factors in DoD); and
- Minimal manual intervention for reconciliation.

The MILDEPs and Agencies are using ERP systems as the primary enabler of business modernization and financial improvement. In the *Final Report on Defense Business Operations to the Congressional Defense Committees*, the Department reported the following on how it is using ERP systems to meet its business transformation goals within the MILDEPs and DLA:[20]

- Army: "[T]he Army is on an incremental path to an integrated architecture and interoperable systems for its general ledger accounting system (GFEBS) and its national and tactical logistics systems (LMP and GCSS-Army), thus giving the Army improved visibility of its financial and logistics assets. These are long-standing priorities for Congress, DoD[,] and the Army."[21]
- Navy: "[T]he Navy Enterprise Resource Planning (ERP) software, a key steppingstone to naval operations in a transformed business environment, was deployed at two of the Navy's four major acquisition commands (the Naval Air Systems Command and the Naval Supply Center). The major acquisition commands are the largest business concerns in the Navy. When fully implemented across the systems commands, Navy ERP will be the sole financial system managing more than half of the Navy's total obligations."[22]
- Air Force: "[T]he Air Force has worked to reduce transactional activities, establish transparent processes and consolidate functions while providing increased capabilities to the warfighter. This is being achieved through the utilization of Enterprise Resource Planning (ERP) systems, such as the Defense Enterprise Accounting and

[20] DoD, *Final Report on Defense Business Operations to the Congressional Defense Committees*, March 15, 2009, http://dcmo.defense.gov/documents/March_2009_Congressional_Report%20.pdf.

[21] Ibid., 39.

[22] Ibid., 45.

Management System (DEAMS) and Expeditionary Combat Support System (ECSS)."[23]

- DLA: "DLA currently employs its Enterprise Business System (EBS) across much of its supply mission area. As DLA's Enterprise Resource Planning (ERP) platform, EBS modernized and refined the agency's ability to manage the supply chain effectively and efficiently. EBS uses the ERP approach to manage seven of its eight supply chains and facilitate over 22,000 users operating in 28 countries worldwide."[24]

The Department confirmed this 2009 approach in its recently released *Financial Improvement and Audit Readiness (FIAR) Status Report*. During fiscal year (FY) 2012, for example, the DoD is dedicating $1,600 million or 82 percent of its $1,941 million FIAR resources on ERP systems to achieve audit readiness. Between FY 2012 and 2017, the percentage of total FIAR resources planned for ERP systems ranged from 75 to 83 percent.[25]

The Department anticipated that cost savings would be achieved as legacy systems were integrated into fewer enterprise-wide ERP systems, congruent modules within the ERP systems would subsume functionality, and, finally, legacy systems would be eliminated. Although some legacy systems were eliminated, many other legacy systems are still operational and redundant; hence, the DoD is bearing the high cost to maintain these systems. Throughout the Department, consequently, there is a duplication of functionality, capability, and data across these systems while few of these legacy systems are considered authoritative sources of data.

None of the ERP systems implemented in the Department spans the entire DoD enterprise. Rather, each addresses a particular set of functions in an organization or an entire MILDEP or Agency (e.g., DLA) within the DoD enterprise. There are many reasons why ERPs have not been adopted more widely across a MILDEP enterprise or DoD enterprise. Several of the reasons are explained in the remainder of this chapter.

1. ERP System Compliance with Federal Standards

When the Federal government embraced ERP systems, government leaders assumed that the ERP software vendors would ensure compliance with Federal accounting, information security, and other standards so the government agency user community would only have to test and verify performance results, not architect them. Ideally, compliance verification could be completed once for all Federal agency users. The reality is somewhat different, however, giving the ERP software vendor responsibility for compliance and the latitude to determine how

[23] Ibid., 51.

[24] Ibid., 58.

[25] Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *Financial Improvement and Audit Readiness (FIAR) Plan Status Report*, November 2011, IV-1, http://comptroller.defense.gov/fiar/documents/FIAR_Plan_November_2011.pdf.

compliance was accomplished. In the current environment, DoD's two ERP software vendors—Oracle and SAP—and the MILDEPs and Agencies are configuring their instances of those ERP applications independently, so the latitude for compliance continues to grow unmanageably.

2. Interfaces Between ERP Systems and Legacy Systems

Today, interfaces between the ERP systems and legacy systems are error prone and non-standard. The Department attempted to economize the interactions between systems by adding communication mechanisms—such as enterprise service buses (ESB) (see Figure 3)—to manage and process a multitude of independent connections [e.g., file transfer protocol (FTP) and secure FTP (SFTP)]. Many of these attempts at "plug-and-play" connections are unreliable because they are unverifiable, frequently lose data, are inefficient in managing large data transfers, and lack proper security. Older technologies are currently being used for these data transactions even when vetted alternatives are available at low or no cost (i.e., SOAP[26]/SAML[27], REST[28] for web service enablement, or the option of full ERP system integration).

To alleviate the consequences of these shortcomings, DoD built organizations and infrastructures [i.e., Global Combat Support System-Air Force (GCSS-AF)] to facilitate ESBs aimed at removing point-to-point system connections and standardizing the interface mechanisms. Once implemented, these communication hubs are rarely upgraded to use modern communication formats and protocols. This is sometimes due to legacy systems' inability to implement modern methods of data sharing or transfer. Communication between legacy systems and ERP systems is largely unsatisfactory due to the lack of traceability, transparency, comprehensive security, or understanding of the business process.

For example, an ERP SI attempted to replicate processes by using Oracle's Business Process Executive Language (BPEL) web service workflow manager. Workflow tools attempt to take the incoming data, apply business rules to it, validate that it is correct and uncorrupted, then place it in the appropriate tables in an ERP system's database. These workflow tools are good at

[26] SOAP is "[a]n XML-based protocol for exchanging structured information in a decentralized, distributed environment." Anoop Singh et al., NIST, "Guide to Secure Web Services: Recommendations of the National Institute of Standards and Technology," Special Publication 800-9, August 2007, C-5.

[27] Security Assertions Markup Language (SAML) is "[a] framework for exchanging authentication and authorization information. Security typically involves checking the credentials presented by a party for authentication and authorization. SAML standardizes the representation of these credentials in an XML format called assertions, enhancing the interoperability between disparate applications." Anoop Singh et al., NIST, "Guide to Secure Web Services: Recommendations of the National Institute of Standards and Technology," Special Publication 800-9, August 2007, C-4.

[28] REST stands for Representational State Transfer architectural style, which became the foundation for the modern Web architecture. Roy T. Fielding and Richard N. Taylor, Session, *Principled Design of the Modern Web Architecture* (22nd International Conference on Software Engineering 2000, Limerick, Ireland, June 9, 2000), 407, http://dl.acm.org/citation.cfm?doid=337180.337228 ("REST is a coordinated set of architectural constraints that attempts to minimize latency and network communication while at the same time maximizing the independence and scalability of component implementations.).

the *localized* process level within a small subset of an organization or one workflow. Unfortunately, the deliverable associated with a workflow tool is analogous to automating a paper process. The main drawback of these workflow tools is that they cannot span the segments of an enterprise to create truly enterprise-wide process flows without ensuring any loss of traceability. Therefore, no capability is possible with a workflow tool to optimize beyond a single interface for the enterprise. It is not clear if this is a limitation of the tool or how the DoD chooses to use the tool.

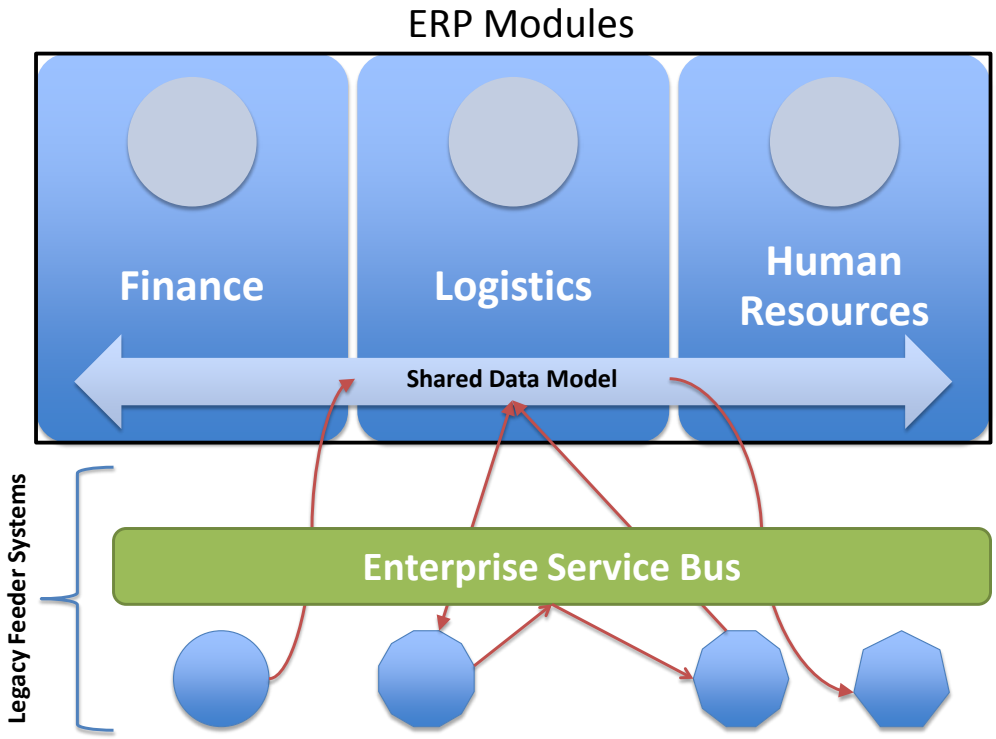


Figure 3. Relationship of Integrated ERP Modules, Legacy Systems, and Enterprise Service Buses that Were Intended to Improve Communications and Interfaces

3. Legacy Risks and Issues that ERP Systems Are Supposed to Solve

The Department identified ERP systems as essential to its efforts to transform its business operations. The major premise of this effort was to leverage principles and success factors earned over the last two decades as COTS software became the primary enabler of business transformation and growth for industry and various DoD organizations.

Implicit in this commitment to ERPs is an expected outcome of a Department-wide unqualified or clean audit opinion. Over the past few decades, Congress made several legislative attempts—most notably, the Chief Financial Officers Act of 1990, the Government Performance

and Results Act (GPRA) of 1993,[29] the Clinger-Cohen Act (formerly the Information Technology Management Reform Act of 1996),[30] the GPRA Modernization Act of 2010,[31] and various National Defense acts—to improve DoD business operations and increase information visibility with the desired end result of improving government performance.

In 2005, the USD(C) issued the Department's first FIAR Plan to "achiev[e] improved financial information and auditability."[32] The FIAR Plans of the MILDEPs and Agencies are combined into the DoD FIAR Plan to provide an integrated view of the financial improvement efforts across the Department's enterprise transformation activities. ERPs were seen as a key component of this transformation in the MILDEPs and Agencies.

An abbreviated summary of the major premises and expectations considered in the DoD's commitment to ERP systems are as follows:

- ERP systems reduce proprietary, unique interfaces between systems [e.g., import tools like BPEL (Oracle) allow importation of data from exported files into the shared data model in the ERP];
- Establishment of well-defined data models could allow the ERP systems to share data in standardized formats and enable interoperability between systems [e.g., Standard Financial Information Structure (SFIS)[33]];
- Interfaces would be real-time and not overnight batch processes;
- Business processes that depended on legacy system developers to hard code could be coded using repeatable methods;
- Faster and automated tools could remove much of the paper-based portion of business processes;
- Costs could be reduced by automation, efficiencies gained in processes, and in the number of personnel required to accomplish data intensive tasks reduced;
- Reducing or removing manual interventions could eliminate accounting inaccuracies by forcing transactions and changes in the ERP system to be completed in a traceable way;

[29] Public Law 103-62, August 3, 1993.

[30] National Defense Authorization Act, Division E, Public Law 104-106, February 10, 1996.

[31] Public Law 111-352, January 4, 2011.

[32] Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, "FIAR Plan Overview," *Financial Improvement and Audit Readiness Website*, last visited on January 12, 2011, http://comptroller.defense.gov/fiar/overview.html.

[33] See http://www.bta.mil/products/sfis.html.

- Users across a MILDEP, MILDEP organization, or Agency could use a single implementation of an ERP system (scaling is difficult or impossible using legacy and proprietary technologies); and
- DoD would have an opportunity to reduce legacy systems drastically; particularly targeting non-web-based, stand-alone, and unconnected systems. The costs reduction realized could be two-fold: (1) elimination of procurement costs, and (2) a reduction in maintenance costs.

4. Legacy Risks and Issues ERP Systems *Did* Solve

Despite early enthusiasm and high expectations associated with ERPs, DoD experienced a range of ERP organizational and execution characteristics and constraints. ERP systems are not intrinsically strategic; they are an enabling technology with a set of integrated functional modules serving as the core engine for transaction processing. An ERP system cannot and should not be used as a forcing function for organizational change management; rather the ability and willingness of an organization to change behavior, cultural norms, and processes are the prerequisites of a successful ERP implementation.

The IDA team evaluated where DoD's ERP systems did succeed (at least, partially):

- The shared data model fixed some data exchange problems and made the ERP system an authoritative source of data, especially within the ERP itself (the modules are well-defined and purpose built) (e.g., ERPs created commonality of interfaces via methods like FTP and ESB).
- Oracle and SAP ERP systems are beginning to handle SOA and XML data inputs, allowing better data exchange and reducing the number of transactions that require manual intervention.
- Oracle and SAP ERP systems reduced the scattered nature of many proprietary systems and hard coding of additional functionality. The problems associated with these proprietary systems were greatly reduced due to the widespread use of these ERP systems and the large developer communities.
- ERP systems have reduced some costs by eliminating paper-intensive processes. Cost savings have also been realized in legacy systems that were decommissioned or retired.
- Moving to ERP systems reduced manual interventions within systems. One important feature of ERPs is that manual intervention (by changing underlying data fields) is not possible. All transactions are logged in the system, thereby providing a high degree of traceability.
- Large vendors—such as Oracle and SAP—provide methods of scaling their ERP products across larger numbers of servers to accommodate more users.

5. Risks and Issues that *Remain* in the Enterprise Resource Planning Environment

The fundamental limitation facing any organization choosing to use an ERP solution is vendor *lock-in*. This is the inability of the organization to migrate out of the vendor's software solution to an alternate ERP or non-ERP solution. ERP systems provide certain core modules of functionality that are the ERP software vendor's intellectual property (IP). These modules deliver standardized business logic but are implemented as proprietary (corporate-owned) IP by each ERP software vendor. The result may be the same in terms of outputs; however, the business logic used to develop these modules is completely individualized in each vendor's implementation. Additionally, there have been no industry face-offs to test for input/output consistency across the ERP software vendor functional modules. Therefore, the configuration and inputs into the modules vary from vendor to vendor.

There is an additional contributor to lock-in. When an organization uses a functional module from a specific ERP solution, the ability to migrate to another ERP or non-ERP solution becomes tedious if not impossible. Each ERP system has a customizable business process component (e.g., Oracle's BPEL manager and PL/SQL) in which non-standard business logic can be created using each software vendor's specific language for the representation of the custom business logic that cannot be represented by the functional modules. This customizable business process component is leveraged primarily by the SI, who may or may not be incentivized to remove some of the customization as the ERP software vendor builds in more and more functionality and improves the functional modules in the base software product. Thus, lock-in is created by the dependency on the native functional modules in the ERP software and by the SI in the development of custom business logic in the software vendor's specific customization environment.

Since the functional modules are native in the ERP software vendor's IP, upgrades, corrections, or root cause analyses are controlled by the ERP software vendor and its respective release schedules. An abbreviated list of the risks and issues associated with DoD's ERP systems, including those previously addressed, are as follows:

- Vendor lock-in—that is, only two ERP software vendors produce a product with the size and scale needed in DoD as is currently being implemented. In contrast, there are dozens of software vendors and products available for smaller size and scale ERP implementations. Alternatives to ERP systems are described later in this document.
- Customization by SIs cause problems with upgrading and patching future releases of the ERP software (e.g., IDA interviewed a Tier 1 ERP software vendor, who recounted his frustration when he discovered that the SI "fixed" 400 problems when in fact the software vendor had already fixed over 100 of the 400 problems in the next scheduled patch. Subsequently, the SI's custom code was incompatible with the software vendor's patch, causing much of the customization to be redeveloped at further cost to the government customer).

- Non-standard data exchange formats lead to rejected data imports. A lack of traceability in this process leads to manual intervention resulting in frequent inaccuracies and missing or incomplete data.
- Outdated technical architectures and infrastructures cause testing and continuity of operations (COOP) environments to deviate from uniformity with production environments, which renders them unlikely to meet recovery time objectives.
- Instead of using widely available commercial options, such as commodity computing and alternative hosting, DoD continues to overpay for under-achieving IT services and infrastructures. This appears to be accepted as the cost of doing business in DoD.
- The MILDEPs and Agencies are still relying upon the ERP software to force organizational changes in behavior and in business processes in direct contradiction to the proven approaches of industry.
- ERP solutions are configured to scale vertically into larger servers in contrast to the horizontal scaling methods used by cutting-edge software. Horizontal scaling permits less powerful commodity hardware to be used in greater numbers to accommodate more users in multiple locations. Horizontal scaling also allows for fast ramp up/down of resources and scales dynamically to the current need. This reduces the cost of underutilized infrastructure and ensures nearly limitless scaling (i.e., data-intense software systems—like Facebook or Salesforce.com—scale successfully using these methods).
- A large number of transactions going through import tools (e.g., Oracle's BPEL) are kicked out into a queue where they must be manually reviewed, fixed, and approved to go back through the import process. This primarily manual process can take weeks, is tedious, and is error prone. Standard data models, common vocabularies, and traceable data exchange formats can improve these data exchanges and reduce error rates. Any manual intervention in the process also removes auditability confidence.
- Costs savings are not being realized at the rate or magnitude possible. Many legacy systems planned for retirement and included in the cost saving estimates during program planning are not yet sunsetted or sandboxed; thus, they continue to drain financial and personnel resources while adding functionality already resident in the ERP software. Alternatives may exist (e.g., BPM-based products that are discussed later in this document) that can be implemented on a smaller scale and integrated together to provide a higher implementation success rate using the same complete business process.

- Just automating a paper process has reached the end of its usefulness and new processes must be built. To move forward and achieve continued improvements in efficiency and automation, stove-piped systems must be disbanded and information and data must flow across organizations within the Department to form true enterprise solutions.

> "A car is not merely a faster horse
>
> And email is not a faster fax. And online project management is not a bigger whiteboard. And Facebook is not an electronic rolodex.
>
> Play a new game, not the older game but faster."
>
> —Seth Godin, *Seth Godin's Blog*, blog post, June 23, 2010, http://sethgodin.typepad.com/seths_blog/2010/06/a-car-is-not-merely-a-faster-horse.html (Godin is a bestselling author that "writes about the post-industrial revolution, the way ideas spread, marketing, quitting, leadership and most of all, changing everything.").

- ERP systems continue to rely on proprietary technologies that are incompatible across vendors. The lack of open standards contributes to vendor lock-in. Furthermore, customizations provided by SIs can cause incompatibilities between software implementations from the same software vendor.
- The majority of inputs into ERP systems remain as flat files transferred via FTP (e.g., as of June 2011, DEAMS had implemented 76 interfaces but only 13 are real-time).[34]
- Generally speaking, legacy or feeder systems do not support real-time interfaces. These systems are unable to use modern technologies with the benefits of real-time transactions, traceability of transactions, and security around transactions without expensive modifications or middleware. Nevertheless, legacy systems are not being turned off, retired, nor migrated as planned.
- Customization by SIs results in few ERP systems with the ability to exchange data compatibly. Moving data between legacy and ERP systems is tedious, error prone, slow, and frequently requires manual intervention to handle outlying data removing the possibility of auditability.

Overall, the migration to an ERP system generally includes a set of legacy business systems that requires consolidation and reconciliation of business logic into a more optimized set of business functions. The ERP software vendor community provides the functional modules that deliver the optimized implementations of the various aspects of business functionality (i.e., financial management, including a government accounting-specific financial module; logistics

[34] *Interface Details and Status*, (Interfaces v1.xlsx), document provided to IDA by the DEAMS Functional Management Office on June 21, 2011.

management; procurement; and human capital management). The ERP migration generally requires the analysis of a complicated legacy system environment, including both legacy systems targeted for ERP migration and those legacy systems not owned by the consolidating organization (or external legacy systems).

The legacy systems that are external to the ERP migration are usually owned and operated by stakeholders who (perhaps organically) grew these systems to include more than just the core business logic relevant to the ERP consolidation. There may be other business functions that are specific to stakeholder needs and customized to the environment, making the business system critical for daily achievement of mission operations. This extended functionality may not have direct value to the ERP migration; however, feeders from this business logic may contain or generate data required for the ERP system to have a comprehensive representation of the stakeholder's data for data aggregation or roll-up. For this reason, the legacy environment continues to be tethered to the ERP system while still in the control of the stakeholder who manages its funding stream for maintenance, upgrades, and possible future ERP migration.

Figure 4 summarizes the risks and issues with today's ERP systems environment in DoD and provides recommendations on how to manage the risks.

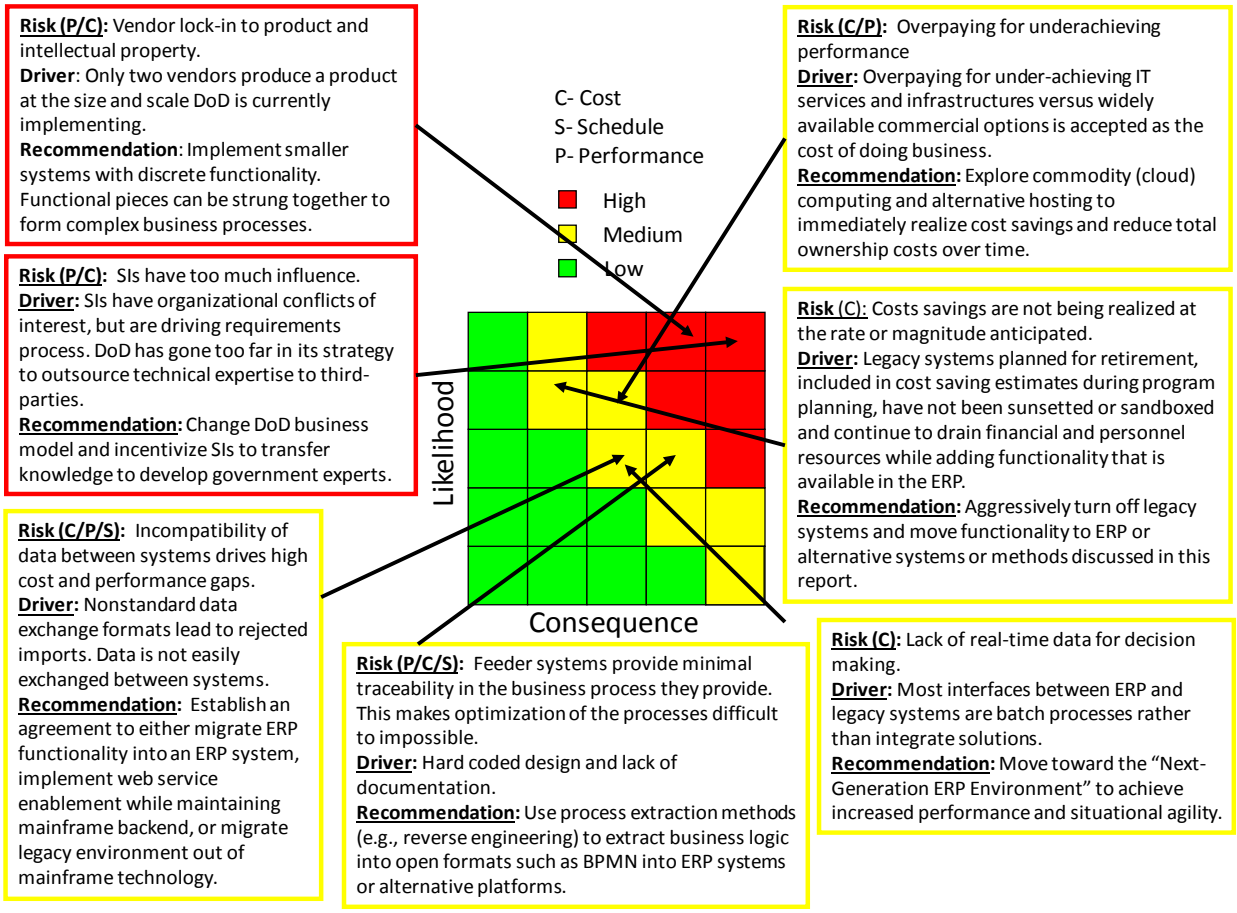


Figure 4. Risks and Issues in Legacy ERP Systems

3. Imperatives and Opportunities in the Next-Generation ERP Environment

With high expectations DoD implemented expensive ERPs, and now two decades later is in a position to evaluate with clarity their benefits and drawbacks. Facing the realities of a next-generation ERP environment, the Department must decide which ERPs have value and should continue, which ones to consolidate or otherwise transform, and which ones to replace with new approaches to data and emerging technologies. This chapter describes the data and technology drivers of change and the evolution of a customer-driven capacity path that characterize the next-generation ERP environment.

A. The Next-Generation ERP Environment

The next-generation DoD enterprise resource planning environment requires solutions beyond the traditional ERP and legacy systems that currently constitute it. This environment needs extensibility for evolving requirements. As with any enterprise business architecture, defining user needs—including anticipation of future needs for scalability and performance—is critical for delivering the optimal underlying system architecture. As system changes continue to occur, it is important to keep up with these changes while minimizing operational user impact.

With retail online banking, for example, the banking industry must accommodate regulatory changes continually. While the system architecture must keep pace with these changes, the impact to the customer must be minimal. The customer is unlikely to be knowledgeable about specific regulatory changes, nor care about them. Therefore, changes to operational systems are accommodated to avoid customer confusion and frustration while allowing for continued efficient daily operations. Any changes—architectural, business process-related, or low-level coding—may result in an exponentially proportional impact on the system but should not affect user experience. Designing for extensibility enables such changes to be incorporated while still meeting mission requirements.

There is a critical need to establish a reliable enterprise resource planning environment that can send and receive data on-demand, predictably, and with accuracy and integrity for processing and reporting. An example of an enterprise value stream that demonstrates this need is *order-to-cash*. Based on an industry standard, the order-to-cash value stream for a new order for a new customer requires the following steps: (1) a customer is established in the ERP accounting environment; (2) order entry is managed with the creation of an order and booking of said order; (3) order fulfillment is traced (physical or logical fulfillment); (4) order is delivered/distributed (physically or logically) and data is tracked; (5) invoice is generated and delivered to customer; (6) customer payments and collections are tracked and managed; (7) cash

is applied as payment is delivered; and, finally, (8) any deductions are made if invoice is "short paid" by the customer. The processes traverse both financial and logistics environments that rely on each other for sending and receiving data predictably to accurately track the operations for accountability. Data integrity and accuracy are also critical for reporting. Since these business processes are based on user-driven operational controls, separation of duties and measures that track these duties are required. Current DoD ERP system implementations do not address these issues with consistency; thus, there is a gap in meeting the 2017 auditability goal of accountability and traceability.

B. Need for Situational Agility

Today's DoD approach delivers situational awareness of the *mission needs*. The current approach also delivers reasonable situational awareness of *business needs*. Having situational awareness, however, is not enough, *situational agility* is also required. Situational agility is the ability to lean forward and predict how future technologies and analytical techniques may improve on or replace methods currently used in DoD business operations. The clean insertion and quick realization of benefits require agility in how the DoD applies contract instruments and in implementing technical modules.

Awareness alone does not provide an understanding of situational agility. Where the methodology fails is in the connection between the two—awareness and agility. Mission and business requirements need (1) *categorization*, (2) *prioritization,* and (3) developing a *trust model* based on the prioritization. These critical steps, not rigorously applied in DoD, enable the development of a common vocabulary set that is the jumping-off point or platform for defining functional requirements. These are the steps that enable situational agility. Although one might argue that DoD entities take these steps, they are not taken in the order required or with the discipline needed to obtain situational agility. Some of the benefits of situational agility include a more stable user environment and the enablement of a more extensible design.

Therefore, it is incumbent upon the Department's leadership to develop situational agility with regard to innovation to address business requirements with ERP and alternative solutions. This agility must be balanced with the DoD's need to continue making progress on more successful ERP program implementations while minimizing the potential loss of momentum or the addition of unanticipated costs in moving to another ERP or alternative solution.

1. Situational Agility: Technology

Changes including software upgrades and added functionality contained in emerging technology are a reality and must be accommodated within the Department. This reality is driven by the accelerated developmental rates of commercial IT, supportability of hardware (viewed as a commodity), and on-demand software applications. The pace of technology change adds pressure to acquisition timelines in the trade-off to ensure relevance and to meet users' needs at the point in time when a solution actually goes into production.

On December 1, 2010, for example, the U.S. General Services Administration (GSA) took a first step among all Federal agencies in moving beyond traditional ERP software vendors (e.g., Oracle, Microsoft, and SAP) when it announced selection of Google to replace an IBM solution for both its cloud-based e-mail and collaboration tools for its 17,000 full-time employees and contractors.[35] According to GSA, the cloud-based environment would save the agency $15 million over five years.[36] By July 2011, GSA's Administrator, Martha Johnson, announced:

> It's official! The U.S. General Services Administration is the first federal agency to successfully migrate its employees to a cloud-based email service using Google Apps for Government. GSA's successful transition is the first step in our effort to provide cloud email as a service option to other federal agencies.
>
> Our own transition to the cloud will save millions in taxpayer dollars annually. We expect that using a cloud-based system will reduce email operation costs by 50 percent over the next five years and save more than $15.2 million for the agency in that time. A large part of these savings will come from a decrease in the number of costly data centers requiring hardware, software licenses, maintenance, and contractor support. In addition to the cost saving benefits, the new email environment provides our agency with an easily accessible suite of services including email and collaboration tools that help GSA employees become a more mobile and more efficient workforce.[37]

During the six-month cloud-based email transition, Unisys migrated GSA's calendar data and content to Google Apps for Government.[38] According to Unisys, GSA will "benefit from new collaboration, such as direct access to onsite and remote colleagues through video chat and shared documents."[39] But this move to the cloud is not without its own set of challenges. For instance, "[t]he successes and challenges faced by GSA in implementing our new cloud email system," blogged GSA Administrator Johnson, "will help inform our decision making and allow us to better serve our customer agencies as they begin moving to the cloud."[40]

[35] GSA, News Release, "GSA Becomes First Federal Agency to Move Email to the Cloud Agencywide," (GSA # 10694) December 1, 2010, http://www.gsa.gov/portal/content/208417.

[36] Ibid.

[37] Martha Johnson, "GSA Is In The Cloud," *The GSA Blog*, July 26, 2011, http://gsablogs.gsa.gov/gsablog/2011/07/26/gsa-is-in-the-cloud/.

[38] Rutrell Yasin, "All of GSA's e-mail now in Google Cloud," *Government Computer News*, July 26, 2011, http://gcn.com/articles/2011/07/26/gsa-email-google-apps-cloud.aspx?sc_lang=en.

[39] Ibid.

[40] Martha Johnson, "GSA Is In The Cloud," *The GSA Blog*, July 26, 2011, http://gsablogs.gsa.gov/gsablog/2011/07/26/gsa-is-in-the-cloud/.

2. Situational Agility: Common Information Sharing

The DoD must control the business logic across financial, logistics, human capital management, and other business functions in lieu of ceding control to the ERP software vendor and SI communities. Today's ERP implementations depend on software vendor-provided functional (business logic) modules resulting in an inflexible lock-in for DoD operations and its business model.

DoD initiated SFIS in 2005 to develop a common reporting schema for its financial management (ultimately reporting into the U.S. Department of the Treasury).[41] An effort similar to SFIS should be developed for logistics, human capital management, and other non-financial business operations. To do so, requires the development of an ERP vendor-neutral, common business logic that enables consistent information sharing across the Department's other business operations. If inputs and outputs are defined, the business logic used for consolidating (aggregation as well as roll-up) and processing, the vendor-specific lock-in becomes less burdensome. Movement of data to and from SAP, Oracle, Microsoft, Appian, or other software solution providers then becomes manageable. An added benefit is that a common structure can reduce the amount of customization required by the SIs who might exploit these business logic gaps to deliver more services (e.g., customization, interface configuration, data translation) than is necessary. Evidence of these additional SI services and challenges of moving data seamlessly between software solutions is seen, for example, in the Air Force's ECSS or the current Army Enterprise Systems Integration Program (AESIP) process, where master data management formulations are being used to optimize data integration.

There is an unanswered need throughout the Department for authoritative data sources as well as dynamic and on-demand combinations of data for processing and reporting. There is also a need for data consolidation to accommodate:

- Business data that is fragmented and in disparate locations and systems; and
- Business information that is often duplicated or in conflict.

Bringing data together into actionable information is complex. Developing custom software continues to be an option to solve the integration problem. Conflicting standards in custom-developed software systems create a brittle environment where changing a process or data model may result in catastrophic breaks in the larger business process. An ideal enterprise resource planning environment should include a data architecture with data exchange standards so that individual systems in the overarching business processes are plugged into or out of the overall environment as the local processes or applications are changed.

[41] Under Secretary of Defense (Comptroller), *Standard Financial Information Structure (SFIS) Implementation Policy*, Memorandum, August 4, 2005, http://dcmo.defense.gov/products-and-services/standard-financial-information-structure/SFIS/SFIS_Policy_Memorandum.pdf.

When addressing a legacy enterprise resource planning environment and its associated non-ERP systems for consolidation or migration, updating authoritative data sources and delivering dynamic and on-demand combinations of data for processing and reporting requires a common vocabulary. This implies defining a common vocabulary, extracting data terms (persistent), and extracting data structures (including any related business rules) from the legacy enterprise resource planning environment. This extraction can be completed using multiple manual or automated methods, which are discussed in detail in Chapter 4's "Knowledge Extraction to Enable Transparency" section.

The extraction of the various data terms and structures along with associated rules provides the transparency needed to address any gaps for ERP migration or system consolidation. With the gaps addressed, a common and updated vocabulary can be developed to deliver a more comprehensive and agile data architecture for the "*to be*" enterprise resource planning environment.

This new data architecture is required whether migrating out of the existing legacy ERP system(s) or consolidating systems through the application of such techniques as master data management (MDM) or data virtualization. Ultimately, these common characteristics of data will be addressed:

- **Metadata abstraction:** the logical characteristics of the stored data such as location, storage structure, application programming interfaces (APIs), access language, and technology.
- **Data convergence:** the connection of differing data sources to make them accessible by using an integration, mapping, or consolidation point.
- **Transformation/integration:** the reshaping of dynamic data into new values, improving quality of dynamic data, and the merging (add/subtract/multiply/divide) of dynamic data for new results.
- **Flexible data delivery:** the publishing or reporting of result sets of either static/dynamic data or data services by consuming applications or users on an on-demand basis.
- **Data federation:** combining result sets from across multiple source systems.
- **Data virtualization:** addresses requirements for data security, data quality, data governance, query optimization, and caching.

Data architecture serves a critical role in business mergers and acquisitions in the banking industry. During the acquisition of Wachovia Corporation by Wells Fargo & Company, for example, a need existed to extract data terms and data structures from the respective banks' operational environments to develop a common vocabulary and consolidate systems for optimizing operations while minimizing change to its customers. Achieving a common vocabulary required the merging of terms with the same meaning. In this case, each bank likely

defined customer number many ways (e.g., "custnum," "custno," "customer number," and "CustN"). Extraction of the data terms (i.e., discovery) and developing a common term (i.e., an alias) and associated data structures and rules consolidation, enabled Wells Fargo to address migration into a new environment or system consolidation using MDM or data virtualization techniques quickly. Similar analogies to the customer number can be constructed for human capital management components, such as annual leave where differences exist between the Air Force and Navy definitions.

C. Master Data Management and Data Virtualization

For legacy ERP and non-ERP system consolidation, two techniques can be used to bring together a set of systems together—MDM and data virtualization. MDM is applied when two or more organizations and their respective systems need consolidation but must retain their own governance, policy, and trust models (e.g., consolidating an Army system with a Navy system). MDM allows real-time translation *between* multiple data models. In contrast, data virtualization is usually applied when two or more organizations and their respective systems need consolidation and their governance, policy, and trust models are also being consolidated. Data virtualization allows for the *combining* of data models for this type of consolidation.

MDM brings together diverse information (e.g., customers, products, and suppliers) into a single view for business data for real-time applications. Although MDM is typically considered a significant financial and staffing investment to implement, the benefits when dealing with disparate environments may be worthwhile because it creates a data federation across multiple source systems. In the DoD enterprise resource planning environment, since there is no predefined DoD schema for logistic management, human capital management, and other business functions, the data inputs and outputs and the logical structures may vary from organization to organization making it difficult to take an output of one ERP system and easily migrate that data into another ERP system. In addition, each organization may have its own method of defining the data structures and terminology. By establishing a mapping schema through the use of MDM techniques, an organization like the Army can integrate its various ERPs into a consolidated environment. This does not remove the maintenance or upgrade burden of the current unconsolidated ERP modules below the MDM structure; it merely provides a mapping for communicating across the various Army ERP systems.

Both the Army and the Navy are beginning to use the basic foundational approach of MDM. The goal is to provide a set of processes for collecting, aggregating, matching, consolidating, assuring quality, and persisting and distributing non-transactional data (i.e., customer details) as it exists in an organization. This ensures consistency, controlled maintenance, and proper application of this information. These common vocabulary sets developed by any organization are used as a baseline. When MDM is applied across multiple stakeholder vocabulary sets, a mapping is established to retain the integrity of the persistent data while providing a mechanism for aggregation.

The DoD business community is now embracing the concept of MDM. MDM is essential for both the Army and Navy due to their multiple ERP system implementations that address the various aspects of their business operations. Each MILDEP has stakeholders with specific and specialized business and mission operations. Consolidation into a single ERP system is not efficient, recommended, nor viable. MDM, however, provides an avenue for addressing the data integrity and aggregation. To keep the integrity of the business objectives intact, further integration of these MILDEP-specific enterprise resource planning environments is critical.

Data virtualization (or data federation) is a newer technique with a set of technology products provided by various vendors. Although the extraction of data terms and data structures and the development of a common vocabulary are still required steps before applying these vendor solutions, the vendor offering (typically a combination of products and services) provides a quicker approach to data consolidation and integration. The value of this approach is that:

> IT staff becomes more agile because new business-line projects don't involve writing a ton of code to glue systems together in a point-to-point manner. Instead, new projects are quickly implemented because the IT staff is focused only on the business logic required and not the integration work that needs to be done to bring together the right view of the information. The job of data integration is done by the data virtualization product, and the mapping leveraged by this type of product is reusable from project to project. Additionally, using data virtualization products reduces the complexity of changing the IT environment. For example, if we want to migrate from Siebel to SAP, then the existing applications don't need to change. Instead, we simply change the mapping inside the data virtualization server of the customer name, … and our existing applications will run unaltered.[42]

This approach works best where the organizational governance, policy, and value streams are streamlined, trust is clearly defined, and the trust model is in operation.

According to John Goodson, who is an executive leader of the Enterprise Data Solutions group at Progress Software and a well-known data connectivity expert, "[d]ata virtualization systems are well suited for integration across systems where there is a trusted information source, and where data is needed real time, but the exact type of data is not known when the application is designed (i.e., information will be requested and updated via queries)."[43] Based on Goodson's recommended steps, Data virtualization technologies approach the single view problem differently from MDM:

[42] John Goodson, *Data Virtualization Provides a Single View Into the Enterprise*, Data At Your Service blog, March 1, 2010, http://www.ebizq.net/blogs/dataservice/2010/03/data-virtualization-provides-a-single-view-into-the-enterprise.php.

[43] Ibid.

1) "[I]dentify what attributes of a customer's data are required (and available). For example, company name, billing address, shipping address, primary contact name, phone number, email address, purchase history, lifetime value, date of last customer support call, etc."

2) "[I]dentify what systems supply the most trusted pieces of this information."

3) "[C]reate a data model within the data virtualization software to define these key entities and create a physical mapping of where the information exists (or how it can ultimately be computed). For example, the customer account number comes from the SAP system, the customer contact is in Salesforce.com, the last support call can be obtained from People[S]oft, and the lifetime value can be found by summing order totals in the homegrown Oracle billing system."

4) "[D]efine where the data virtualization software can find the information when requested to do so (this is sometimes called creating the data model, the common model, or the business object model)."

5) "[R]etrieve the information from these disparate systems real time when requested – that is, to virtualize the data when requested to do so. For example, a customer service rep will want to receive the customer's contact information, what products/services they own, a flag to indicate if they've paid their bill, and a brief history of their prior call history… ."[44]

D. Alternative Options for Data Exchange

1. Open API System Environment

A systems environment with open APIs allows for an ecosystem (e.g., an enterprise resource planning ecosystem) where functionality of one application can build on top of the functions and capabilities of other systems in the environment. This is analogous to the evolution from single line code (e.g., Fortran) to inheritance languages (e.g., C++) that build on existing and proven code. Application developers throughout the organization can use published APIs (or services) and knowledge about other systems to integrate these APIs into their applications. This allows the new application to build upon an existing implementation through the API rather than rewriting what other application developers have already done. Having linkable data enables the combining of data sources for the purpose of meeting business and mission objectives. Once external reference points (outside the application) to authoritative data sources exist, information can be joined to create insights into business operations that were not possible before.

[44] Ibid.

In the open Internet environment, there is a proliferation of published, open APIs that are accessible to layer additional functionality on top of other software tools. Because of a wide array of available APIs, application developers now can choose from an abundance of pre-built functionality to incorporate into their applications. In addition, newer applications make use of these APIs to provide more context and better user experiences. Free flow of data between applications allows for the creation of complex capabilities from simple capabilities that can be strung together in novel ways. Each capability, once published to an API, becomes a building block to assemble in larger processes.

The DoD could arguably adopt a similar model where different MILDEP and Agency organizations create capability and functionality in APIs and then offer those APIs to anyone else within the Department who needs the data or process. Capability is created once and then reused (rather than recreated from scratch or purchased) by each organization needing a particular functionality. Such API offerings would help to optimize resources across MILDEPs and Agencies.

Open APIs are something DoD must *do,* not something it can *buy.* The concept proposed here cannot be purchased as a product or as a service from an SI; rather, it requires a cultural shift in the Department by requiring organizations to treat their systems as enterprise-wide capabilities and not restrict their usage to their own MILDEP or Agency. The power of open APIs is the advantage created in a federated system environment. This requires an environment that goes beyond leadership to an era of stewardship as the baseline for managing the Department's IT investments. An investment must have a common purpose that achieves an outcome beyond just one MILDEP or Agency.

For example, federated system environments contain loosely coupled systems that communicate using APIs and interoperate to deliver orchestrated capabilities beyond an individual system's functionality. Each of the federated system environment's systems can be easily replaced without impact on other systems (with the exception of those systems dependent on the output from the replaced system). Changes to a system's backend should not affect consumers as long as the published API remains the same. While maintaining the functions and capabilities provided to other systems, systems and processes can be optimized in this way.

Since published APIs or API services are widely accessible, building new functionality or processes is simply a composition of existing services. The best API services available (authoritative data sources) can be used internally and externally to DoD to provide the best possible solutions without building a large-scale architecture for each new system or capability. Conversely, a larger system can create software lock-in with slow, cumbersome, and expensive-to-change processes. The building blocks of a federated system environment with open API-based enterprise-wide processes are flexible and can adapt to a changing business environment as needed. This enables the highest impact solutions at the lowest total cost.

Open APIs also afford the DoD the opportunity to enable a consumer system to build the interface itself without requiring stove-piped development efforts. Since APIs can be used by multiple organizations, once one organization is using the APIs, others can expect a similar level of performance. Unfortunately, current interfaces are largely negotiated individually between two system owners, resulting in inflexible arrangements, high servicing costs, and the inability for reuse by another organization.

2. Trust Requirement

The lack of trust between data producers and data consumers is an issue in the DoD. Program managers are not incentivized to deliver a completely factual report on their program's status to leadership since anything negative reflects poorly on their performance or may result in cuts to the program's budget. This lack of trust drives excessive oversight, which in turn, negatively affects program execution. One driver of this problem is the use of oversight and compliance data that is separate and distinct from the data used to monitor the system's daily operations. A well-defined API platform will use the same APIs for monitoring a system's daily operations as it does for reporting on the system's status to third-parties (e.g., an application status dashboard). This ensures that data and information available to oversight entities is the same as and available at the same time as the data is available in the application itself. This may cause short-term discomfort but will result in long-term gain for all.

Companies—like Google, Facebook, Twitter, and Foursquare—allow users to obtain additional functionality or capability without requiring explicit licenses for an application. For example, Foursquare provides a service that logs user location via a user's mobile phone. A second service: "Where next?!" ("A quick and easy way to answer the question: 'Where should I go for lunch today?'"),[45] takes a user's last location from Foursquare, notes the specified time of day, and sends the user a list of nearby restaurants. "Where next?!" is not affiliated with Foursquare and only requires a secure token containing the user's authorization to get the required data to present this new functionality. This simple example demonstrates what can be accomplished by stringing multiple services together. Here a record of location and a time preference for lunch are leveraged along with a directory of food establishments and their locations. The result is increased utility for the user without rebuilding any components of the federated system. Each API service (with an inherent trust model) provides expert functionality and, by stringing the data together, a new capability is created that could not be offered by one of the individual services.

Unplanned and unexpected functionality may be created in this manner as the number of building blocks of services increases. The DoD's ERP community of interest (COI) must build trust and take ownership in the development of an open API that results in the exchange of

[45] https://wherenextapp.appspot.com/

services, data, and the composition of both for an optimized set of business systems. Even if the utility of groups available to be joined is very small on a peer-group basis, eventually the network effect of potential group membership can dominate the overall economics of the system.

3. Democratization of System Design

A fundamental issue with a consolidated monolithic approach to system design is that it results in a set of characteristics that are unwieldy and inflexible, which is orthogonal to the dynamic nature of both system and mission requirements. Unfortunately, the DoD enterprise resource planning environment developed these characteristics. While some DoD ERP system implementations have shown characteristics of organizational efficiency in specific functional areas, the flexibility needed in today's enterprise resource planning environment makes for incompatibilities and unnecessary investments. Additionally, the budget size and enterprise impact within a MILDEP or Agency of these DoD ERP solutions caused decision making to rise to levels higher than necessary, abstracting it away from the stakeholder(s) with the necessary ongoing operational interest to lead to successful implementations.

The concept of democratization of system design introduces the idea of bringing the requirements and the decision making for the optimal system solutions down to the broader operational stakeholder community. A balanced trade-space decision environment is then created in which traditionally stove-piped stakeholders are brought together to democratically trade off and prioritize requirements and, ultimately, make decisions for delivering optimal solution across the organization to fulfill mission needs. Although not a new concept, DoD's stove-piped enterprise resource planning environment creates inefficient implementations in which many cross-enterprise stakeholder requirements are not met.

Democratizing the full business process into smaller functional portions allows optimization at the local functional level. End-to-end business processes are complicated and include many interconnections. Allowing local functional stakeholders more control over data products and flows encourages better implementations because they have the best ideas for what needs to be accomplished and generally know the most efficient ways to achieve them. Starting with small systems (with only a few functions) and connecting them together embraces the chaos of a large business process that mirrors the real-world implementations. Over time, larger processes built from the connections between these small systems can become more efficient by cutting out some of the unnecessary steps or optimizing flows of data. The stakeholder group responsible for the results handles each portion of the process, and because that portion is a small system, it can be more quickly and easily modified or replaced with a more optimal system or service in the overall process.

For example, the Interstate Highway System is a nationwide network of roads. When a highway requires an update or change or integration with other roads, states and cities/municipalities take responsibility, not the Federal government. While the funding may come from the Federal government, the local governments better understand the traffic flows,

weather, and materials needed. Local governments have a better understanding of time, costs, and readily accessible resources for a given geographic location. A similar analog exists for the Department of Veterans Affairs' Veterans Health Administration's associated hospital network that provides medical service through a distributed and democratized health delivery approach.

E. Producer/Consumer Data Exchange Model

One way to view the interactions between organizations in DoD is to consider that they are merely passing data between each other. One organization's financial management personnel complete a number of processes based on data inputs (possibly transaction data) from other organizations that conduct those transactions. These personnel in turn complete a set of processes and produce new data that is passed to another person, organization, or system for further processing.

By considering these interactions purely as processes and data exchanges, all involved in the exchange model are merely producers and consumers of data products. When linked with responsibility and authority management principles, this enables the Department to realign missions to produce data for other data consumers. Some interesting properties emerge:

- If a system is a data producer, but there is not a data consumer of that data product, the system producing the data is either not needed or the Department is missing the capability to consume and process that data.
- Over time, each system can consolidate its functionality into a core set for data production. As a consequence, each type of data will be pushed into a single authoritative source for that data. This results in reducing data duplication and making clear where to go for a particular set of data.
- Data flows can be optimized across the enterprise using graphics from data reduction techniques.

Producers of data are responsible for producing the best data product, but are not responsible for the use of the data. Conversely, consumers of data are responsible for their processes based on incoming data but are not responsible for the quality of the incoming data. This is contrary to current principles where system owners often duplicate data sources or even data production to obtain a high level of assurance of data correctness (or assumed data correctness). By moving toward a data producer/consumer model, the DoD can make the process of consuming and producing data the core competency of the group adding their value in that processing. In the end, the data producers and consumers will only need to concern themselves with the focused responsibility of their role and function and not with the extraneous activities associated with other roles and functions.

F. Roll-up vs. Aggregation of Data

1. Roll-up of Data

When data is *rolled up*, a snapshot is taken of the data in the producer system where it resides. Roll-up data is static; whatever data is currently in the system is exported—no changes (e.g., edits, additions, or transformations) can be made until the next data export. The exported data is limited to what is in the export—that is, no further questions can be asked of the data. In some cases, identification (ID) fields are exported from the producer system; however, in many cases they are not. The ID fields are required to link the exported data back to the source of the data, which is lower than the system and table level in the database. Without this ID field information about the source of the data, it is impossible for a user to drill down on the data any further than what is contained in the export. Data in the producer systems may be highly relational; if it is, then the static export removes the ability for consumer systems to exploit the relational information.

The data contained in exports is usually defined via agreements [e.g., a memorandum of agreement (MOA)]. Changing the content of an export is difficult because any change may require renegotiating said agreements. This may mean that positive changes in the data available in the producing system cannot be used by the consuming system until the data-exchange documents are amended. For example, in DEAMS, the Air Force system of record, approximately 87 percent of its interfaces utilize roll-up methods of data exchange.[46] In many cases, this data is then copied into static documents (i.e., PowerPoint slides or reports). Since the data is not dynamically driven (or even if dynamically driven by a consumer system that does not dynamically update from the producing system's data), what is displayed to decision makers is typically incomplete and out of date.

Roll-up data is useful if the consumer will never need to obtain a different level of detail about the data to produce a useful product or make a key decision. Unfortunately, this is almost never the case. Therefore, roll-up data should be restricted to raw data (such as transactional data) and rarely used for any data involving summaries of data for information or knowledge products.

2. Aggregation of Data

Aggregation of data is a dynamic process with various types of data, including non-hierarchical, dynamic, and referential. Data is referenced rather than copied or exported so that, as the original source data changes in the producing system, so too should the data in the consuming system. As data is aggregated, it is combined as needed to produce results at a correct

[46] Document provided to IDA by the DEAMS Functional Management Office, "Interface Details and Status," (Interfaces v1.xlsx) on June 21, 2011.

level of output. Aggregation can include various data elements, elements that tie together two or more data sources, elements that analyze and create new information from inputs, or user interfaces that display or collect information and data. Over time, the number of systems and the overlap of functionality between systems can be decreased due to aggregation.

For instance, in an aggregation one might say "we spent $1 million on staffing in science and technology (S&T) areas and $3 million on other resources so the total Quarter 1 cost is $4 million." Notice that at a high level, the result is the same, but the aggregation of the data allows a drill down into that data to see the breakdown of that total cost of $4 million. The advantage of this method is that a high-level decision maker can get lower levels of detail as needed but without being forced into reviewing too much detail (or looking at the raw data directly). In a standards-based and properly integrated collection of systems, the drill-down can happen almost instantly and seamlessly. This can be accomplished since the consuming system is referring directly to the data in the producing system rather than referring to a copy of the data at a high level that was imported into the consuming system's own tables. To some extent, such interaction is possible because the data requirements were not specified in advance. The consuming system stated that it needed the quarterly S&T cost numbers. In contrast to roll-up data methods, however, because it is aggregating the data from the source system directly, a decision maker can drill down in many areas without having to agree contractually to have those areas of detail exported.

A common method of allowing aggregation of data is to provide open APIs for the data. Instead of requiring a contractual process to change what data is exchanged, the consuming system is focused on satisfying user requirements based on the APIs so that the contract requirements only need to address access control management.

Aggregate data methods should be used in almost all cases. As DoD systems become increasingly linked and start to be hosted in dynamic commodity computing environments, the data model will need to evolve from data ownership to data stewardship. The aggregation concept becomes increasingly important to allow decision makers and system architects to build effective systems with a minimal amount of inefficiency and duplication of effort across the DoD enterprise.

G. Getting Ahead of the Vendor Curve[47]

As a result of the government's major outsourcing of technology expertise over the past two decades, the ERP software vendors and SIs that are awarded government contracts are a significant source of information in determining the chosen technologies and implementation timelines.

[47] For additional information, see Mark Fabbi, Vendor Influence Curve: A Model for Dealing with Major Vendors," Gartner, Inc., February 6, 2007.

Consequently, the Department finds itself in a vendor-driven implementation curve for these ERP system implementations. To get ahead of this curve DoD needs to demand solutions from the ERP software vendors and SIs that are current, relevant, and optimal for the Department. Government personnel providing oversight for systems, such as ERPs, must become as knowledgeable about their implementation as the ERP software vendor or SI, which is rarely the case today. DoD must invest in upgrading specific skill sets of the department's information technology and program management workforce to avoid substantial configuration and (if appropriate) customization of proprietary systems.

Considerable amounts of time were and continue to be invested in mapping the Department's *"as is"* environment of today while ambiguity exists in the "*to be*" environment of the future. A nagging question about this ambiguity is whether the monolithic approach of all-encompassing ERP systems will achieve the business transformation desired. Simpler, yet functionally rich, solutions are now available as industry has evolved to a more global solutions set.

Figure 5 shows how the path from "*as is*" and "*to be*" is a continuum putting the client and its software vendor/SI support in a cycle of updates/upgrades and maintenance. This continuum has an upper and a lower pathway. The top path is defined by the software vendors and SIs. The software vendor listens to what the customer says it wants—typically referred to as the "voice of the customer"—and implements partial or full features to accommodate those stated requirements. A software vendor is also incentivized to listen to customer feedback and incorporate the features into its existing solutions in the least expensive ways possible.

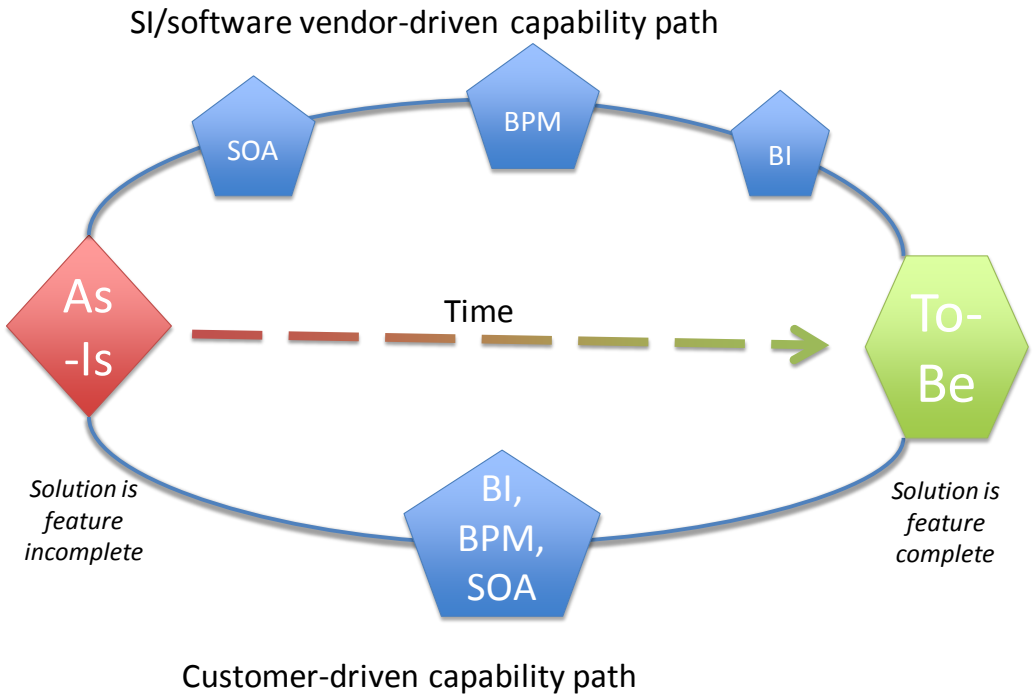


Figure 5. Vendor Curves: Either SI/Software Vendor- or Customer-Driven

Over time, a software vendor will incorporate additional features and technologies into its product offering, but initially a bolt-on solution is less expensive than new development. It meets the stated customer requirement, complies with a standard, or both. These initial bolt-on features, however, are frequently expensive, custom, and may underperform. In addition, the bolt-ons become a revenue stream for the SIs even after new features become available in the underlying software product.

The SI is incentivized differently than the DoD. Its goal is to maximize billable revenue, often accomplished by staffing large numbers of personnel who do not require additional training for a project. Smaller increments of technology (rather than rapid changes of systems) are better for the SI as the installation, customization, and maintenance revenue is similar but at significantly reduced costs. Additionally, over time, an SI's ERP experts leave the project and are often replaced by more junior and less knowledgeable staff. Consequently, the SI team is not as capable of quickly integrating new features, and may not be as knowledgeable of the features that exist.

In many cases, features or technologies are implemented with high hopes of success only to be implemented so slowly or in such complex ways (requiring additional licenses, intermediary contractors, expensive maintenance, and customization fees) that the customer ends up believing the technology was not worth the effort or cost to implement.

The lower path in Figure 5 is customer-driven. In this path, the customer defines guidelines, features, and timelines. The customer defines the future he wants and is not be driven by the software vendors or SIs. In effect, the customer is saying, "I know the future my organization wants, believe it is achievable by this date, and will no longer purchase non-optimal solutions that do not satisfy the requirements as we defined them." Hence, skills in business and technology are required by the customers, not administrative skills.

The customer-driven path is the best path for the Department. To take advantage of the customer-driven path adequately, however, the Department needs highly qualified government employees with the technical understanding to design and drive implementation of the path the Department needs. To demand the right technologies and implementations from the software vendors and SIs, these individuals must make a commitment, as a condition of employment, to remain in their positions long enough to make a decision and see it followed through on the project.

Currently, the SIs and software vendors take the lead in developing mission requirements, value streams, and vocabularies because the government does not have the skill sets or because the individuals who gain on-the-job experience leave for better positions before project completion. This means the Department is constantly in the low end of the innovation curve. Rather than adopting the best technologies and system methodologies, the Department is implementing what is convenient and resource effective for those who are both selecting the technologies and profiting from the implementation and maintenance.

While serving as the Federal Chief Information Officer for the White House, Vivek Kundra repeatedly referred to this arrangement as an "IT Cartel." During a July 2011 speech to the President's Council of Advisors on Science and Technology, for instance, Kundra stated, "We almost have an IT cartel within federal IT, where we have very few companies. These companies, frankly, a lot of them benefit because they understand the procurement process better than anyone else, not because they're providing superior technology."[48] A few weeks later and just after departing his post at the White House, Kundra more fully explained his earlier comments in an opinion piece to the *New York Times* that the cloud provides an escape from the IT cartel of private contractors:

> As the global economy struggles through a slow and painful recovery, governments around the world are wasting billions of dollars on unnecessary information technology. This problem has worsened in recent years because of what I call the "I.T. cartel." This powerful group of private contractors encourages reliance on inefficient software and hardware that is expensive to acquire and to maintain.

[48] Jory Heckman, *Kundra seeks broader vendor pool*, Federal News Radio, August 3, 2011, http://www.federalnewsradio.com/index.php?nid=110&sid=2460112.

> In one particularly egregious example of waste, the Defense Department last year pulled the plug on a personnel system devised by Northrop Grumman after spending approximately $850 million on it in 10 years.
>
> When I joined the Obama administration as the chief information officer, we quickly discovered vast inefficiencies in the $80 billion federal I.T. budget. We also saw an opportunity to increase productivity and save costs by embracing the "cloud computing" revolution: the shift from hardware and software that individuals, businesses and governments buy and then maintain themselves, to low-cost, maintenance-free services that are based on the Internet and run by private companies.[49]

The most critical risks association with implementing a successful next-generation ERP environment and recommendations for addressing those risks are summarized in Figure 6.

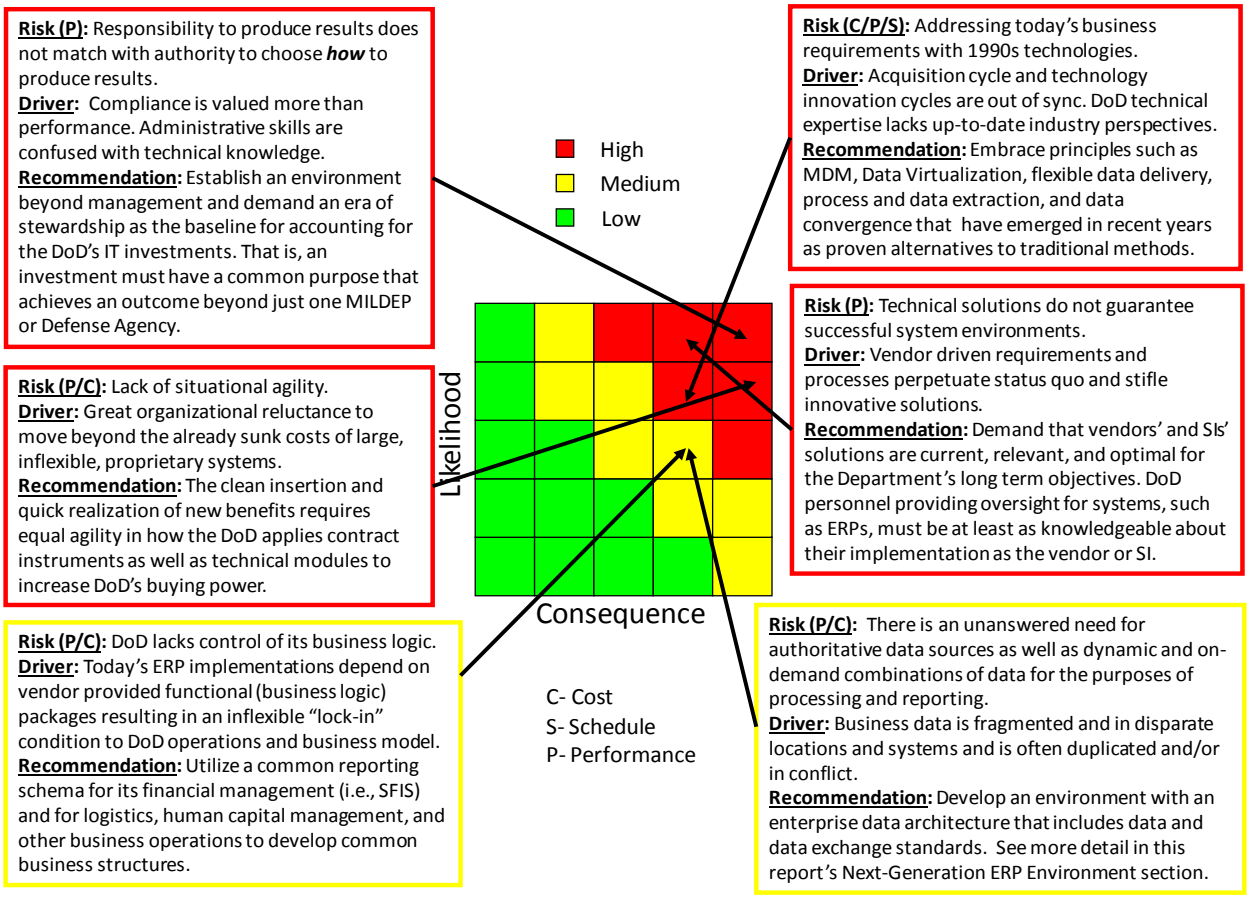


Figure 6. Risks of Moving to the Next-Generation ERP Environment

[49] Vivek Kundra, "Tight Budget? Look to the 'Cloud,'" *New York Times*, Aug. 30, 2011, http://www.nytimes.com/2011/08/31/opinion/tight-budget-look-to-the-cloud.html?_r=1.

4. Next-Generation Technologies and Standards

The challenge for DoD is to determine how to move from its current reliance on ERPs, vendors, and SIs to the next-generation ERP environment. In this chapter, the IDA team explores emerging technologies and standards for their potential for software systems, and raises the alternative to large pre-integrated sets of functional modules of smaller distributed systems.

A. Technology/Standards Enablers[50]

New standards and technology enablers can provide significant efficiencies for optimized performance and cost reduction. This section describes these enablers and the value they can provide to an enterprise resource planning environment.

The international standards for cost-effective enterprise resource planning environment change management include:

- Knowledge Discovery Metamodel (KDM): An International Organization for Standardization (ISO)/Object Management Group (OMG) standard providing ontology (a set of definitions) for system knowledge extraction and analysis. KDM provides a framework for the capture of code, platform, and other software system characteristics. This further allows the extraction of data flows, control flows, architectures, business/operational rules, business/operational terms, and the derivation of business/operational process; the extraction can be delivered from source, binary, or byte code. Additionally, the intermediate representation of the extraction is in executable models creating the possibility of simulation and code generation.
- Business Process Modeling Notation (BPMN): An OMG standard delivering a modeling notation used to capture business/operational processes in support of system and organizational process simulation and analysis. It is used today to capture both human and IT system processes for the purposes of simulating environments, both as-is and to-be, for software modernization. This notation is compatible with KDM so that system extraction can be represented in BPMN for gap analysis of the current

[50] See Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, *Principles for Federal Engagement in Standards Activities to Address National Policies*, M-12-08, 3, January 17, 2012 (one of the Obama Administration's five fundamental strategic goals for Federal Government engagement in standards activities is to "[p]romote standards and standardization systems that promote and sustain innovation and competition"), http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08.pdf.

state of the system versus what is thought to be the current state of the system, which is critical for modernization and compliance.

- Rules Interchange Format (RIF): A World Wide Web Consortium (W3C) standard that delivers representation used for specifying, analyzing, and exchanging information about business rules. Once captured in this format, business rules may be also be used in simulation, gap analysis, and compliance analysis. The analysis of business rules is also an important aspect of application modernization.
- Data/Metadata Storage Standards (old and new): With the emergence of the standards noted above and the need for storing this information for analysis, a set of storage standards were also developed. XMI (XML Metadata Interchange), RDBMS (relational database management system), and RDF (Resource Description Framework) are the three formats that are compatible with these standards. RDF—perhaps the least known of the three—is a W3C standard that is compatible with KDM and BPMN. The value of RDF is that it can manage large amounts of data and metadata, which is critical for doing comprehensive software system analysis.
- Semantics of Business Vocabulary and Business Rules (SBVR): An ISO/OMG standard that provides a structured process for formalizing, in natural language, the existing English language representation of compliance points. The standard enables the various compliance specifications [e.g., Federal Information Security Management Act of 2002 (FISMA) and Health Insurance Portability and Accountability Act of 1996 (HIPAA)] to be formalized, reducing the room for interpretation from organization to organization when implementing the compliance and auditing requirements.

1. Knowledge Extraction to Enable Transparency

Managing both consolidation and operational efficiency when consolidating an enterprise resource planning environment requires significant understanding of the business logic implemented in the legacy system environment. The operational details of both the processes and systems are critical. Over the past couple of decades, the legacy systems environment automated (manual) human processes that now reside in legacy (or operational) systems. These legacy systems—whether older business systems supporting various business operations or ERP systems with significant custom code—need architectural improvements for more cost-effective implementations to meet security, compliance, and functional efficiencies. Incorporating an *as-is* system into the *to-be* environment requires extraction and analysis of the as-is system. In the past, extraction and analysis of the as-is system was dependent on initial documentation and the knowledge about the system in the minds of its analysts.

Standards and technology innovation for extraction and analysis have advanced considerably. Over the past decade, the software systems modernization community comprised

of nearly 40 global companies—including enterprise solutions, modernization services, and software analysis tools providers—participated in the development of standards that defined the constructs for granular representation of system characteristics for the specific purpose of analysis and transformation. This standards-based granular representation enables the extraction and analysis of existing software systems and the migration to new platforms. The two core standards relevant to the enterprise resource planning environment are KDM and BPMN.

Both the KDM and BPMN standards provide a framework to model operational systems in the standards format for detailed extraction and analysis. The benefits of these standards to the enterprise resource planning environment are as follows:

- With significantly reduced investment, legacy systems tethered to ERP systems can either be (1) web-service-enabled to the ERP systems or (2) the business processes extracted and migrated directly into the ERP systems with both accuracy and granularity. For web-service enablement, the ability to discover a service and automatically generate a WSDL (Web Services Description Language)[51] to wrap and integrate it with the ERP system becomes less complex. In many legacy systems, both client and data-facing services are likely to be mixed creating complications for discovering and extracting services. By using these standards, discovery of services, splicing of mixed services, and WSDL generation can become automated processes.
- Extraction tools, including KDM standards-based tools and some non-standard tools, are useful for extracting business logic (i.e., processes, terms, and rules) from the enterprise resource planning environment (including ERP and legacy feeder systems) using automated mechanisms that can feed either MDM or data virtualization efforts.
- In many cases, previously developed custom business logic by the SI is a duplication of the software vendor's existing native functionality within the ERP system. This duplication adds unnecessary development and maintenance costs. With KDM and BPMN, the duplicated custom business logic can be extracted and retired using the standards extraction when the ERP system is upgraded to a newer release or version. In an Oracle ERP system, for example, the extraction and analysis of custom business logic implemented in PL/SQL[52] can be extracted and analyzed to understand which

[51] WSDL is "[a]n XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. WSDL complements the UDDI [(Universal Description, Discovery, and Integration)] standard by providing a uniform way of describing the abstract interface and protocol bindings and deployment details of arbitrary network services." Anoop Singh et al., NIST, "Guide to Secure Web Services: Recommendations of the National Institute of Standards and Technology," Special Publication 800-9, August 2007, C-5.

[52] PL/SQL or "Procedural Language/Structured Query Language" is based on SQL. "SQL is a declarative language that allows database programmers to write a SQL declaration and hand it to the database for executive. As such, SQL cannot be used to execute procedural code, with conditional, iterative, and sequential statements. To overcome this limitation, PL/SQL was created." For Oracle, "PS/SQL is Oracle's Procedural Language extension

portion of the custom logic can be eliminated by simply using the native functions in the Oracle ERP systems—thus, reducing the amount of custom business logic and reducing the cost of maintenance.

- Extraction, analysis, modification, and migration of custom business logic into new non-ERP system solutions are now a reality. Cutting over from an existing ERP system is still complicated due to the reliance on the functional modules (i.e., financial management, logistics management, and human capital management) that are the software vendor's intellectual property. New standards-based solutions are now available via re-usable, standards-based business logic functional components for migration out of an ERP system should the need arise.
- Migration to SaaS requires the extraction of custom or not-yet integrated business logic from ERP systems and legacy feeder systems. This is accomplished through the extraction of business logic using KDM and BPMN standards. It also provides a pathway to potentially retiring legacy systems and the reduction of custom business logic to further leverage state-of-the-art business logic in the most recently released ERP systems.

Migrations of legacy applications (partial or whole) into an ERP system, from an ERP system to SaaS, from an ERP system to an alternative ERP system (i.e., Oracle to Microsoft Dynamics), or from an ERP system to a non-ERP system solution are optimized through the use of international standards and automated extraction and analysis tools that are available but are not yet adopted for use within enterprise resource planning environments. Clearly, the automated extraction and analysis tool providers are viewed as a threat to the ERP software vendors and SIs providing the custom services. The ERP software vendors are concerned with protecting their IP and the potential migration out of their ERP products reducing customer lock-in. Surprisingly, the financial impact as a result of the loss of customers is not as significant to the software vendors as it is to the SIs. Since their revenue generation is directly tied to the number of persons (billable labor) engaged in the service delivery process, SIs are not incentivized to automate these processes.

2. Comprehensive Analytics

Figure 7 provides a pictorial representation of the system information that is extractable using the expanded set of standards and how the standards knit together to deliver the foundation for software system knowledge extraction and comprehensive static analysis. Static analysis can be used to deliver comprehensive automated knowledge extraction and analysis whether addressing enterprise integration, ERP system migration, business logic updates, or compliance.

to SQL." Oracle, "PL/SQL FAQ," *Oracle FAQ's*, last visited on January 12, 2012, http://www.orafaq.com/wiki/PL/SQL_FAQ.

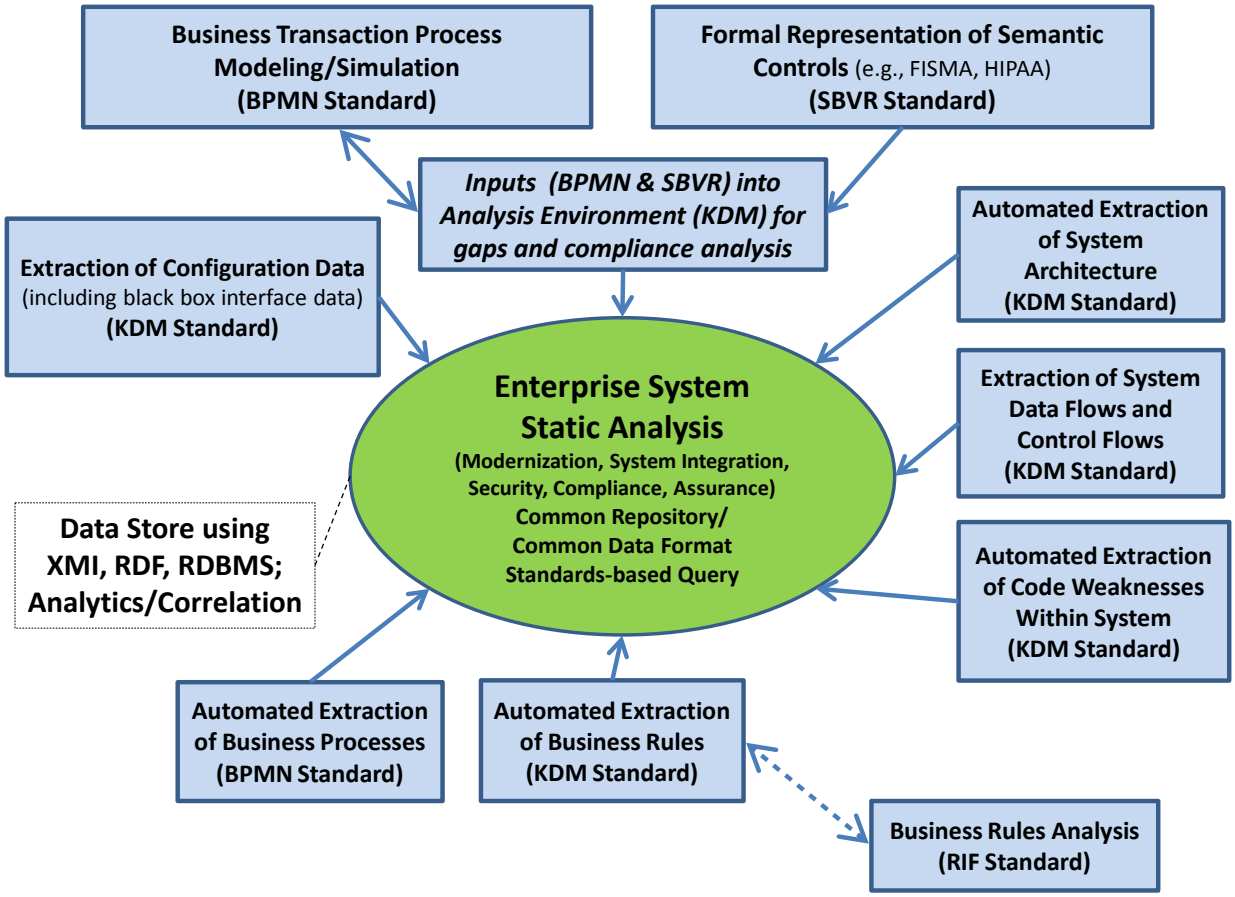


Figure 7. Relationship of Software System Knowledge Extraction and Comprehensive Static Analysis

3. Alternative Hosting

Currently, the Department hosts all of its ERP systems within DoD data centers. Some of these systems are hosted at DISA sites (e.g., Montgomery, AL, and Ogden, UT) while others are hosted at sites controlled by the MILDEPs, such as the GCSS-AF data center where DEAMS resides. Hosting the ERP systems within a DoD data center gives the Department physical control over the servers and security; however, it is not without its share of problems. For instance, complaints about DoD data center hosting range from high latency between the data center and the user community, significantly higher pricing than industry rates for storage and hosting, and the shortage of skilled technicians, such as database administrators.

Alternative hosting environments are readily available from a number of commercial providers. Recognizing the special needs of the Federal government, several of these providers currently offer *federal cage* hosting options that are only available to government agencies. In some cases, this specialized hosting option can accommodate requirements for cleared personnel, connectivity to the NIPRNet, and security that meets or exceed all associated security requirements.

Alternative hosting, which is distinct from cloud computing, denotes a potential range of services from traditional data center to cloud options. In this report, the focus is on outsourcing installation, setup, and maintenance of the ERP system in question, not the particular methodology the hosting provider uses.

Shortcomings of existing hosting solutions that indicate the Department should consider alternative hosting solutions include:

- Latency issues exist between DISA data centers and base networks;
- Shortages of properly trained or skilled personnel exist in the locations where data centers reside;
- The cost per unit for DISA storage and processing is as much as 21 times the cost of similar services offered by commercial vendor [e.g. Amazon Web Services (AWS)].
- DoD data centers do not typically offer state-of-the-art or the most up-to-date technology;
- Patching and updates to servers and software, including ERP software, are not timely and may lag optimal schedules by weeks or months. Third-party providers are able to and are incentivized to update their infrastructures on a more timely basis;
- Maintaining multiple environments (e.g., production, pre-production, testing, and COOP) synchronized to ensure accurate testing has proven difficult. The environments are often weeks out-of-date and, in many cases, do not contain the same infrastructure components;
- DISA and MILDEP data centers (e.g., GCSS-AF) are not focused on ERP delivery. A dedicated provider, such as the Oracle On Demand service for the Oracle E-Business Suite, which is its ERP software product, may provide better service than a generic data center provider;
- Problems exist between inter-DoD support organizations. Interviews indicate that root cause analysis is difficult across organizational boundaries;
- DISA and other DoD hosting providers do not yet offer elastic solutions. An elastic, on-demand option may provide significant cost savings if used across the Department;
- Service level agreements (SLAs) with other government organizations have limited enforcement capability. In contrast, SLAs with commercial providers are highly enforceable, resulting in serious business or financial consequences for non-performance (e.g., past performance and reputation); and
- Deploying additional infrastructure in a DoD data center requires significant investment and the pre-planning of activities. Typically, commercial providers are focused on one specific service and are able to expand and quickly deploy additional

environments on an on-demand basis (e.g., for testing or prototyping). Commercial environments often have the ability to clone another environment. Companies, like Amazon, make continual improvements to the features to manage and stand up infrastructure almost instantly.

While many hosting problems exist, the problems are not universal across all DoD data centers or ERP systems. Some ERP systems—Navy ERP—run their own infrastructure.

Commercial-hosting providers offer a range of services from providing raw servers and storage to integrated full-service solutions. Some of the DoD issues previously highlighted are also inherent to any alternative commercial provider. For example,

- Lack of physical control over systems and data. Since data is hosted externally at a non-DoD data center, trust must be placed in the measures taken by the commercial provider to secure the premises. This risk should be balanced against the fact that most DISA and DoD data centers are predominantly staffed by cleared contractors;
- DoD systems may not be a priority at a commercial data center;
- Hosting prices among commercial providers are low today, but that is not guaranteed in the future. Current demand is causing many of the service offerings' prices to fluctuate. Historically, these prices are going down and often every few months. To plan for these fluctuations, customers of commercial providers can purchase blocks of capability months or years in advance to guarantee a specific price;
- Hosting portability between commercial providers is not a mature feature. Portability allows a customer to migrate existing infrastructure to another commercial provider without changing underlying API calls. Newer offerings, like OpenStack Software, provide a basis for commercial provider portability but are not yet widely adopted in the marketplace;
- Moving to a commercial data center may impact latencies between data center and DoD networks;
- Not all commercial providers offer a federal cage hosting option nor employ cleared personnel; and
- With a move to a commercial hosting provider, encryption at rest and in motion becomes a major consideration as a result of the loss of DoD physical control over the infrastructure.

While there are concerns among various DoD program offices about commercial hosting, they can be alleviated by market forces that demand a higher standard for performance (than that of the government) because of the consequences resulting from publicly exposed and media-reported sub-optimal performance resulting in a loss of reputation and, thus, business. Objective analysis of the risks of off-site commercially hosted infrastructure—including physical security,

information security, and personnel security—is required to reach a conclusion for a specific DoD program. This analysis is highly dependent on the specific service and service offerings chosen as well as how those services are implemented.

Two specific services aimed at ERP systems are:

- **Oracle On Demand:** a service offered directly by Oracle that is focused on hosting Oracle applications, including its E-Business Suite. Oracle refers to it as "Oracle managing Oracle";[53] and
- **SAP-certified AWS:** AWS runs the SAP ERP software.

According to Oracle, its Federal Oracle On Demand service offers the following advantages:

- "For a predictable, recurring fee, Oracle offers an agency a comprehensive set of managed application services based on a Service Level Agreement (SLA) for administering, managing, and maintaining Oracle applications" leading to "predictable O&M costs"[54]
- Multiple hosting options at Oracle (@Oracle), at a customer's location (@Customer) ("Oracle application software residing on servers located … within the Department of Defense") or at a partner's location (@Partner)[55]
- Its Federal Zone ("cage") is secure and segregated for Federal government customers at Oracle's Austin Data Center, which is: (1) a Tier IV facility with Oracle experts (all U.S. citizens) that manage the Oracle applications, database, operating systems, and hardware; (2) 24x7x365 security; (3) complies with relevant FISMA and DIACAP regulations and guidelines; and (4) maintains a Tier II disaster recovery environment[56]
- "The single point of contact is the Federal Service Delivery Manager (SDM). All SDMs that support Federal customers are U.S. citizens"[57] to provide a "single point of accountability for software, hosting, and applications management solutions"[58]

[53] Oracle, *Overview of Oracle Federal On Demand: Hosting and Infrastructure Support Services for Agencies of the U.S. Government*, version 2.0, July 2010, 3 (white paper provided to IDA by Oracle). Additional information about Oracle On Demand is available at http://www.oracle.com/us/products/ondemand/extended-services-068570.html#.

[54] Ibid., 3.

[55] Ibid., 4.

[56] Ibid., 4, 6 and 8.

[57] Ibid., 18.

[58] Ibid., 3.

- "Oracle On Demand uses FIPS 140-2 compliant storage security appliances and provides a unified platform for encrypting data"[59]
- "Proactive patch and upgrade assessments and execution":[60] "As part of software management, Oracle Federal On Demand proactively applies patches. Oracle will identify and analyze individual patches or patch sets and apply them to the Oracle Production software environment and operating system, as necessary."[61]
- "With unrivaled expertise in managing and maintaining Oracle software, and access to the product strategy and development teams, Oracle Federal On Demand can advise a Federal customer on current and future functionality, reducing customizations, integrations, and modifications"[62]
- "Ability to measure and improve performance[,] … automate processes[, and] … achieve standardization and streamline IT"[63]
- "Shortened implementation lifecycle"[64]

Another example of an alternative hosting option is leveraging the close collaborative alliance between SAP and Amazon. SAP ERP systems are now certified to run on the Amazon infrastructure. AWS's infrastructure hosting incorporates features like on-demand changes in infrastructure and elastic computing. Unlike Oracle, however, AWS does not provide the application services as part of its service offerings so either a third party or internal DoD staff is required to manage the infrastructure and patching. In the near future, a third party may offer an integrated SAP solution run on AWS that operates similarly to Oracle on Demand from the customer perspective. The benefits of AWS, according to Amazon's Chief Information Security Officer, are as follows:

- AWS offers an option for dedicated servers as opposed to its standard offering where many customers may use a single physical server for processing. This option is considered more secure as exploits across the hypervisor are not possible.
- One cost-reduction strategy is to turn off resources not needed during slower times while increasing them as needed during higher-usage periods, such as end-of-month or end-or-quarter, when transaction processing requires many more resources than

[59] Ibid., 15.
[60] Ibid., 6.
[61] Ibid., 13.
[62] Ibid., 11.
[63] Ibid., 3.
[64] Ibid., 3.

other times. Many DoD applications have predictable cycles in resources required and are good candidates for this type of service.

- Using AWS Virtual Private Cloud option, the resources located in AWS data centers can operate as if behind the customer firewall and all traffic is routed through the customer site. This may increase options for security.
- AWS offers several geographically separated data centers with options to use multiple centers for high reliability applications. Organizations, such as Netflix, have successfully architected high-reliability solutions that have withstood an entire data center outage while successfully rerouting traffic and resources to other data centers.
- Amazon is continually evolving its architecture and service offerings from a security and functionality standpoint. Since IDA's initial analysis of AWS, Amazon added additional encryption capabilities as well as features to increase ease of deployment and redundancy.
- Hot backups are streamlined with the AWS architecture. New server instances can be started instantly when problems are detected, eliminating the need for a cold COOP site, which carries a duplicate cost. The cost of AWS resources is based on active usage.
- On-demand instances allow a pay-as-you-go business model for computing capacity (by the hour) with no long-term commitments. This minimizes the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs.[65]

In general, Amazon's security is similar to the DoD's technological footprint. For instance, AWS:

- Accommodates a high volume of accounts receivable and accounts payable data with sensitive customer's personal data;
- Receives and transmits banking data such as routing numbers and gateway information;
- Is undergoing DIACAP certification for a member of the Intelligence Community; and[66]
- Options exist for dedicated servers that are not shared with third parties.

[65] IDA interview (conference call) with Steve Schmidt, Chief Information Security Officer, Amazon Web Services, on November 23, 2010. Additional information about AWS is available at http://aws.amazon.com/.

[66] Ibid. (interview with Steve Schmidt).

As with any contractor, Oracle and Amazon employees can physically access the system. Prior to moving to any alternative hosting environment, a trade-space analysis should be conducted to balance the risks of non-DoD commercial providers rendering hosting services for DoD business systems.

4. Cloud Computing—IT Transformation, Not a Technology

Cloud computing is an old concept in computing with research and theory dating back to the 1960s. Utility or commodity computing came in vogue in the 1990s through managed services as a platform. The major premise is the customer pays only for what is used. The *use more, pay more* model evolved into today's cloud computing. It was not until recently (circa 2000) that cloud computing became feasible for implementation.

> "[W]orkers in the field of computers are now becoming increasingly excited about the birth of a remarkable new method for the distribution and utilization of computer power. This method has a variety of names— ... in this book, simply 'computer utility.' Regardless of the name, however, the development of this method does open up exciting new prospects for the employment of computers in ways and on a scale that would have seemed pure fantasy only five years ago."—Douglass F. Parkhill, *The Challenge of Computer Utility*, Reading, Mass.; Addison-Wesley Publishing Company, 1966, v.

Amazon launched its AWS cloud services in 2006. Cloud services are possible because of a convergence of four aspects: (1) the *concept* of utility computing; (2) the *suitability* for using utility computing services (i.e., a need to abstract out unnecessary details of the computing stack to focus on core competencies); (3) the *technology* to achieve it (e.g., large data centers and virtualization); and (4) an *attitude* of business leaders to change and a willingness to adopt these models.

In September 2011, NIST finally published the long-awaited official definition for the Federal government regarding cloud computing that signals its interest in cloud computing.[67] NIST defines cloud computing as:

> a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is

[67] NIST, U.S. Department of Commerce, "The NIST Definition of Cloud Computing," Special Publication 800-145, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. For additional information on public cloud privacy and security, see NIST, U.S. Department of Commerce, "Guidelines on Security and Privacy in Public Cloud Computing," Special Publication 800-144, December 2011, http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

composed of five essential characteristics, three service models, and four deployment models.[68]

For reader convenience, these essential characteristics, service models, and deployment models are included in Table 1.

To further develop NIST's definition cloud computing, it is essential to consider that cloud computing is the *commoditization* of the IT industry from a product to a utility-like service for IT-based economy. It is a *transformation* of a group of technologies and not a technology itself. This is where most IT vendors get it wrong.

To understand cloud computing as a utility better, it might be helpful to understand how technologies in general progress through their lifecycles into a commodity or utility. First, as depicted in Figure 8, they begin as innovations. At this stage, technologies are: (1) very rare, perhaps one of a kind; (2) not well understood; and (3) uncertain as to their survival, that is, whether the technology will make it out of a lab or testing environment (e.g., the first web server was coded from scratch).[69]

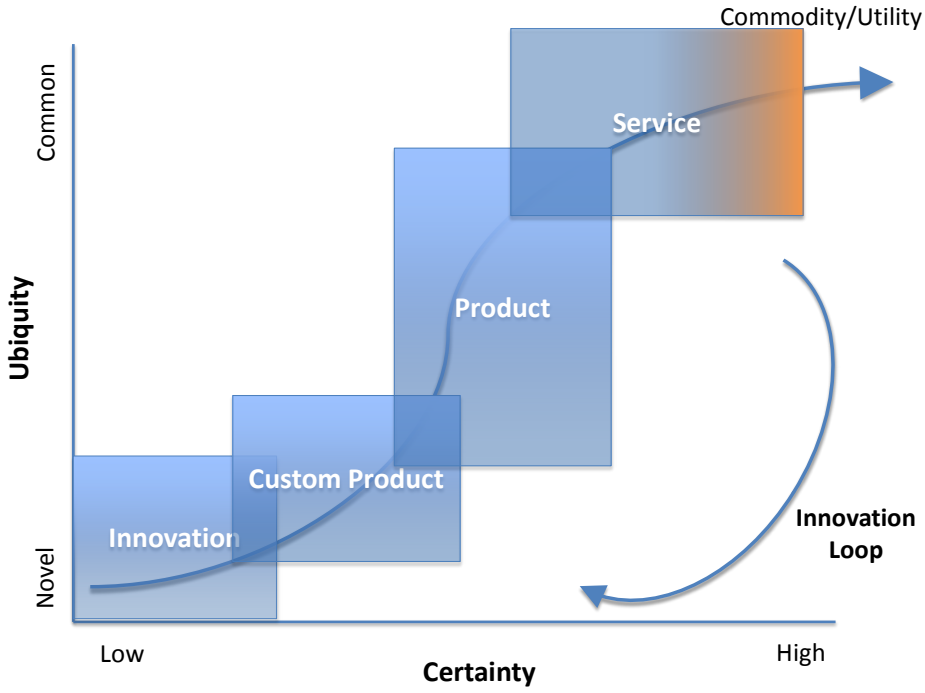


Figure 8. Cloud Computing: Transformation From Product to Utility-like Service for IT[70]

[68] Ibid., 2.

[69] Simon Wardley, "Cloud Computing—Why It Matters," presentation at O'Reilly OSCON (Open Source Convention 2009," July 23, 2009, http://www.youtube.com/watch?v=okqLxzWS5R4.

[70] Ibid.

Table 1. Cloud Computing: Characteristics, Service Models, and Deployment Models[71]

Essential Characteristics	
On-demand self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
Broad network access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
Resource pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
Rapid elasticity	Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
Measured service [(often referred to as "billing")]	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.
Service Models	
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.
Platform as a service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Infrastructure as a service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
Deployment Models	
Private cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Community cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Public cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Hybrid cloud.	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

[71] Ibid., 2-3.

Then, as a technology becomes better understood (and moves up the S-curve), greater market appreciation results in the availability of a number of custom products (e.g., the next few web servers were built from scratch but used the concepts learned from the first one). Over time, these technologies are afforded a greater market share and become a product. In software, these products are purchased off-the-shelf or downloaded (e.g., web servers are now widely and freely available with Apache and Microsoft's IIS products dominating the market).

If market forces allow, eventually the technology further progresses and matures, resulting in a proliferation of providers offering the technology as a service (the crest of the S-curve). An example of this is the web-hosting market. Organizations can forgo maintaining their own servers and installing web-server software; instead, they can purchase web hosting for about $2 per month from thousands of service providers (e.g., Rackspace Hosting or Amazon).

Some technologies can be offered as utility-like services (top of the S-curve). The customer no longer pays a subscription fee (e.g., cable television) but instead pays for actual usage (e.g., electricity). Under this utility-like service, an organization no longer pays in advance for the number of users or the amount of bandwidth or resources it may consume; rather, it pays for what it actually consumes. At this stage, the technology is widespread and its features are complete. It is now a commodity that is technologically indistinguishable from other offerings.

As a result of commoditization, contractual concerns like SLAs and portability between providers (driven by widely adopted standards) gain importance.

Service Level Agreements

When an organization moves its operations to cloud computing, its operations become reliant on the SLAs it negotiates with a service provider for that specific technology. At a minimum within DoD, these SLAs should address the following:

- Data security: protecting data from disclosure;
- Confidentiality: obligation not to disclose data;
- Compliance: legal obligations (e.g., privacy, restrictions on data location);
- Availability: accessing data (includes data back-up and storage procedures), notification procedures for scheduling maintenance, when maintenance cannot be performed, what time zone is used for notification, how availability is measured;
- Service Levels: resolving errors, user support, and technology refresh;
- Technology Determination: notification procedures and timeframes for vendor's technology upgrades and changes;
- Remedies: credits and/or penalties imposed for service non-availability;
- Termination: immediate return of data and vendor assistance in transitioning customer to a new vendor; and
- Subcontracting Limitations: obtaining the contracting officer's consent to subcontract before establishing any subcontracting relationships affecting DoD's availability or data.*

The goal with these SLAs is to incentivize service providers to meet the terms of the SLAs. Any remedies sought for non-availability should not punish the vendor to the extent of hindering its future performance under the terms of the SLA because such a punishment would result in additional harm to the Department given it no longer maintains that inherent technological ability.

* H. Ward Classen and Philip D. Porter, "Negotiating Major Legal Issues in Cloud Computing," presentation at the 12th Annual Information Technology Legal Institute – 2011, Virginia Law Foundation.

As technologies become commodities, they turn into the cost of doing business. While there is a tactical need for the commodity, the strategic value for an organization diminishes to zero.[72] Innovative tools are a source of competitive advantage while commodity tools are not. When an organization treats a commodity as if it is an innovation, they expend unnecessary resources to produce a similar result at an increased cost. For example, imagine trying to generate electricity for an organization rather than being connected to the power grid. The cost would be astronomically higher per watt as well as less reliable.

When technologies become services and utility-like, freeing up resources that used to be expended on maintaining, implementing, or creating those technologies, those resources can then be recycled into new innovations via an innovation loop (see Figure 9). In the power grid example, the cost of power becomes less per watt on the grid; however, this calculated cost savings must be balanced against the control over a commodity that is an underlying resource

[72] See Nicholas Carr, *Does It Matter? Information Technology and the Corrosion of Competitive Advantage*, Boston, Mass.: Harvard Business School Publishing Corp., 2004.

requirement for the operation of the business. For example, if the electricity is lost for an extended period of time and electricity is a required resource for business operations, the consequence to the business far outweighs the benefit of the cost savings. This is a tradeoff between cost and control. As fewer resources (e.g., people, equipment, or physical space) are required to deliver electricity at a facility, redundancies such as backup generators, at a reasonable cost, can offset any problems at the power company.

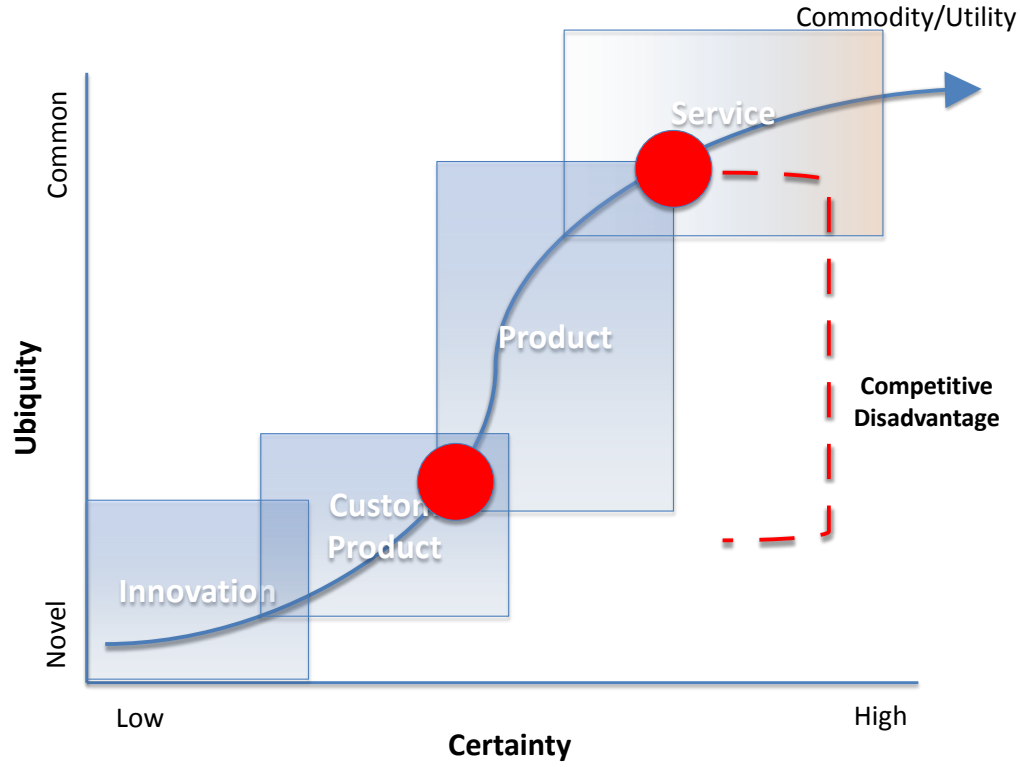


Figure 9. Competitive Disadvantage When Treating Commodities as Innovations.[73]

If DoD anticipates that a technology is likely to become a utility-like service, then it should attempt to make that technology utility-like as quickly as possible. This will allow the MILDEPs and Agencies to pay a lower cost and to reuse their scare IT resources for innovation. For DoD, the primary cost driver is DISA's data centers and the innovation should be the movement of these centers to cloud computing.

Planned failure of resources is an important concept of cloud computing. Here individual resources (e.g., hardware) are not relied upon singly but rather viewed as fungible. Given a large enough family of hardware (e.g., a large data center or the data center ecosystem), an accurate

[73] Simon Wardley, "Cloud Computing—Why It Matters," presentation at O'Reilly OSCON (Open Source Convention 2009," July 23, 2009, http://www.youtube.com/watch?v=okqLxzWS5R4.

prediction of how much hardware will fail at any given time is possible (although rarely known is *which* specific hardware will fail). For example, RAID[74] arrays in a single server are used to mitigate the risk of hard drive failure. The likelihood that one drive in a RAID array will fail is predictably low, but the probability that two will fail at the same time is usually sufficiently low to rely on tape backup beyond that point. The same holds true at a larger scale with the difference being that a very large infrastructure provider (e.g., Amazon and Rackspace Hosting) can predict that perhaps 3 percent of their millions of hard drives will have failed at any given time. Therefore, a plan for rapid movement of data stored on those drives to alternative drives as each individual drive fails is already in place.

Failures are irrelevant if data and applications can move freely between commoditized hardware. This concept in cloud differs from that of traditional IT. In traditional IT, the assumption is that—given a failure—the hardware in question will be fixed within a defined window of time (i.e., 4-hour response). Typically, architectures accommodate an "n+1"—that is, on demand expansion of capacity to address failover as a method of redundancy. In a cloud environment, it is expected that when a resource fails, the failed resource will be automatically replaced by *any* equivalent resource. This means a gigabyte (GB) is a GB and a processing cycle is a processing cycle. The customer does not care where it is or what server it is in, only that it works and it adheres to the standards agreed to in the SLA.

Due to overuse in vendor marketing materials, cloud computing is increasingly referred to by thought leaders as *commodity computing* or *utility computing*.

a. Everything as a Service (XaaS)

XaaS refers to the commoditization of the computing stack from a product to a service. The lead word—*Software as a Service* or *infrastructure* as a service—indicates how much of the stack is abstracted, thereby relieving user responsibility. For example, infrastructure as a service (IaaS) abstracts very little since the IaaS user must still be concerned with the operating system, platforms, and software installed. In contrast, Software as a Service (SaaS) abstracts the entire stack except for a few application configuration options (see Figure 10).

[74] RAID (redundant array of independent disks) "is a way of storing the same data in different places (thus, redundantly) on multiple hard disks." TechTarget, "RAID," last visited on January 4, 2011, http://searchstorage.techtarget.com/definition/RAID.

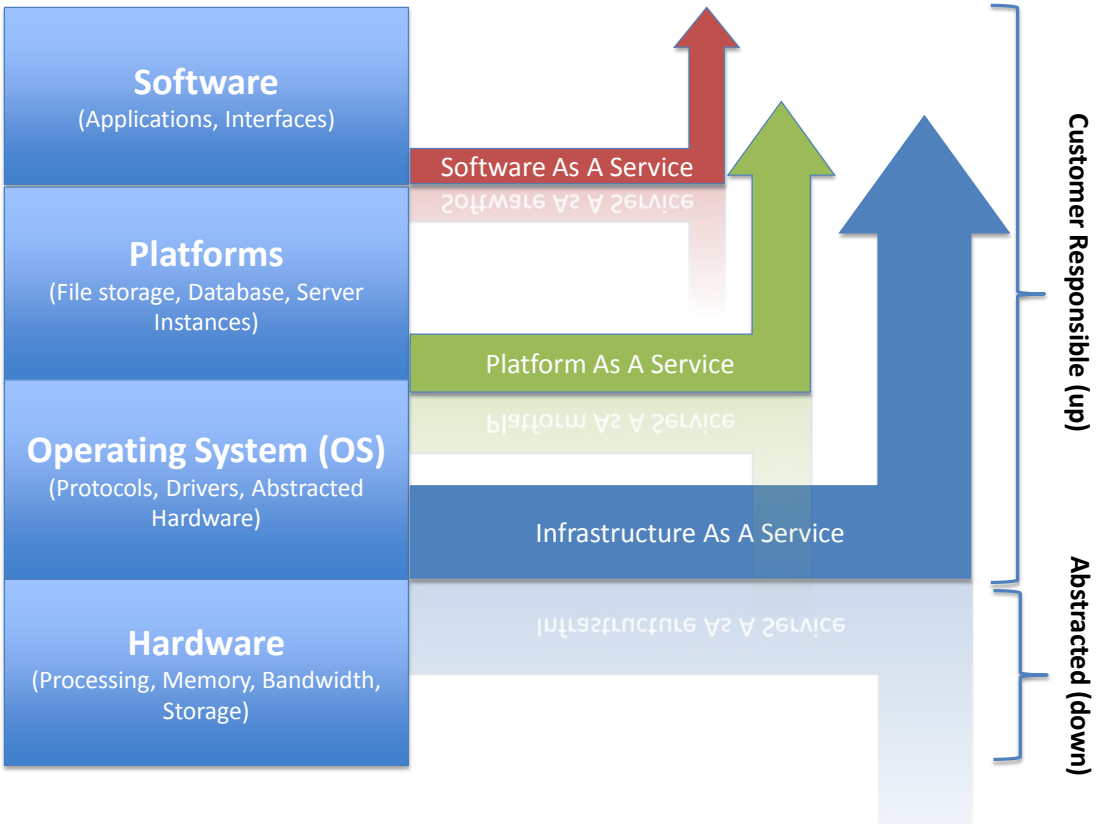


Figure 10. XaaS and Abstraction of the Computing Stack

From a service perspective, consumers are concerned with the delivery of that service, not how that service is set up or implemented at lower levels of the computing stack. This is important because it means that others (e.g., a user, developer, group, or organization) can build upon existing services available in the marketplace without understanding how to build them. Instead, a consumer's only focus is interacting with the available APIs.[75] With XaaS, a new system can then be architected with concern paid only to those elements that are of a core concern to the system. In general, that focus will be on the business processes being implemented. An early adopter of this methodology is the Army Chief Information Officer/G-6-led migration to Enterprise Email and a unified cloud computing operational model.[76]

Simon Wardley, who is an executive at Canonical, a leader in operating system-level cloud solutions, and a researcher at CSC Leading Edge Forum, correctly observes that in a service economy:

[75] From a systems engineering perspective, it is important to understand how the services are constructed to ensure an organization's system is built in a way that guarantees the proper level of redundancy and reliability, but a developer may only need to know, for instance, that additional storage is available via calling an API.

[76] *See* Army Chief Information Officer/G-6, *America's Army: Powered by a Networked Force*, http://ciog6.army.mil/EnterpriseNetworkUpdate/tabid/100/Default.aspx.

> SLAs are not as important as portability between providers. Without such portability you will remain still stuck in a product based economy, albeit one that you can rent over the wire. The companies who accept that service is the key to competitive advantage in a service economy will have no problem embracing this; those who believe their technology is their "secret sauce" will always have problems adapting.
>
> …
>
> Like it or not, we are moving towards a world where ubiquitous IT activities will be provided by utility computing markets. Providers will openly compete based upon price vs. QoS (*quality of service*) and services will be defined by open sourced standards.[77]

b. Data as a Service (DaaS)

DaaS was initially used for combining data from multiple sources automatically and using the aggregated data stream as input to another web application. Increasingly, DaaS is used across enterprise organizations wishing to make financial and logistics data available to other applications in the organization.

DaaS is the provisioning of the commoditized data layer of applications. The data is separated from any application viewing or processing and offered independently from the originating application to anyone granted access to that data. As data is accessible via open APIs to anyone authorized to retrieve it, it does not matter where the data resides. There is a distinction between data and information; the application processing and viewing of the data will provide a context to the data that can provide information based upon the data.

Data provided as a service enables:

- SaaS and platform as a service (PaaS) solutions that rely on access to large datasets.
- Centralization of data to a single authoritative source of data that is accessible via open APIs. Data quality is improved, as a single source of data is updated and instantly available to all users of that data.
- Easy access to data so that the users of data can focus on core competencies of processing data and not on the storage, access, and acquisition of that data.
- Access to small subsets of large datasets without requiring an infrastructure to host and access that data. Only the data needed from the larger data set must be transmitted to or stored at the processing system, resulting in less overall duplication

[77] Simon Wardley, "Here comes the farmer...," *Bits or pieces?*, blog post, April 19, 2008, http://blog.gardeviance.org/2008/04/here-comes-farmer.html.

of data across systems. Ideally, data could be pulled in real-time as needed, although this is not always feasible.

- Sharing of data with other users who may or may not have previously expressed a need for the particular data in question. DaaS enables new users and users of data to discover innovative solutions not possible before access to data sets was fast and easy.
- Agility and simplicity of data access, which allows data users to quickly develop solutions using a variety of data sets or aggregations of data sets.
- Focus on core competencies—that is, producers of data can focus on the best production of data while consumers of data need not be concerned with how to produce data for use in their systems. Rather, consumers need only subscribe to the best available data source for their output.

The concept of DaaS is crucial to DoD's move into a distributed enterprise resource planning environment and out of software vendor-specific ERP systems. DaaS allows a multitude of systems to publish data for use by others in the environment and work together with open APIs.

c. Software (or Application) as a Service (SaaS)

SaaS removes the requirement for the consumer to manage or control the underlying cloud infrastructure, including the network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. It is typically delivered as:

- A web-based application or in some cases a mobile interface. This removes the need to install software to a server or desktop. The service provider then handles all maintenance, including upgrades and patches; or
- Via a subscription model, as opposed to a single purchase price plus ongoing maintenance fees with traditional software. Although overall cost may not be lower, often a subscription model lowers the upfront cost significantly. In essence, it changes the software expense from a capital expense to an operating expense. The cost of an additional user is minimal, especially across a larger cloud provider. Even the added cost of a new organization, with many users, is small compared to the cost and complexity of a traditional hosted application model.

SaaS differs from the Application Service Provider (ASP) model of the 1990s, which is where the service provider would install one instance of software per customer. In SaaS models, there is one copy of the software running with a multitenant architecture to secure and separate data from one customer to the next. In the ASP model, scaling up was a problem; in contrast,

SaaS is installed across a large number of machines—typically referred to as horizontal scaling—making scaling effortless for the customer.

SaaS enables a specific functionality complete with a user interface. This allows for input and output of data by a user of the system with no concern over other aspects of the system. SaaS also allows fast deployment, usually instantly to new users. Multitenant architectures allow additional organizations to be added quickly as well as enabling a *develop once, deploy many* model. For DoD, this means the best SaaS functions are those that are ubiquitous across the Department (e.g., financial management, logistics management, human capital management, or inventory management) as they can be built once, then deployed to others needing similar functionality without large development efforts. SalesForce.com is an example of a commercial customer relationship management (CRM)[78] SaaS provider; thousands of organizations use the same CRM application configured differently to meet their specific needs.

SaaS is delivered via a web browser or mobile device and the interface is independent from the data in the system. Data is more secure because only limited amounts of data are downloaded from the data center to the device at any given time. This increases control and auditability of the data. Data is also always up-to-date and any connections to other data sources are faster. The user—be it many users, a remote user, or many remote users—is presented with only the information relevant for their current interaction. A similar statement can be made about ERPs.

SaaS enables seamless updates on the user side. Once software is updated in the data center, those updates are immediately served to the user when a page is requested. New applications can be pushed out quickly to users because they only need a web address or access to an application distribution platform (i.e., Apple's App Store). The application itself can be quickly created on top of PaaS or IaaS components allowing for faster innovation based on commoditized resources already in place.

The benefit of SaaS to the Department is the ability to build once and deploy to many. DoD should determine similar functionality across many organizations that currently maintain separate systems. SaaS applications can be built for one organization; then, additional configuration options can be added iteratively for small changes in how specific organizations will use the software. This allows a single horizontally scalable application to accommodate many different organizations within the Department while allowing for easy scalability, less maintenance, lower development costs, and fewer numbers of projects to manage. An early

[78] CRM is "a company-wide business strategy designed to reduce costs and increase profitability by solidifying customer satisfaction, loyalty, and advocacy. True CRM brings together information from all data sources within an organization (and where appropriate, from outside the organization) to give one, holistic view of each customer in real time. This allows customer facing employees in such areas as sales, customer support, and marketing to make quick yet informed decisions on everything from cross-selling and upselling opportunities to target marketing strategies to competitive positioning tactics." CRM Magazine, *What is CRM*, Destination CRM.com, February 19, 2010, http://www.destinationcrm.com/Articles/CRM-News/Daily-News/What-Is-CRM-46033.aspx.

instance of SaaS is the Joint Chiefs of Staff migration to the Army's Enterprise Email system. The power of SaaS is increased when applications leverage open APIs from other systems to incorporate additional data and functionality.

The potential reduction of application installation, support, and maintenance costs at the user's desktop could be significant. If software runs in a standards-compliant web browser, almost any hardware platform (device independence) can be used with minimal support. This affords the organization the opportunity to focus on application support (e.g., usability and training) rather than support issues related to individual users and their personal desktop (i.e., those *outside* the application). It should also increase the ability of the user to access software from a variety of locations and devices.

Interviews with industry indicate that there is a growing belief that native applications on a variety of mobile devices are crucial for the Department to move forward technologically. Native applications allow for integration with sensor platforms on the mobile device. This allows the user to utilize functionality such as a camera, location- or positioning-based service, or barcode or QR (Quick Response) code reader. With an increasing number of third-party hardware manufacturers integrating with Android and iOS (formerly the iPhone operating system) devices for their communications and application capabilities, the mobile space may prove to hold significant advantages over desktop-only applications.

A powerful feature of SaaS, especially on mobile devices, is that data remains mostly in the data center; only a portion of the data that is being viewed by the user is on the device at any point in time. This allows for enhanced security as less data is leaving the data center than if the user must synchronize data to a device or laptop. The tradeoff is less functionality or available data when disconnected from the network.

d. Platform as a Service (PaaS)

PaaS provides the capability to the consumer to deploy languages and tools (e.g., databases, programming languages, or server instances). The consumer is abstracted from lower levels of the stack (i.e., servers, operating systems, and network infrastructure) while retaining control over deployed applications and configurations.

PaaS enables the deployment of applications without the cost and complexity of acquiring and managing underlying infrastructure, including hardware, software, and facilities. PaaS offerings may include facilities for application design, application development, testing, deployment, and hosting as well as application services, such as web-service integration, database integration, security, scalability, storage, persistence, state management, application versioning, and developer community facilitation. These services may be provisioned as an integrated solution over the web.

Today, the ERP systems and some of the legacy systems could benefit from taking advantage of PaaS infrastructures either within or outside of DoD data centers. ERP systems are

underutilizing their current computing resources much of the time and the high costs of entry prevent testing and development with other platforms. PaaS allows for resources to be provisioned on-demand at the time they are needed. Platforms can be stood up across DoD in a redundant, distributed manner. Enterprise-wide PaaS offerings, such as database or file storage platforms, can reduce licensing costs and create a higher degree of standardization across the enterprise.

e. Infrastructure as a Service (IaaS)

IaaS provides an abstraction to the customer for provisioning processing, storage, network, and other fundamental computing resources. The consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying infrastructure but maintains control over operating systems, storage, deployed applications, and, possibly, limited control of select networking components (e.g., host firewalls).

IaaS enables developers for DoD to build platforms and applications without concern for the specific hardware systems that they will run on. Thus, developers can focus on their core competency of developing applications and platforms and not on application implementation or vertically scaling the application.

Department-wide IaaS can greatly reduce infrastructure costs. Since individual applications will use varying amounts of infrastructure, the total infrastructure across the Department is reduced as unused cycles, memory, and bandwidth can be consumed by other applications.

A typical data center or program will estimate required server resources using a variety of methods. One is “peak + 20 percent” where the peak usage on a system is measured over a period of time (usually a month) and then resources are acquired to achieve that peak level plus a 20 percent performance cushion. This method results in large amounts of unused resources at non-peak times across an enterprise. One specific way to take advantage of IaaS, for example, is to eliminate the “peak + 20 percent” model and instead purchase resources for the average usage and then utilize horizontal scaling methods to expand extra needed resources into an IaaS environment (see Figure 11).

Alternatively, ERP systems could run entirely in an IaaS environment. For financial management systems, this could have an added benefit. These programs have very predictable, high-volume times such as the end of the month. If these times can be predicted accurately, then two systems with peak times can be scheduled not to conflict with one another while lowering the total infrastructure needed by the Department significantly.

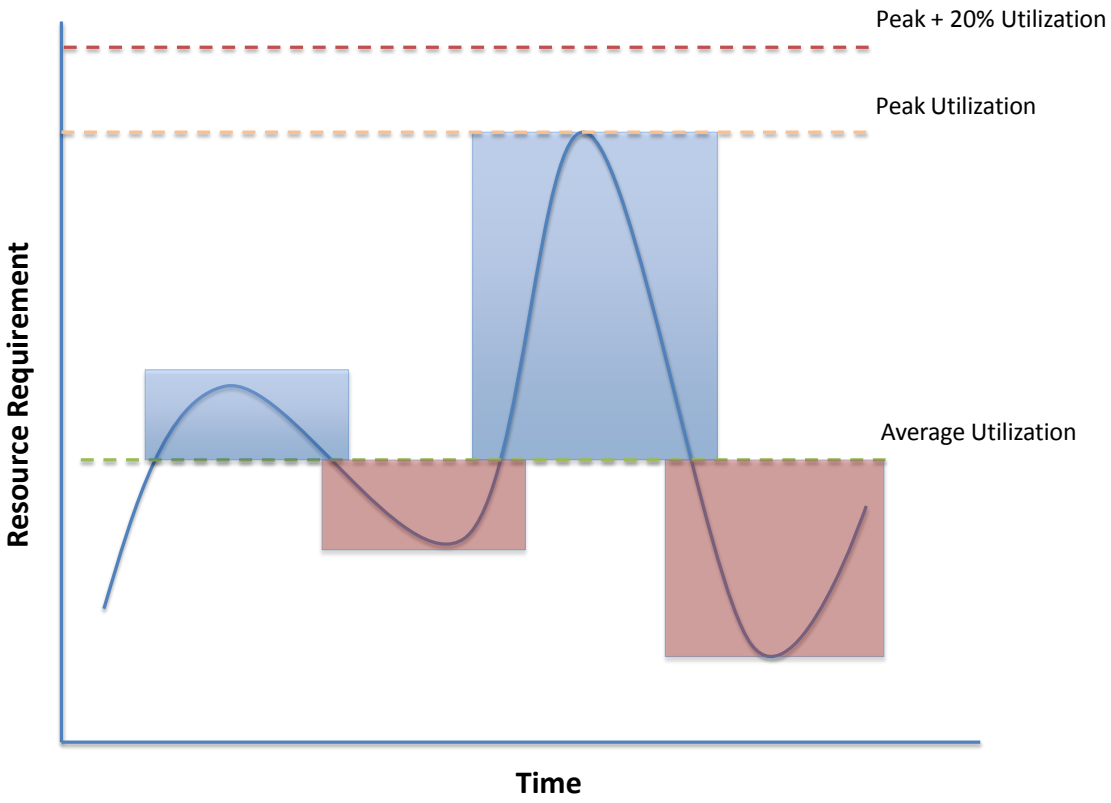


Figure 11. Data Center Resource Utilization Strategies

The DoD's ERP systems and some of the legacy systems could benefit today from IaaS infrastructures in or outside of DoD data centers. ERP systems are underutilizing their computing resources much of the time, and servers and other equipment must be procured well in advance of initial deployment. IaaS allows for resources to be provisioned on-demand at the time they are needed and paid for only during those times.

f. Devices as a Service

A new concept emerging in commercial and government IT is *bring your own device*. Instead of the company or agency providing all the equipment (e.g., laptops, mobile devices, iPhones, Androids, and tablets), the user uses his or her own existing equipment or is afforded an allowance to purchase the equipment of choice for work.

BYOD policies can significantly lower the cost of equipment since many users already own many of the devices they would like to use in the workplace. Users often have a better sense of personal requirements or preferences for these devices. DoD organizations, such as National Defense University's new policy regarding student computers, are already moving toward these policies as they face significantly reduced IT budgets in the coming years.

Embracing a BYOD policy can ready an organization to handle an influx of devices. Traditional IT posture forbids devices, software, and practices not explicitly approved. The abbreviated development lifecycle of these devices creates a dynamic whereby organizations' procurement offices cannot keep up with user demands. Users anxious for the newest thing or for something that gets the job done faster are likely to work around IT policies. BYOD policies mean that the IT department is focused on helping users resolve problems on a range of devices and software. However, these IT departments must also be ready to handle security and data breach issues outside a narrowly defined scope.

g. Integration

Figure 12 depicts the integration of the *as a service* offerings described in this chapter. Notice that SaaS offerings are built upon IaaS or PaaS while DaaS is integrated with all other services. The business process is the overarching beneficiary of the supporting services.

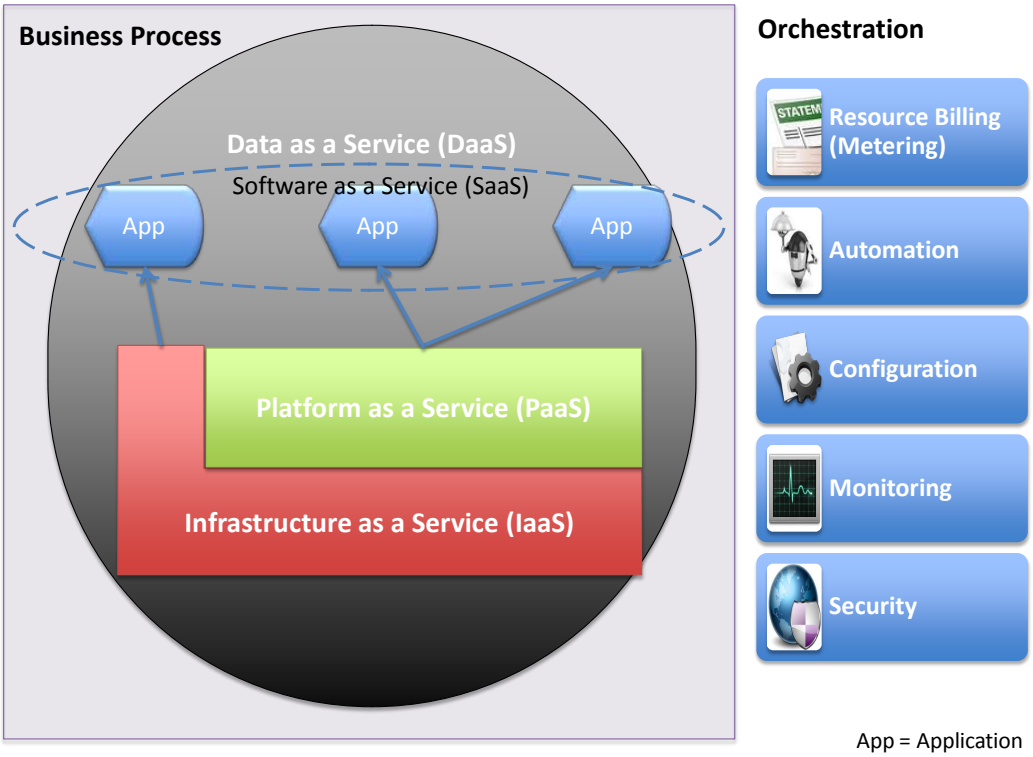


Figure 12. Overall Integration of "As a Service" Construct

Additional "as a service" models are emerging. These services typically fit within either SaaS or PaaS delivery models. For example, *security as a service* is one of these new cloud service offerings. Currently, some security vendors are providing outsourced environments into which code analysis can be completed for the purpose of identifying any weaknesses incorporated into the source code (open or closed source) that may pose either a direct security impact or a create an environment for a cybersecurity breach. This type of service is still

evolving to expand its offering, but the focus thus far has been in software assurance/code analysis.

While cloud and other technologies beyond ERPs may not solve all of the Department's enterprise integration and efficiency issues, they deserve critical consideration as part of DoD's portfolio. One industry expert, Gunnar Hellekson, Chief Technology Strategist for Red Hat's U.S. Public Sector, "cautions against viewing technology as a panacea when it comes to cloud computing." As reported by *Defense Systems*, Hellekson said that:

> "All the technology in the world won't overcome inefficiencies in the enterprise, and the move to cloud infrastructures draws those inefficiencies into the open … So if you're DISA, and you're building a cloud, you want to pay attention to the entire ecosystem of policies and procedures around your infrastructure. If you focus on the narrow technical questions, you'll be unpleasantly surprised."
>
> As an example, he points to DISA's Rapid Access Computing Environment (RACE), the agency's private Infrastructure-as-a-Service solution that was one of its first cloud implementations. RACE, which went operational in late 2008, is a self-service portal which allows DOD users to provision servers in its secure computing environment.
>
> "[DISA] did a lot of work to make it simple for their users to pay for computing power with a credit card," said Hellekson. "Technically, the solution works just fine. In practice, their internal business rules make it impossible to transfer money between departments any quicker than three days. That means that no matter how flexible their internal IT systems are, they're only moving as quickly as their weakest business process."[79]

B. Build or Buy—Integration Costs as a Risk

ERP systems are large pre-integrated sets of functional modules. The initial purchase cost of these systems is high as is the complexity of the solution. Further costs are realized as SIs are hired to customize and maintain the systems in long-term contracts. ERP systems require integration with feeder legacy systems at an additional cost to implementing the ERP itself.

The alternative to purchasing pre-integrated modules is to buy one-off optimized applications for a smaller function set. These solutions then need to be integrated together to produce an enterprise resource planning environment at an additional cost. Generally, customization of these modules will be less expensive individually, but possibly more expensive in total than with an ERP system.

[79] Greg Slabodkin, "DISA makes headway on key enterprise initiatives," *Defense Systems*, December 5, 2011, http://defensesystems.com/articles/2011/12/13/cover-story-disa-enterprise-initiatives.aspx.

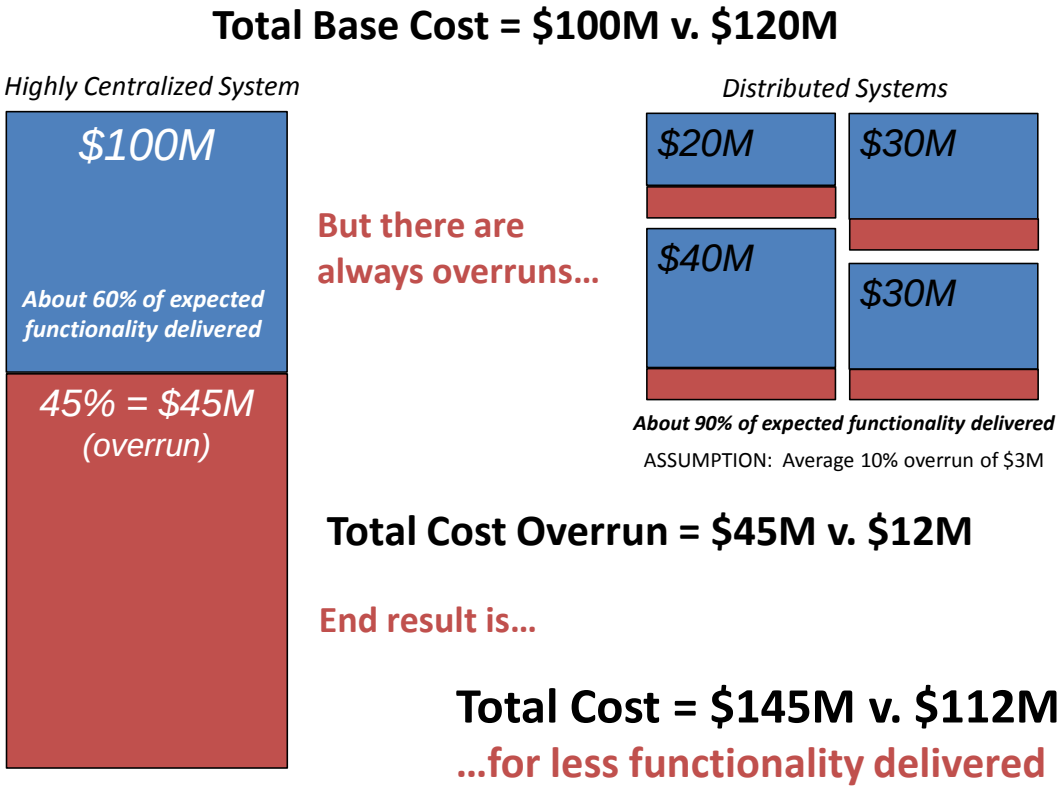


Figure 13. Pre-integrated Large System Investment Versus Small System Investment[80]

The cost overruns experienced by the ERP systems in DoD are not unexpected. Figure 13 shows that a software project success depends upon its size; that is, smaller systems (those with fewer project function points[81]) have higher early and on time completion rates than larger, more complex systems (those with over 1,000 function points).[82]

[80] GAO, *DoD Financial Management: Reported Status of Department of Defense's Enterprise Resource Planning Systems*, (GAO-12-565R) March 30, 2012, Enclosure III, http://www.gao.gov/assets/590/589796.pdf [based on the data available to the GAO as of December 31, 2011, the average life-cycle cost estimate overrun is 45 percent (original life-cycle cost estimate as compared to current life-cycle cost estimate) for the following DoD ERP programs: DEAMS=45 percent over; ECSS=73 percent over; GCSS-Army=8 percent over; GFEBS=0 percent over; GCSS-MC=773 percent over; LMP=62 percent over; and Navy ERP=42 percent over].

[81] "Function Points measure software size by quantifying the functionality provided to the user based solely on logical design and functional specifications," International Function Point Users Group, "About IFPUG," last visited on January 27, 2012, http://www.ifpug.org/about/faqs.htm; "The reason that function points are the best choice for measuring defect potentials is that the older "lines of code" or LOC metric can only be used to quantify coding defects," Capers Jones and Olivier Bonsignour, *The Economics of Software Quality*, Boston, MA: Pearson Education Inc., 2011, 39.

[82] See Business Transformation Agency, "Lesson 1 – Background and Challenge," *Service Oriented Architecture (SOA)*, Slide 8 ("BMA Transformation Principles – Platoon Sized/NOT Battalion Sized") last visited on January 18, 2012, http://www.bta.mil/products/training/SOA/index.html (according to BTA, the source of the data is Capers Jones).

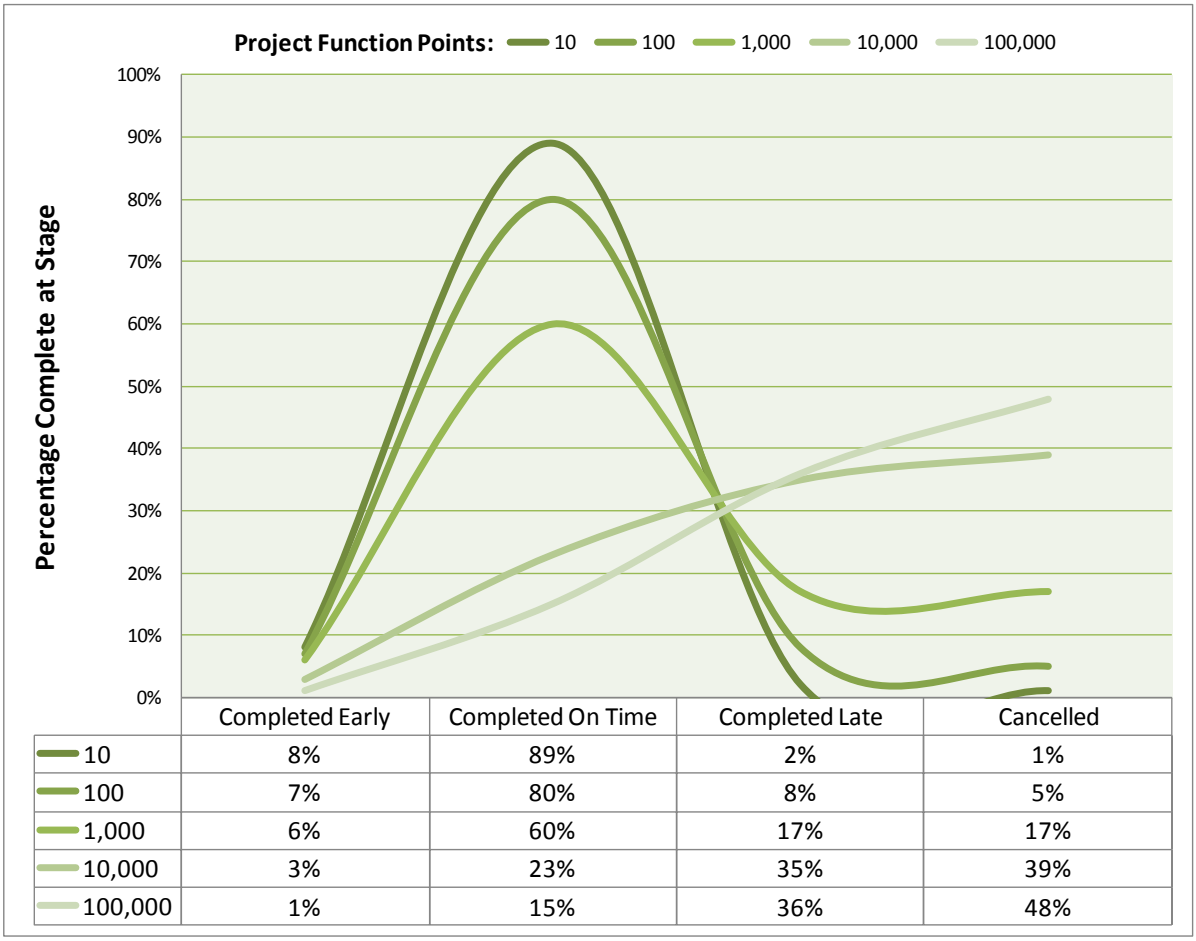
Larger highly centralized systems are tightly coupled for operational efficiency, but are burdensome for maintenance. As a result of their complexity due to numerous function points, traceability and transparency of the system, functions, and architecture are easily lost making it difficult to conduct root cause analysis should failures occur. Maintaining an up-to-date understanding of the system's business logic—terms, rules, and processes—becomes cumbersome. Therefore, these systems are difficult to customize without cascading effects on other components within the system. This leads to protracted requirements development and validation times reducing the ability to be agile in developing additional functionality. Finally, when these large systems fail, the mission of DoD is in jeopardy as risk spans across many operational components. "Incidentally," according to Capers Jones and Olivier Bonsignour in *The Economics of Software Quality*, "the largest known software projects as of 2011 are in the range of 300,000 function points. Such large projects include military and defense applications and some large civilian projects such as enterprise resource planning (ERP) applications."[83]

In contrast, smaller, distributed systems with fewer function points allow for quicker deployment of functionality. In Figure 14, the Project Function Points (the first column) represent the number of features the software delivers. The more complex a project becomes, the more Project Function Points it accrues. If incomplete, smaller projects do not jeopardize the entire transformation effort, are easier to scrap and redo, and cost less to manage and implement; most importantly, the risk is localized to that system so a DoD mission is not in jeopardy.

With smaller systems, hundreds of software vendors exist who are incentivized to be high impact, low cost solution providers. There is also added incentive for small systems to be standards-compliant because of the marketplace advantage that comes with being able to integrate with other solutions. Moreover, smaller systems can be designed, developed, and iterated very quickly. The use of standard development methodologies, libraries, and APIs with small systems avoids lock-in and allows for third-parties or other developers to contribute at a later stage of development.

Smaller, however, does not necessarily mean better. With many smaller systems there are more moving parts and more boundaries, potentially resulting in reliability and compatibility issues. ERP software vendors cite this as a marketing reason to implement their ERP systems. Therefore, the complexity of integration and contracting with many smaller software vendors must be considered against a pre-integrated solution from a single large software vendor that requires customization (at additional cost) and lacks situational agility.

[83] Capers Jones and Olivier Bonsignour, *The Economics of Software Quality*, Boston, MA: Pearson Education Inc., 2011, 444.



	Completed Early	Completed On Time	Completed Late	Cancelled
10	8%	89%	2%	1%
100	7%	80%	8%	5%
1,000	6%	60%	17%	17%
10,000	3%	23%	35%	39%
100,000	1%	15%	36%	48%

Figure 14. Software Project Success Depends on Its Size[84]

[84] Ibid. (source data).

THIS PAGE INTENTIONALLY LEFT BLANK

5. Portfolio Management and ERP Consolidation

The preceding chapters discussed the history and status of DoD ERP implementations, the next-generation ERP environment, and technologies and standards that can be leveraged in the next-generation ERP environment. This chapter presents several key findings and associated recommendations related to managing the entire business IT portfolio and the risks associated with the Department's reliance on SIs and recommends portfolio management solutions, including consolidation.

Information technology tools are continually evolving. More than ever, the consumer—not government-sponsored research and development initiatives—influences investments in technology solutions and mainstream adoption of these technologies. While return on investment (ROI) is the basic industry measure of success or failure, the Department focuses on total cost of ownership (TCO) of IT investments. A better indicator of value to the organization should take into consideration the economic characteristic of the investment and the ROI evidence by adoption rates (e.g., number of users and the ease of use). The portfolio manager, who considers the enterprise as a whole and not just its pieces, must exercise extreme discipline to achieve situational agility by assessing performance against expectations of each segment of the portfolio. Although there are multiple feasible solutions, new and more efficient solutions must also be considered during this assessment phase to achieve a portfolio's optimal performance. In other words, the Department must apply portfolio management as opposed to treating requirements and systems as distinct and unrelated, and continuously assess new technologies, approaches, and models to foster its agility for productivity and performance in tomorrow's dynamic environment.

The investment in ERP systems is substantial throughout the MILDEPs and Agencies. The DoD ERP systems have high investment costs with moderate adoption. The adoption classification of moderate is due to mixed system usage or roll-out results. For example, the DLA's EBS currently serves a relatively large user population compared to ECSS's minimal user population. If the DoD continues to invest at the high rate required to deploy ERP systems fully, several fundamental changes to the strategic segments of the portfolio management profile must be addressed.

First, the reliance on SIs and software vendors as de facto decision makers or influencers must be minimized to the greatest extent practicable. To undo this reliance requires an investment in the recruitment and retention of key government personnel who have the technical knowledge to understand software systems.

Second, whenever possible, performance and technical reviews and evaluations should carry more weight than compliance and oversight briefing reviews. Cost and schedule are highly visible measures throughout the acquisition lifecycle of a program while performance is not visible until the program reaches the test phase or is being utilized in a production environment. Therefore, there is a need for balance in terms of how the Department procures solutions and approves acquisition milestones from the cost, schedule, and performance perspectives regardless of whether it is enabling warfighting or business capabilities.

Third, the ERP system itself must become much more than just a single focused platform (e.g., financials and logistics). These ERP system investments must become a jumping-off point or platform for integrating many of the other technologies mentioned in this report (e.g., cloud computing initiatives, mobile applications, CRM, and business intelligence) in the portfolio.

And fourth, the Department should analyze the business system portfolio for potential culling when an individual ERP system is underperforming, can be integrated or accommodated by existing or new technology, or is without a significant user base. TCO can be significantly lowered for the portfolio as a whole with the retirement or canceling of a single high investment, such as an ERP system. Furthermore, when considering the net present value of money, time is truly of the essence when making this decision. Care should be taken to minimize the loss of momentum and interruption to already established business collaboration channels.

A. Reliance on Software Vendors and System Integrators

Often software vendors and SIs are too influential over DoD's systems strategies. Generally speaking, these for-profit third parties' goals and incentives do not necessarily align with those of the DoD. The Department is in need of the optimal IT solutions of today, with the lowest maintenance and overhead costs, while still producing accurate and timely results. Acquisition-compliance activities, however, are often confused with results or high performance.

Software vendors are incentivized to introduce new technology and functionality via a slow roll-out to maximize revenue. They are also driven by demands from a broader, non-DoD client base with differing and often conflicting priorities for functionality enhancements.

SIs that deploy and maintain large software systems operate business models that incentivize revenue perpetuity. Labor costs are a significant line on the cost-of-goods-sold profit/loss project statements. Most SIs use a cost reduction model that includes replacing experienced implementers with junior staff. This has the further consequence of reducing the knowledge base required for optimized client upgrade and maintenance activities and often requires extending the contracts because of schedule slippages due to rework.

The DoD's strategy to outsource technical expertise in place of internal government expertise has proven to be a false sense of economy. Instead of having government personnel with adequate breadth and depth of knowledge about technology and systems, the same software

vendors and SIs who are ultimately awarded the contracts become the de facto decision makers and influencers when choosing technologies and implementation timelines.

1. Lack of Diversity in ERP Software Vendors in the DoD

Only two ERP systems exist for the scale of users and data that the DoD is attempting to implement in an ERP system: Oracle and SAP. The complex and proprietary data models in these software solutions are incompatible with one another. All but two of DoD's ERPs implementations analyzed in this report—the Air Force's DEAMS and ECSS—are SAP. With the Department's heavy dependence on only two software vendors, a single point of failure was created should either company become insolvent, acquired, or otherwise determined no longer capable of supporting either DoD or its already implemented products within DoD.

Beyond Oracle and SAP, there are many ERP systems available from other software vendors for smaller implementations (scale of data and size of user base). In contrast to DoD's ERP implementations, no commercial entities are currently scaling their ERP systems to the size and scope of DoD. In fact, many large global corporations or conglomerates (e.g., General Electric) maintain many implementations of ERP systems across different divisions and portions of the organization and do so at a higher rate of success than DoD is achieving with its ERP systems.

2. Customization

There is a trade-off between purchasing smaller discrete software systems and taking on the cost of integrating those systems' business logic versus purchasing a pre-integrated solution, such as an enterprise ERP system with its many modules pre-integrated out of the box by the software vendor. These pre-integrated ERP solutions come with already built-in and configured data exchanges between modules; however, other customizations are still required to meet the needs of the organization's mission and associated business logic requirements. These customization efforts are widely known to cause problems when the software vendor issues patches or new releases of the software product. Customization usually attaches its own associated maintenance cost. Additionally, as the software vendor continues to improve its product, the need for customization reduces. Unfortunately, after the ERP system moves into maintenance mode, there is no incentive for an SI to either remove the previously integrated customization or maintain the top ERP system experts on the development team so as to take advantage of the software vendor's product updates and enhancements.

As described earlier in this report, one software vendor learned that an SI made 400 customizations to its product without once notifying it that changes were needed. Further, more than 25 percent of the customization items developed by the SI failed when the software was updated because the software vendor had already fixed these items in the latest patch. Without privity of contract with the DoD, the software vendor was frustrated by the inefficiency of the

environment and remarked that the customers it serves in the commercial sector would never tolerate this type of business scenario.

B. A Distributed ERP Ecosystem

The DoD ERP ecosystem can be defined as a set of distributed systems that combine to provide integrated—loosely in some cases and tightly in others—operational business systems. IDA recommends that the Department implement an distributed ERP ecosystem approach in order to consider the multiple missions and operational needs of its various organizations. As is the case with many distributed architectures, some systems are more efficiently implemented than others are. In such a diverse COI as DoD, an ecosystem approach would enable a feasible set of solutions that can be optimized for a manageable impact to the larger ecosystem's operation. Under such an approach, a producer/consumer data architecture can be established with federated trust and data exchange requirements incorporated across the ecosystem. Implementing such an ecosystem can deliver the flexibility and extensibility necessary for both diversity of mission and operations.

With the large-scale investments already committed and expended by the DoD in building its enterprise resource planning environment, retiring the existing infrastructure is neither cost effective nor efficient. There are successful and unsuccessful ERP systems. Some ERP system implementations in operation are delivering reasonable efficiencies to specific organizations. These ERP systems can and should continue to be maintained and upgraded as long as they continue to support business and operational objectives. Other ERP system implementations, however, should be considered for retirement due to excessive spending, few (if any) operational users, and unsuccessful delivery of the objective—operational efficiency and cost reduction.

Within the enterprise resource planning environment, many legacy feeder systems remain in operation. These legacy feeder systems are not usually under the control and management of the organization's decision makers for the ERP systems. As a result, different priorities must be deconflicted for these feeder systems because they may not be dedicated to just providing data to or receiving data from the ERP system. In some cases, the feeder systems were retired when the functionality of the ERP system incorporated the feeder system functionality. In other cases, RICE (reports, interfaces, conversions, and enhancements (or extensions)) components or objects were developed for the reporting of data through web service-enabled or, more commonly, legacy communications approaches between the ERP system and the feeder systems.

1. ERP Systems

To bring this disparate set of ERP systems into a distributed, yet coherent distributed DoD ERP ecosystem, a number of factors must be considered. Current ERP implementations, which require some degree of change to run efficiently in the ecosystem, fall into three action categories:

1) Integration of operational ERP systems;
2) Retirement or changes to unsuccessful ERP systems; and
3) Legacy feeder system management.

The distributed DoD ERP ecosystem should reflect the following set of characteristics for delivering operational efficiency:

- Stewardship, not ownership, of data and functionality;
- Extensibility/flexibility (e.g., producer/consumer architecture);
- Minimal user impact/ease of use;
- On-demand data access;
- Federated data management; and
- Flexibility to migrate to optional solutions (i.e., match responsibility for results with the authority to achieve them).

The Department's operational ERP systems support many users today (e.g., Navy ERP, GFEBS, LMP, and EBS). These systems are still functionally limited, resulting in each MILDEP or Agency maintaining the overhead support for legacy feeder systems. Most of the current implementations are not yet fully deployed. All the systems would require significant change to deliver the consolidation and cost efficiencies sought by DoD leadership.

2. Enterprise-Level Data Exchange Mechanisms

One component of this change to a coherent DoD ERP ecosystem can be addressed through the development and implementation of enterprise-level data-exchange mechanisms. The development and implementation of an enterprise-level data-exchange open API is critical to the DoD ERP ecosystem. It creates a foundational building block for reaching the goals of cost reduction and consolidation. If defined and implemented correctly, this API would ease integration of the disparate MILDEPs and Agency systems comprising the ERP systems environment (e.g., ERP systems, non-ERP next-generation solutions, and legacy feeder systems). Additionally, open APIs ensure the DoD COI is focused on the delivery of a federated and standardized data exchange structure, the establishment of a manageable trust model, and a flexible environment to ensure a pathway is established for the adoption of new and innovative solutions. The various MILDEP and Agency authoritative data sources can be integrated to establish a flexible composition through aggregation of any number of these data sources, based on need and demand. Insights into the Department's ERP systems that were not possible before can be delivered for planning, reporting, and risk management.

3. Integration of Operational ERP Systems

In addition to an open API, there are also existing mechanisms that can be implemented within each MILDEP and Agency for the operational ERP systems to deliver consolidation and data exchange. These mechanisms include MDM and data virtualization.

Integrating ERP systems into MDM or data virtualization mechanisms requires the extraction and comprehensive understanding of the current vocabulary set defined within each system implementation. This understanding enables stakeholders to define both the intersection points and the trust model for the data exchange. The value of such an implementation is that both aggregation and roll-up can be addressed while complying with reporting requirements.

4. Retirement of or Changes to Underperforming ERP Systems

ERP systems that are either already deployed or still under development with significant funds already consumed, but with little user adoption or use resulting in an overall underperforming evaluation, require a reassessment prior to any further funding. It may be best to retire an individual ERP system and migrate it into an existing operational ERP system. When the user community is small, migration of business functions should not be a significant investment, especially if the ERP system implemented is from the same software vendor (e.g., ECSS accounting functionality to DEAMS).

Should the ERP system migration not be to the same vendor (e.g., Oracle to SAP or SAP to Oracle), migration may require extraction of custom business logic for porting to an alternate software vendor solution—either another ERP or a business process management solution (e.g., Appian). The extraction of this custom business logic for migration can leverage KDM/BPMN standards based automated extraction tools.

This migration can significantly reduce the costs of an ERP system investment, SI custom development, and maintenance costs of the ERP system or its custom code. When bringing different functions—such as financials and logistics—into a consolidated solution set, understanding the business logic between operations and the vocabulary set as it relates to the business logic is an important step in a successful consolidation. This effort would enable the organization to develop a solution based on not only doing a situational analysis but also considering the situational agility for implementing the more complex set of enterprise business processes across multiple business functions (e.g., financial and logistics, financial and human capital management). Additionally, vendor software lock-in instances are reduced or become manageable.

5. Legacy Feeder Systems Management

Legacy feeder systems will continue to exist in the DoD enterprise resource planning environment. Depending on the flexibility of the owner/steward of these legacy systems, retirement may or may not be an option. The best approach to addressing these legacy systems is

to first understand the complexity of the implementation of ERP-specific feeder functions within these legacy systems. The understanding and extraction of business logic and data structures opens the door for stakeholder discussion on how best to approach these legacy systems, including:

- Removal of business functions for direct integration into the ERP systems;
- Web service enablement; and
- Establishment of the legacy system as an independent authoritative data source by integrating the system into the enterprise API.

Funding for such activities is driven by the legacy feeder system stakeholder and may require decisions outside of the scope of the ERP system owner to invest in extraction activities. In the past, this activity was tedious and manual with rudimentary tools. With the advent of international standards and automated tools delivering comprehensive extraction, this step may be less painful to fund and implement. Managing the SI for proper application of tools is an important step because the SI has little incentive to apply these tools optimally—the automated tools have a direct negative impact on revenue. These activities can be managed through the clear definition of what is to be extracted (business logic and data structures). With close management, web-service integration into the ERP system, web-service enablement of the legacy system, or integration into the API are reasonable to manage and are cost-effective.

Bringing together a combination of system elements to achieve enterprise-level ERP system consolidation within the DoD requires multiple steps by multiple MILDEPs and Agencies along with specific stakeholders who may or may not be directly tied to the goals and objectives of the enterprise resource planning environment. By bringing together a common API, leveraging some innovation in extraction and analysis standards/technology, and applying alternate business process management and data integration mechanisms while retaining existing ERP implementations, the DoD enterprise resource planning environment can reach a level of optimization and cost-effectiveness. With such an implementation, the ability to deliver agility, extensibility, traceability, and operational efficiency can become a reality in the Department.

C. ERP Consolidation Risks and Considerations

Transitional risks are often deferred by protracted cutover plans (longer timelines) from legacy systems to the new technology that is meant to subsume the requirements of the previous processes/systems. The increasingly abbreviated development cycle of new capabilities requires transitional approaches that take into account what an organization thinks will be compatible with a future technology and what future operations of that organization will demand. The benefits of further consolidation of DoD's ERP systems beyond what has already been accomplished, while feasible, may result in a false sense of economy for the Department for the following reasons:

1) Potential loss of momentum in DoD business ERP system implementations that service a significant user base and are providing benefits to the enterprise;

2) The inherent technical risks; and

3) The possibility of interruptions to already established and tested business collaboration channels.

1. Legacy ERP Integration vs. Functionality

In Figure 15, one would be inclined to believe that Systems A and B may be consolidated because of the existence of an overlap in capabilities and functions. This is the case if the functions and capabilities as depicted are suitably generic to allow for this occur. If Function 1 is Manage Funds, for instance, DoD may view that GCSS-Army, GFEBS, and Navy ERP all have and can handle this function; however, at the Manage Funds level of description, it is not discernible whether the functions underlying each ERP systems' functionality are implemented in a way in which combination of the user communities is compatible. There may be cultural or procedural reasons why the two cannot be consolidated.

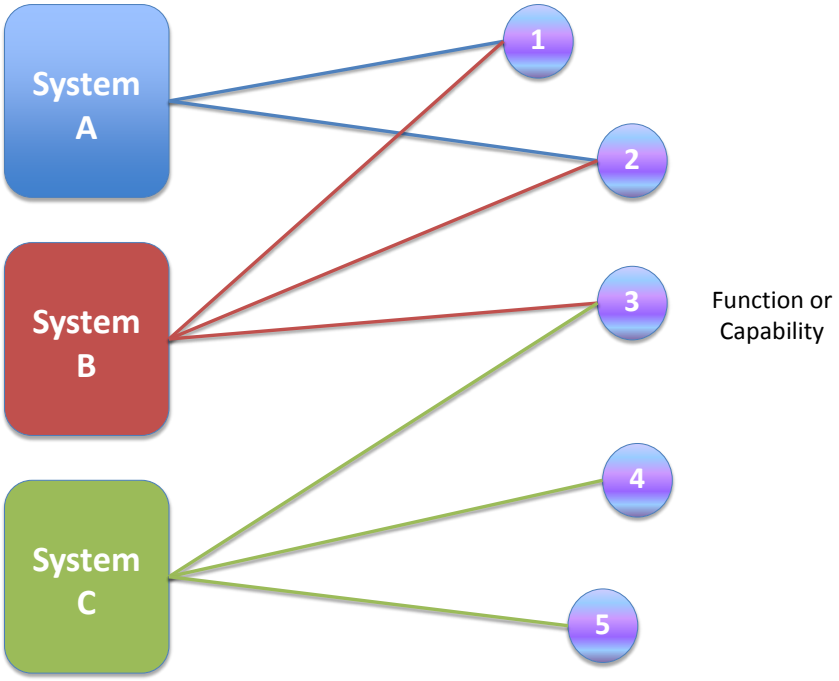


Figure 15. System Consolidation and Functionality Matching

Surprisingly, it may be a better alternative to consider a consolidation of Systems A and C since there is no overlapping functionality between the two. In this case, perhaps Functions 1 and 2 are financial management functions while Functions 3, 4, and 5 are supply functions. Consolidating Systems A and C may result in several benefits, such as (1) reduced costs due to smaller program and functional management offices, (2) fewer software licenses across the DoD enterprise, and (3) less hardware required to run the software. None of these benefits is the result

of the ERP system's inherent capabilities; rather, the benefits come from the approach that DoD takes to implement the management aspects related to such an application.

2. Examples of ERP System Consolidations

Two obvious examples of ERP system consolidation and integration are provided by current consolidation activities occurring within the Navy and the Army. The remaining potential consolidation examples are derived from IDA's analysis of the ERP systems. They are:

- Merging GFEBS into GCSS-Army; and
- Moving the accounting functionality in ECSS to DEAMS.

All the consolidation examples involve ERP consolidation within a single MILDEP.

a. Navy ERP

Within DoD, the Navy ERP is the leading example of ERP system consolidation underway. The Navy System Commands (SYSCOMS)—Naval Air Systems Command (NAVAIR), NAVSUP, Naval Sea Systems Command (NAVSEA), and Space and Naval Warfare Systems Command (SPAWAR)—developed four pilot programs called SIGMA (Financial and Program Management), SMART (Supply and Maintenance), NEMAIS (Maintenance), and CABRILLO [Financial (Working Capital Fund) and Work Force Management], respectively in the late 1990s and early 2000s.

In 2003, the Assistant Secretary of the Navy (Research, Development and Acquisition) directed convergence of these pilots into a single ERP implementation based on SAP.[85] With NAVY ERP Version 1.0, NAVAIR consolidated Navy financial management for use by all the SYSCOMS. With Version 1.1, NAVSUP is in the process of consolidating Navy logistics management for use by all the SYSCOMS.[86] The Navy received a Full Deployment Decision acquisition decision for Navy ERP on June 30, 2011.[87]

As depicted in Figure 16, the Navy ERP is called an apartment or a multi-tenant ERP system because each user sees only one ERP system. Also shown is the generic representation of the user and legacy system interfaces. The Navy ERP architecture indicates that the NAVAIR consolidation of Navy financial management is complete, whereas the NAVSUP consolidation of logistics management is incomplete.[88]

[85] Navy ERP Program, History, http://www.erp.navy.mil/history.html.

[86] Navy ERP Program Management Office.

[87] Navy ERP Program, "USD(AT&L) Signs Full Deployment Decision (FDD) Acquisition Decision for Navy ERP," News and Releases, July 11, 2011, http://www.erp.navy.mil/news_and_releases/news38.html.

[88] Navy documentation currently available to IDA does not permit determination of legacy application integration status or ERP functionality to be consolidated by NAVSEA and SPAWAR.

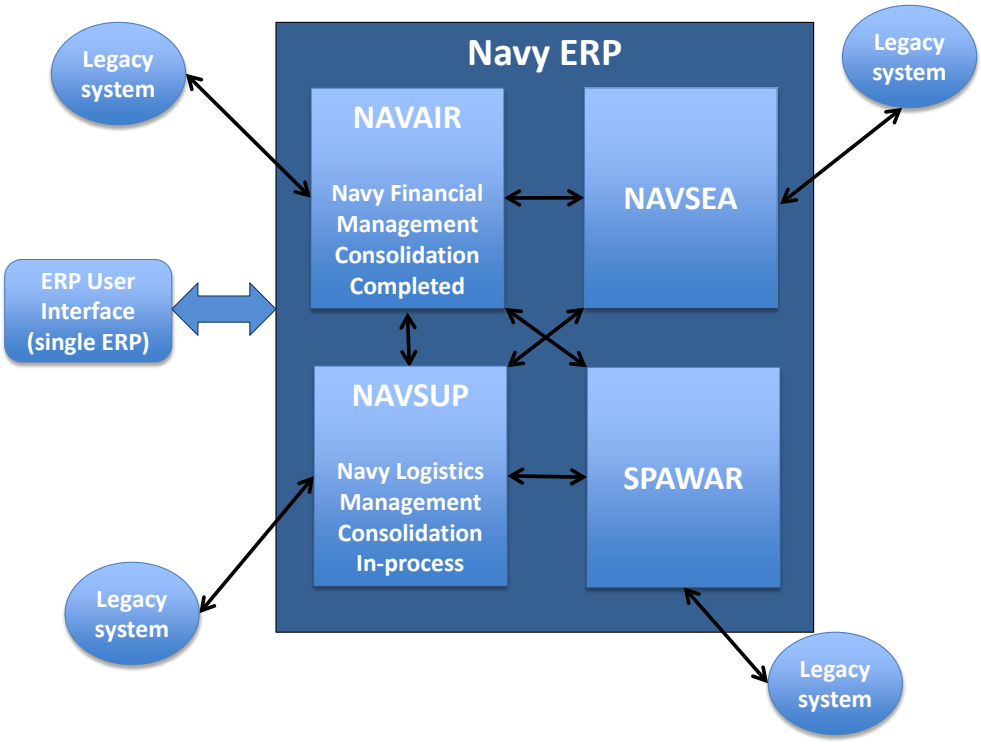


Figure 16. Depiction of the Navy ERP Architecture

b. Army ERP Integration

The Army is also in the process of consolidating its ERP systems via a federated approach, which is described in the *Army Business Systems Information Technology Strategy 2011* (BSIT Strategy). The BSIT Strategy explains the Army's system integration as follows:

> The process for defining the system integration methodology among the key deployed Army ERP systems (GFEBS, GCSS-Army, LMP) and their non-ERP systems has required a pairing analysis in which the integration requirements of each set of systems are understood in the context of the broader business processes they support. This is a critical step for aligning with end-to-end processes for execution across the Army. Further context and standardization of methods are applied in cross-program coordination efforts and with the support of the Army's ERP integration platform, the Army Enterprise Systems Integration Program (AESIP).[89]

89 Department of the Army, Office of Business Transformation, *Army Business Systems Information Technology Strategy 2011*, February 14, 2011, 8, http://www.armyobt.army.mil/downloads/sec-army-approved-bsit-strategy_final.pdf.

With AESIP, the Army will "use a data management/data broker concept to enable master data management, eliminating, where possible, point to point communications and enable cross-functional reporting capabilities as appropriate" to achieve data quality management and data integrity.[90]

GFEBS, GCSS-Army, and LMP are all SAP ERP software implementations; AESIP is not an ERP but incorporates SAP's MDM capability. Using MDM, AESIP "synchronizes and syndicates select enterprise master data (e.g., vendor and customer master) as applicable to each Army ERP system. Additionally, AESIP supports integration hub services for each ERP system, as applicable."[91] Examples of master data known to SAP MDM are material, equipment, assets, customers, vendors, and cost centers. MDM assigns unique internal IDs to everything to aggregate and build structures on which all functionality is based.

The Army's ERP system integration is shown in Figure 17. The role of each ERP—GFEBS (Army general ledger), LMP (wholesale logistics), and GCSS-Army (tactical logistics)—is identified with supporting functions. AESIP is the hub or data-integration broker that links the ERP systems through brokering, MDM, and Cross Functional Business Intelligence.

The Army's BSIT Strategy claims that "[t]he Army's governance and oversight eliminates the risk of redundant capabilities built in multiple ERP systems and ensures compatibility and the appropriate level of integration among the programs."[92] This federated approach to consolidation is innovative and may demonstrate scalability of the SAP ERP systems; it may also be of interest in other contexts within the Department.

[90] Ibid., 16.

[91] Ibid., 10.

[92] Ibid., i.

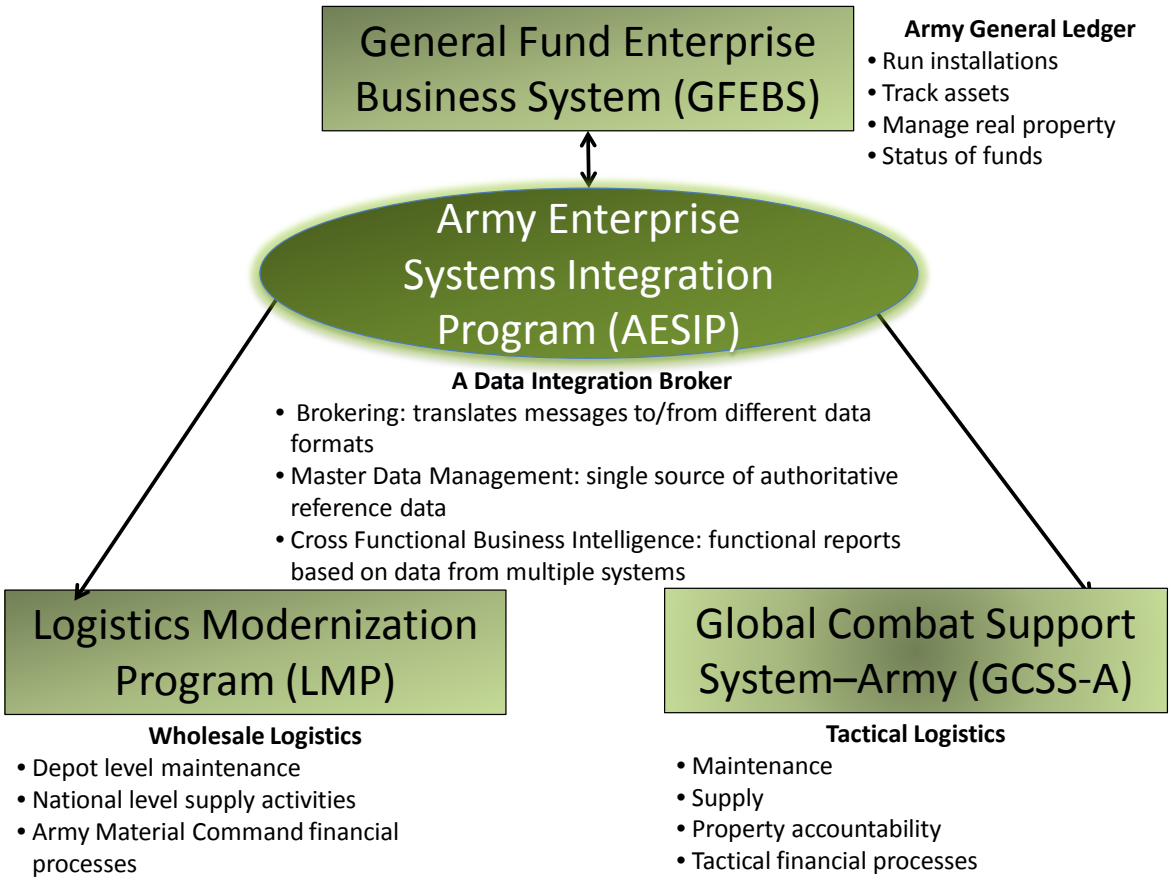


Figure 17. Army ERP Integration Strategy with AESIP

c. GFEBS to GCSS-ARMY

In comparing BEA 8.0 capabilities of GFEBS and GCSS-Army, the results in Table 2 suggest that GCSS-Army could implement almost all of GFEBS capabilities. Only one GFEBS capability (Real Property Acceptance) is not currently reported as being performed by GCSS-Army.

Table 2. BEA Version 8.0 Capabilities: GCSS-Army and GFEBS[93]

BEA Version 8.0 Capabilities (21 of 38 capabilities implemented by these ERP systems)	GCSS-Army	GFEBS
Collect and Disburse	■	■
Conduct Program Management	■	
Deliver Property and Forces	■	
Dispose or Return Property and Materiel	■	■
Environmental Liabilities Identification and Valuation	■	■
Financial Reporting	■	■
Forecast, Plan, Program, Budget, and Funds Distribution and Control	■	■
Hazardous Materials Process Controls and Information Management	■	
Manage Acquisition Oversight Integration	■	■
Manage Financial Assets and Liabilities	■	■
Manage General Ledger	■	■
Manage Organization	■	
Manage Payment	■	■
Manage Receipt and Acceptance	■	■
Manage Request	■	
Manage Sourcing	■	■
Managerial Accounting	■	■
Perform Asset Accountability	■	■
Perform Build and Make and Maintenance and Sustainment	■	■
Real Property Acceptance		■
Real Property Inventory	■	■
Grand Total	**20**	**16**

d. ECSS's Accounting Functionality to DEAMS

When considering a transition of functionality related to accounting activities for Working Capital Fund (WCF), a transfer of the WCF functionality from within ECSS, where it currently resides, to DEAMS, where the General Fund functionality or General Ledger is contained, should be considered with the caveat that the associated logistics that drive those transactions must be taken into account. The current performance of ECSS requires alternatives to the Air Force's accommodation of accounting functionality. First, this pull-through of functionality

[93] DITPR data extracted on January 10, 2012. The Army last updated the DITPR for GCSS-Army and GFEBS on December 11, 2011.

would be an Oracle-to-Oracle consolidation since both DEAMS and ECSS are Oracle-based ERPs. Although the Air Force experiences the same ERP software vendor lock-in condition as described earlier in this report, the lock-in for both DEAMS and ECSS is with the same software vendor. Therefore, there is a reasonable expectation that Oracle would have more of an incentive to accomplish a collaborative knowledge transfer because of past performance tracking and reputation considerations. Second, the functionality to be combined is an accounting-to-accounting transition. DEAMS is the Air Force's accounting system of record. The details regarding the relationship of the business event operationally to the financial trigger and final transaction posting and recording could potentially be streamlined. Third, the users of both of these systems are small in magnitude at this point in the deployment schedule. In particular, ECSS has very few users. The timing of this decision is important because current exposure is limited, and change is more manageable. However, the current SIs may be reluctant to work together (each program has a different SI). The Navy faced a similar dilemma when it consolidated its ERP pilots with IBM and BearingPoint as SIs.

Based on a comparison of the financial management capabilities in BEA Versions 7.0 and 8.0 for DEAMS and ECSS (see Table 3), the results suggest that DEAMS could likely implement all of ECSS's planned financial management capabilities. Only one ECSS financial management capability (Managerial Accounting[94]) is not currently reported as being performed by DEAMS. However, given DEAMS' role as the Air Force's general ledger system of record, performing this capability could be easily implemented through the Oracle ERP software.

[94] BEA Versions 7.0 and 8.0 both define "managerial accounting" as "Ability to accumulate, classify, measure, analyze, interpret and report cost and other financial information useful to internal and external decision makers reviewing the execution of an organization's program or project resources to ensure they are effectively being used to meet objectives." *CV-2 Capability Taxonomy (Business Capability)*,BEA Version 7.0, http://www.bta.mil/products/bea_7_0/BEA/iwp/bealist_businesscapability_na.htm;*CV-2 Capability Taxonomy (Business Capability)*, BEA Version 8.0, http://www.bta.mil/products/BEA_8_0/index.htm.

Table 3. BEA Capabilities: DEAMS and ECSS[95]

BEA Capabilities [16 of 38 implemented by these ERP systems; of these, only 7 are related to financial visibility(marked with an "*")]	DEAMS -- BEA 8.0	ECSS -- BEA 7.0
Collect and Disburse*		
Deliver Property and Forces		
Dispose or Return Property and Materiel		
Environmental Liabilities Identification and Valuation		
Financial Reporting*		
Forecast, Plan, Program, Budget, and Funds Distribution and Control*		
Hazardous Materials Process Controls and Information Management		
Manage Financial Assets and Liabilities*		
Manage General Ledger*		
Manage Payment*		
Manage Receipt and Acceptance		
Manage Request		
Manage Sourcing		
Managerial Accounting*		
Perform Asset Accountability		
Perform Build and Make and Maintenance and Sustainment		
Grand Total	**5**	**16**

D. A Different Approach to Consolidation

With the rare exception of pulling the AF's accounting and financial functionality through from ECSS to DEAMS, a better strategy may be to redefine what is meant by consolidation. The Department should begin expending resources to initiate a shift from a product-centric approach to a utility services approach to achieve the Department's transformation and efficiency goals. Furthermore, additions to development funding for the legacy ERP systems now in place should be minimized and the solutions currently in place should be leveraged to the maximum extent

[95] DITPR data extracted on January 10, 2012. The Air Force last updated the DITPR for DEAMS and ECSS on December 30, 2011. BEA 8.0 data not available for ECSS. "Financial Visibility" is defined as "[h]aving immediate access to accurate and reliable financial information (planning, programming, budgeting, accounting, and cost information) in support of financial accountability and efficient and effective decision-making throughout the Department in support of the missions of the warfighter." http://www.bta.mil/products/bea_7_0/BEA/html_files/bep.html.

possible. In other words, the Department should accept an 80 percent solution. Those ERP systems with a minimal user base should be cancelled and, when and where possible, the funds should be reallocated to more forward-leaning approaches.

Some caution is still recommended when it comes from shifting to a utility-services approach. Wardley, an expert on cloud, recently blogged that:

> …The shift from products to utility services inevitably incurs various forms of risks. These include **disruption** risks such as loss [of] previous skillsets and political capital to **transitional** risks such as changes to governance and transparency of suppliers to **outsourcing** risks such as pricing competition and loss of strategic control. There is an inevitable cost of architectural transition from one set of best practices to another.[96]

The inevitable cost alluded to can be clarified by reviewing Jevons paradox (sometimes referred to as Jevons effect). This proposition in economics states that:

> …as technological improvements increase the efficiency with which a resource is used, total consumption of that resource may increase, rather than decrease but it is not a paradox at all and is well understood by modern economic theory which shows that improved resource efficiency may trigger a change in the overall consumption of that resource, but the direction of that change depends on other economic variables.[97]

In illustration of this paradox, Wardley further noted that:

> …cloud is simply a result of a standard process of evolution that inevitably leads to operational efficiency through provision of a commodity. A consequence of this is it also enables higher rates of innovation for new business activities (such as big data) through the combined effects of [componentization] and creative destruction.
>
> …As competitors gain the benefits of more efficient commodity provision and higher rates of creation, this is unlikely to result in a reduction in IT budgets but instead more IT activities undertaken... We've seen this for the last thirty years i.e., as IT has become more efficient, IT budgets haven't fallen but we've just ended up doing more stuff.[98]

Figure 18 summarizes the risks and recommendations associated with ERP Consolidation.

[96] Simon Wardley, "Future costs and Cloud," *Bits or pieces?*, blog post, December 7, 2011, http://blog.gardeviance.org/.

[97] "Jevons Paradox," Webster's Online Dictionary, last visited on January 5, 2012, http://www.websters-online-dictionary.org/definitions/Jevons.

[98] Wardley, "Future costs and Cloud."

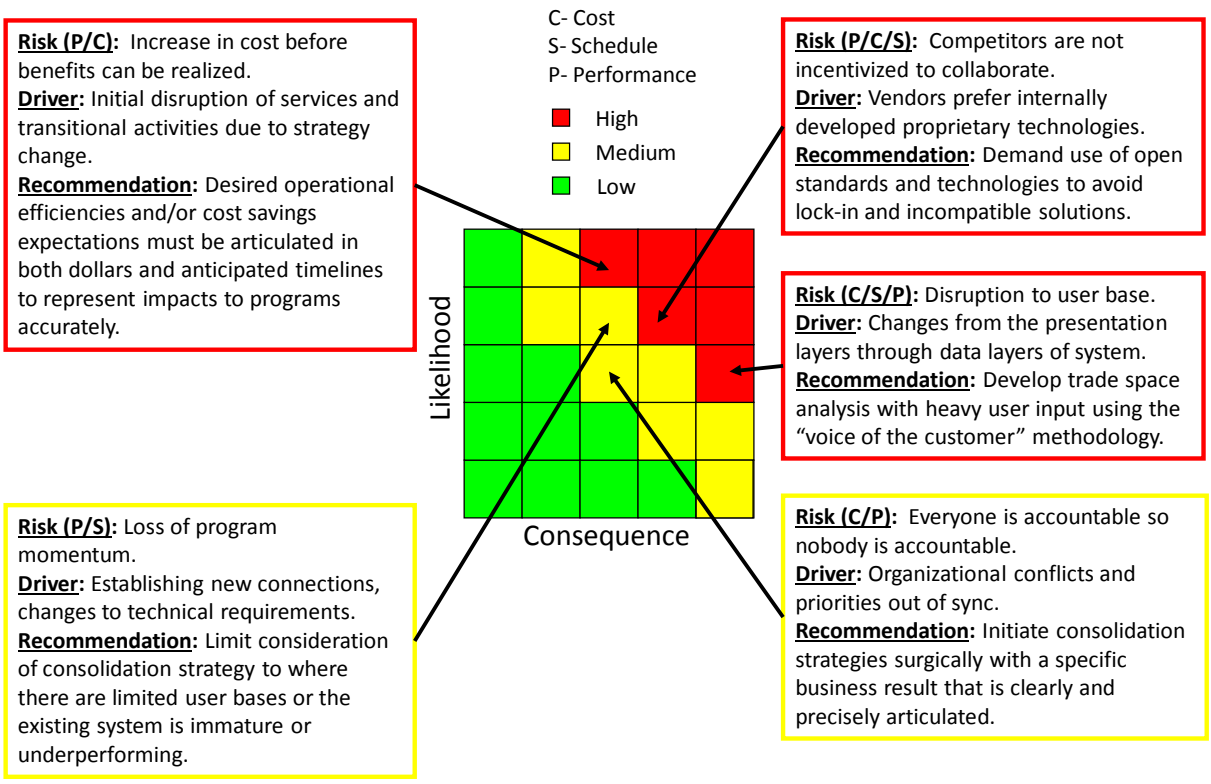


Figure 18. Risks and Issues with ERP System Consolidation

THIS PAGE INTENTIONALLY LEFT BLANK

6. Overarching Findings and Recommendations

This report describes DoD's history and current status with ERP systems, new technologies and data architecture models, and opportunities and constraints for moving forward to the next-generation ERP environment. The preceding chapters provide detailed trade-space analyses of the risks associated with DoD legacy business systems and the current ERP system environment, the next-generation ERP environment, and ERP system consolidation. This chapter summarizes some of the common themes related to findings and recommendations from the trade-space analyses.

A. Overarching Findings

Situational agility is critical to addressing business requirements more effectively. It leverages evolving technologies and analytical techniques that may improve on or replace methods currently used in DoD business operations. The clean insertion of new approaches and quick realization of benefits requires agility in how the DoD applies contract instruments and in implementing technical modules.

This agility must be balanced with the DoD's need to continue making progress on more successful ERP program implementations while minimizing the potential loss of momentum or the addition of unanticipated costs that are required to meet the 2017 deadline for audit readiness (consolidated balance sheet and a net cost for the entire Department) and the 2014 Statement of Budgetary Resources (funds received, obligated, and expended).

The need to streamline processes and gain efficiencies through the use of IT is complicated by the evolving nature of IT. More than ever, commercial consumers—not DoD's buying power—influence technology developments.

While ROI is the basic industry measure of success or failure, the Department focuses on TCO of IT investments. A better indicator of value to an organization would be to take into consideration the economic characteristic of the investment and the ROI evidence by adoption rates (e.g., number of users and the ease of use).

Portfolio management forces an enterprise perspective of requirements, investments, and priorities instead of treating requirements as distinct and unrelated. With this approach, portfolio managers must exercise extreme discipline to achieve situational agility by assessing performance against expectations of each segment of their portfolio. Situational agility involves dynamic understanding and leveraging of financial, logistics, human capital management, and other business functions using portfolio management as an enabler of innovation to fulfill needed capabilities.

If the DoD continues at the high investment rate required to deploy the business ERP systems fully, the following fundamental changes to the strategic segments of the portfolio management profile must be addressed:

- The reliance on SIs and software vendors to implement ERP systems must be minimized to the greatest extent practicable. To undo this reliance requires an investment in the recruitment and retention of key government personnel who are knowledgeable about ERPs and systems.
- ERP program compliance with the Defense Acquisition System (including administrative and oversight activities) must not be confused with achieving results. Whenever possible, performance and technical reviews and evaluations should carry more weight than compliance and oversight briefing reviews.
- Each ERP system must become much more than a single-focused platform (e.g., financials and logistics). These ERP system investments must provide the foundation for integrating other technologies (e.g., cloud computing initiatives, mobile applications, customer relationship management, and business intelligence). The Department's heavy dependence on only two software vendors will result in vendor lock-in, potentially leading to a single point of failure.

B. Overarching Recommendations

DoD can better manage its investments in ERP systems and the next-generation ERP environment by:

- Taking advantage of the emerging technologies and approaches, such as the increasing shift from products to services as tools to accomplish business transformation goals as alternatives to ERPs.
- Initiating an objective assessment of what the ERP systems can realistically deliver.
- Creating an environment where decisions to cancel under-performing programs and re-allocate funding are as routine as decisions to continue performing programs.
- Establishing incentives for enterprise leadership (beyond the Services) and stewardship for managing the Department's IT investments. Every investment should meet a common purpose that achieves an outcome beyond just one MILDEP or Agency.
- Using aggregate data methods to the greatest extent practical. As Defense business systems become increasingly linked and are hosted in dynamic commodity computing environments, data ownership will evolve into a data stewardship model.
- Recognizing organizational constraints—both mission and political—and focusing on high performance, not just high compliance, when making IT investments.

- Implementing IT solutions that address the entire doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) spectrum.
- Controlling the business logic across financial, logistics, human capital management, and other business functions instead of allowing the ERP software vendor or SI communities to set the logic. Control of the business logic will prevent inflexible lock-in to particular vendors, products, or business models.

C. Discussion of Recommendations

In lieu of simply enforcing compliance, DoD should undertake a portfolio management approach to manage its ERP investments and enable innovation. Physical collocation and mental collaboration among developers, end users, and program managers is essential for successful programs to produce results (data products). The functional operational managers (i.e., logisticians, accountants, and program managers), in turn, need to determine if the products will meet mission needs (data production) and whether the products will be able to interoperate with the small number of data producers. Functional operational managers should also be afforded the opportunity to use products from other MILDEPs and Agencies, which results in the re-use of existing investments in the DoD portfolio. Alternative options include purchasing COTS products that better meet the needs at a local functional level or even developing small-scale applications tailored to the business process and mission needs of that functional organization. In this scenario, government personnel who are *part of* the organization requiring a tool rather than part of a distant IT group have greater understanding of user issues and requirements without lengthy requirements gathering processes.

Furthermore, developers throughout the organization can re-use published APIs and implemented systems to integrate their solutions with and build upon already implemented systems, rather than building the same systems twice. An industry analog would be where a functional manager is required to use SalesForce.com to manage customer relationships for the company. This manager has a particular requirement for mobile devices to accomplish the company's mission most effectively. SalesForce.com runs in a web browser and does not meet this requirement. However, if the manager is empowered to find a way to meet this requirement, he could extend the Salesforce.com product by using its Appforce engine to create or purchase third-party applications for mobile-device platforms that connect into the main Salesforce.com product.

Placing the power to produce results at the functional level within constraints set by the portfolio manager allows for a responsible champion at a local (functional) level rather than just at a high level. Although senior-level champions are needed to support critical initiatives, high level executives are generally too removed from the local business processes to create a sense of ownership over results alone; ownership at both high and low levels is necessary for success.

When developing smaller systems for a local group, functional managers should own development (democratization of system design/development). The major premise remains the same; that is, each individual solution should fit into the larger system of systems (enterprise resource planning environment) and obtain buy-in from the highest-level business champions. This organizationally minimizes the perceived disconnect of higher-level champions with regard to day-to-day processes. Democratizing to a lower level for development fosters executive buy-in and organizational alignment across all levels of the enterprise.

Cloud and other technologies still may not solve all of DoD's enterprise integration and efficiency issues. Nevertheless, where practical, cloud and other technologies are available alternatives to the ERP systems to meet user needs and requirements as part of the overall Department's IT investment portfolio.

D. Related Recommendations in Support of DoD Productivity and Performance

1. Extending Should Cost Guidance to Defense Business Systems

Affordability analysis as a requirement at milestone decision points for all Acquisition Category (ACAT) I programs was mandated effective November 15, 2010.[99] Although the Department's business systems were not included in this initiative, IDA recommends that similar implementations of affordability-based decision making at milestone decision points for these systems be considered.

In addition, IDA believes these Defense business systems should also target productivity through *will-cost/should-cost* management—that is, "executing to what the program *should cost*."[100] This would include should-cost targets developed using proven estimating techniques based on bottom-up assessments of what programs should cost if reasonable efficiency and productivity enhancing efforts were undertaken. These costs would be used as a basis for contract negotiations and renegotiations as well as contract incentives to track contractor and program executive officer performance. In addition, capability redundancies should be identified for elimination with enthusiasm as individual MILDEP and Agency portfolios are reviewed for possible reductions in costs to that component and across the DoD enterprise.

99 Ashton B. Carter, USD(AT&L), *Implementation Directive for Better Buying Power—Obtaining Greater Efficiency and Productivity in Defense Spending*, Memorandum, November 3, 2010, 1, http://www.acq.osd.mil/docs/USD(AT&L)_Implementation_Directive_Better_Buying_Power_110310.pdf (hereinafter referred to "Implementation Directive for Better Buying Power").

100 Ashton B. Carter, USD(AT&L), *Better Buying Power: Guidance for Obtaining Greater Efficiency and Productivity in Defense Spending*, Memorandum, September 14, 2010, 3, http://www.acq.osd.mil/docs/USD_ATL_Guidance_Memo_September_14_2010_FINAL.PDF ("*I will require the manager of each major program to conduct a Should Cost analysis justifying each element of program cost and showing how it is improving year by year or meeting other relevant benchmarks for value.*").

The Department's initiative to reduce nonproductive processes and bureaucracy in the acquisition process includes a requirement to review all MILDEP and Agency-required "acquisition documents for redundancy with OSD-required documents and eliminate redundant documents and non-value-added content,"[101] This initiative should be extended to the ongoing multi-layered reviews of business system programs.

2. Ongoing Department Changes—Organizational and Processes

Multiple and redundant governing bodies at the OSD-, MILDEP-, and Agency-levels create a lack of trust, confusion, lack of unity of effort, increased resource requirements, and distraction from program execution. DoD views business modernization and financial improvement problems as IT system investment problems, not operational problems. DoD should solve business modernization and financial improvement problems that span the entire DOTMLPF spectrum (including auditability) by focusing on the entire enterprise resource planning environment as opposed to just ERP systems.

The growth of governing bodies within DoD continues. The passage of the National Defense Authorization Act for Fiscal Year 2012 again took aim at DoD's redundant systems for accounting and business operations. It directed the DCMO to establish an investment review board by March 15, 2012. This board will conduct trade-space evaluations of business systems and management processes from a number of perspectives, including scope, complexity, and cost. The goal is to streamline systems aggressively across DoD's business management communities.[102] It is imperative that this new board be aligned, combined with, or replace existing governing bodies.

Finally, cost and schedule are highly visible measures throughout the acquisition lifecycle of a program, but performance is not visible until the program reaches the test phase or is being used in a production environment. Therefore, whenever possible, performance and technical reviews and evaluations should carry more weight than compliance and oversight briefing reviews in determining whether a program should continue.

[101] "Implementation Directive for Better Buying Power," at 7.

[102] National Defense Authorization Act for Fiscal Year 2012, Sec. 901. REVISION OF DEFENSE BUSINESS SYSTEMS REQUIREMENTS. Public Law 112-81, December 31, 2011.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A. Trade-Space Analyses

For reader assistance, the following trade-space analyses are provided as full-page figures:

- Figure 19: Risks and Issues with Legacy Systems in an Enterprise Resource Planning Environment
- Figure 20: Risks and Issues in Legacy ERP Systems
- Figure 21: Risks of Moving to the Next-Generation ERP Environment
- Figure 22: Risks and Issues with ERP System Consolidation

THIS PAGE INTENTIONALLY LEFT BLANK

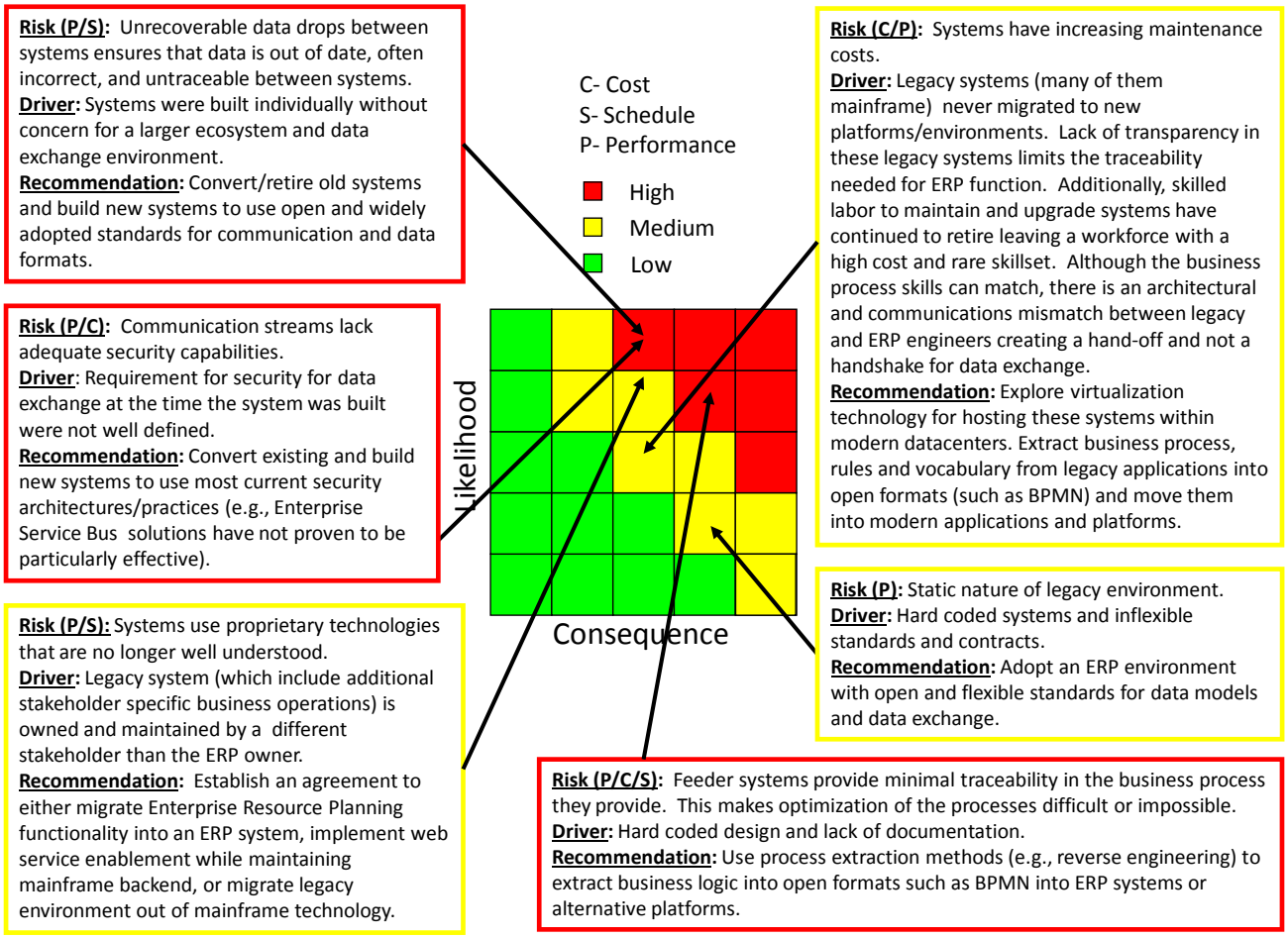


Figure 19. Risks and Issues with Legacy Systems in an Enterprise Resource Planning Environment

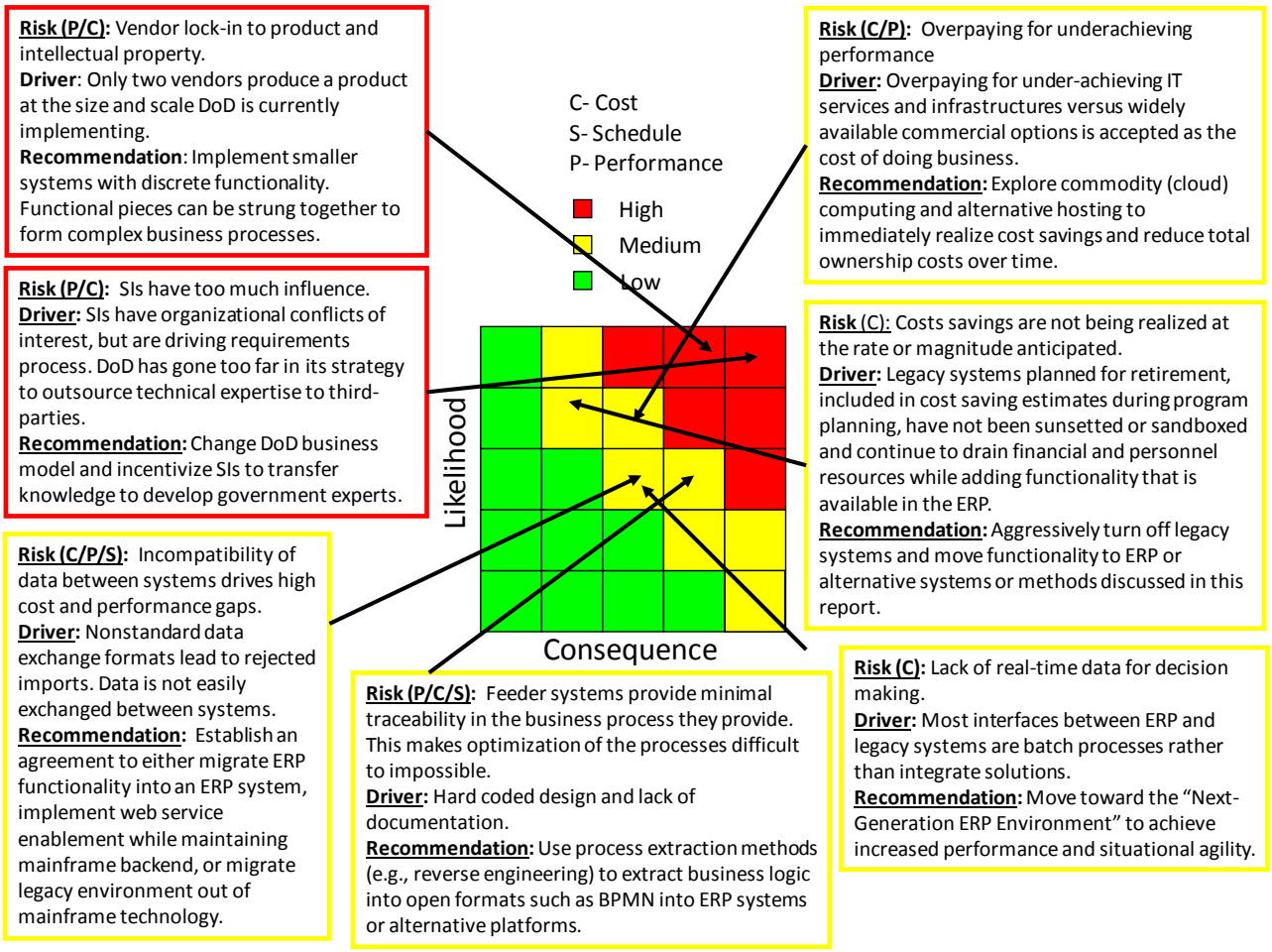


Figure 20. Risks and Issues in Legacy ERP Systems

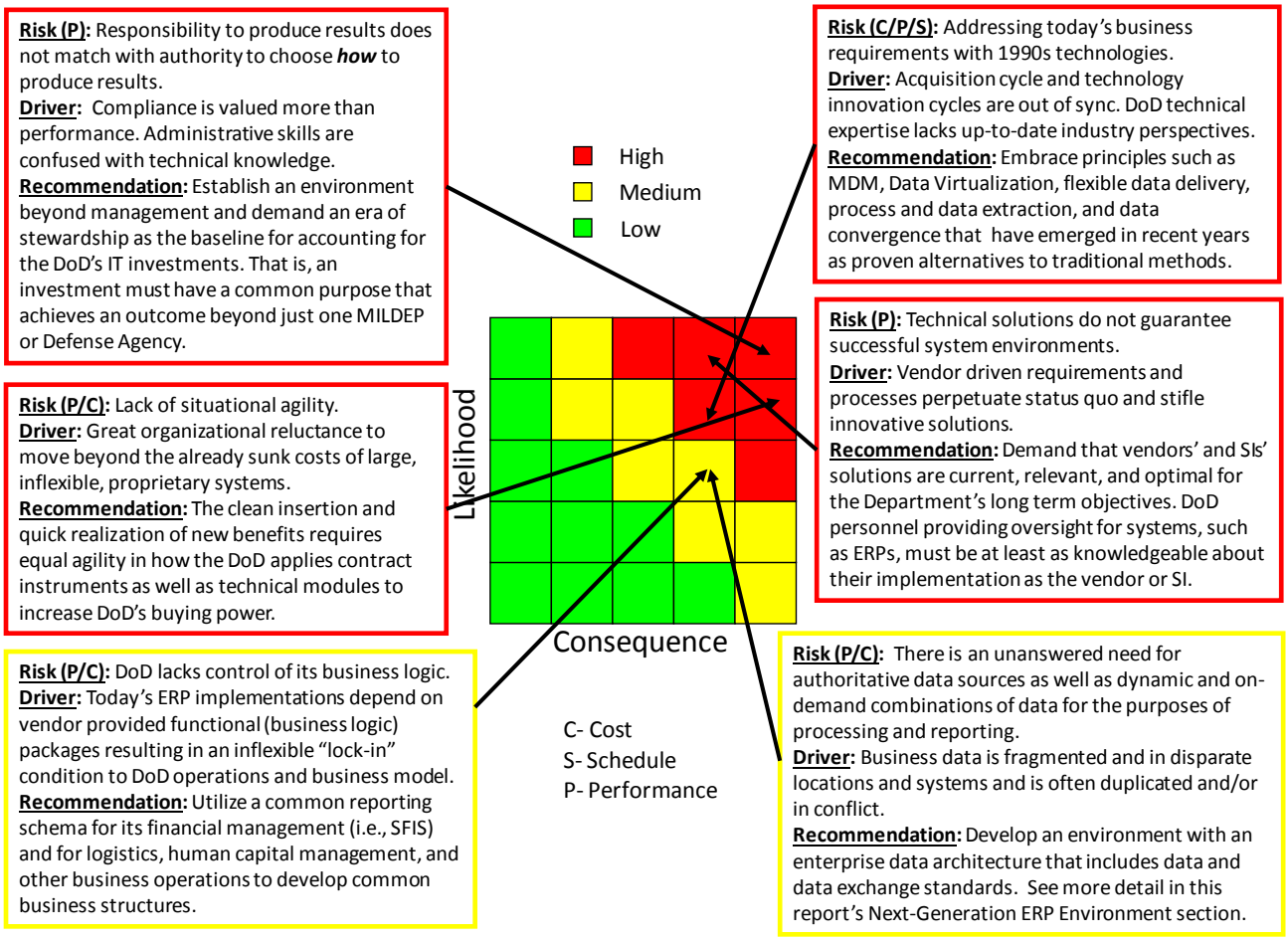


Figure 21. Next-Generation ERP Environment Risks

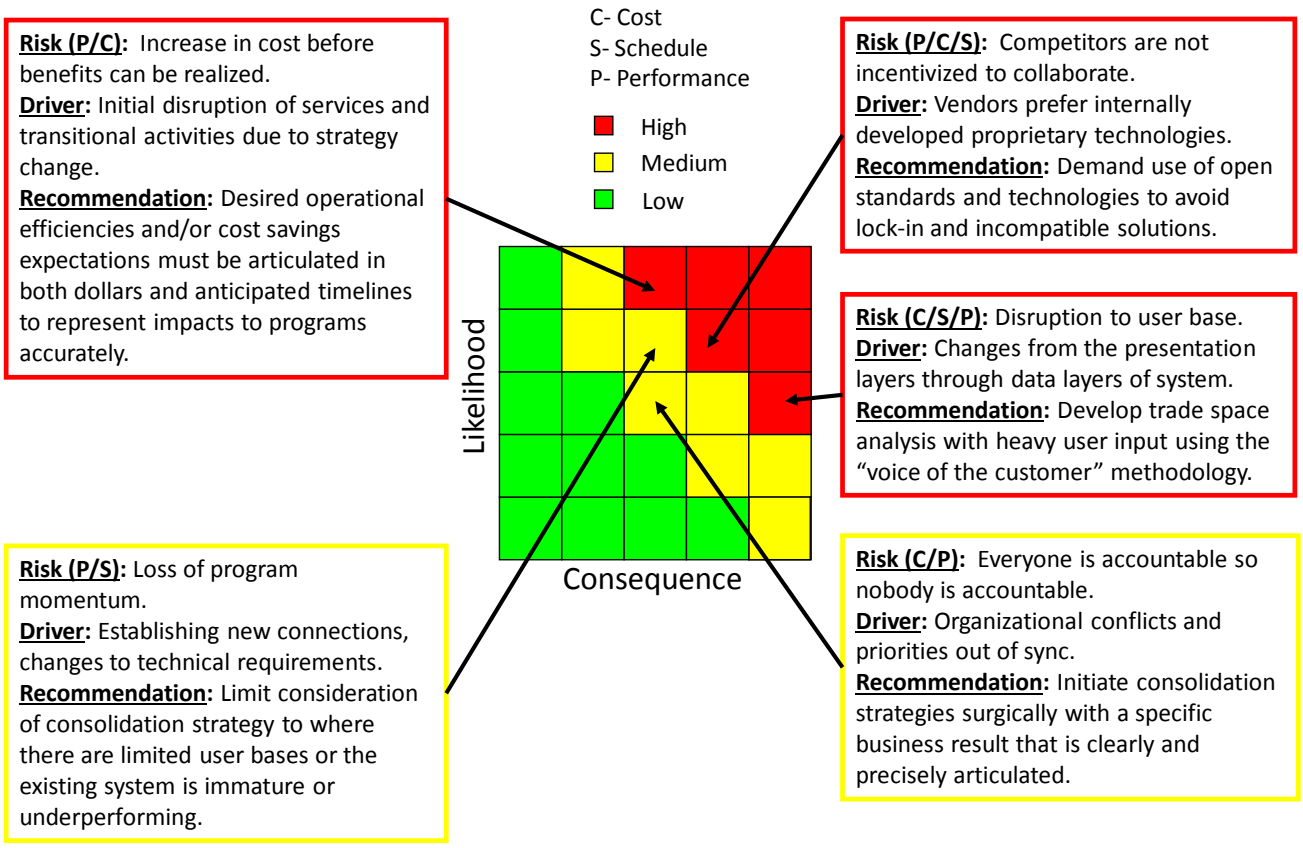


Figure 22. Risks and Issues with ERP System Consolidation

Appendix B. Industry Consortia Case Studies

Industry consortia have a demonstrated and successful record in developing the U.S. standards system. When it comes to national priorities, however, the private sector should not develop such standards without the active engagement of the Federal Government because of the need "to accelerate standards development and implementation to help spur technological advances and broaden technology adoption."[1] Recently, the U.S. Chief Technology Officer, Deputy U.S. Trade Representative, and Administrator, Office of Information and Regulatory Affairs of the Office of Management and Budget, issued a memorandum to the Heads of Executive Departments and Agencies on federal engagements in standards activities. Two of its five fundamental strategic objectives are:

- "Achieve cost-efficient, timely, and effective solutions to legitimate regulatory, procurement, and policy objectives;" and
- "Promote standards and standardization systems that promote and sustain innovation and competition[.]"[2]

These strategic objectives underscore the Department of Defense's ongoing efficiency initiatives and would help to alleviate the software vendor lock-in currently being experienced by the various the ERP system implementations.

A. Case Study: Utility Industry

Over the past five years, the utility industry underwent a large effort to bring its disparate and stove-piped set of communities together for the purpose of addressing supply chain concerns, and cyber security concerns and incidents. Even though the utilities—gas, electric, and water—all have their own set of value streams and operational business goals, there was baseline recognition that similar types of technologies, vendors, and channels were being used by each of the utilities as they transitioned into a Transmission Control Protocol/Internet Protocol (TCP/IP) based infrastructure for its operations. During this timeframe, various utility industry groups worked on understanding where their individual value streams in their business architectures intersect and the relationship between each other for the development of a trust agreement. The trust agreement determined what information would be valuable for exchange and the value and

[1] Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, *Principles for Federal Engagement in Standards Activities to Address National Policies,* M-12-08, 1, January 17, 2012, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08.pdf.

[2] Ibid., 3.

priority of that information. A common vocabulary also was developed with a standard structure to enable a method and means of communication among them. This common vocabulary was leveraged as a foundation for a Smart Grid Maturity Model (through the sponsorship of the Department of Energy), which is used by electric utilities to assess their current state of smart grid implementation, define their goals, and generate inputs into their planning and implementation processes. This utility industry effort for defining common vocabulary also added value to the National Institute of Standards and Technology's effort to bring standards into the smart grid for better information sharing.

B. Case Study: Auto Industry

In the early to mid-1990s, the U.S. automotive industry was struggling to keep up with the process innovations—Just-In-Time (JIT) production, Kanban system, and Lean manufacturing—developed and embraced by the Japanese auto manufacturers. Driven by the Big Three—General Motors, Chrysler, and Ford—the U.S. automotive industry came to the realization that in order to improve reliability and reduce costs a number of things needed to change. One core activity included the delivery of a more efficient supply chain order management system in which all layers of the automotive supply chain needed to participate. At the time, electronic data interchange (EDI) was the preferred method of electronic transaction management for order management, shipping, receiving, accounts payable, receivables, etc. recordkeeping. A consortium was formed that developed value streams and a supply chain for the U.S. auto industry. Additionally, trust was determined among players in the consortium to be a common goal in fighting a common enemy—the Japanese automotive industry. With the Big Three as the driving force, the consortium took it upon itself to establish a common vocabulary in order to establish transaction process standardization in the complex and nested supply chain. The common vocabulary allowed for a standards-based transactional structure that could be used by the end-to-end supply chain. Eventually the technology evolved out of EDI but the business architecture and the process of retaining a common vocabulary enabled the U.S. auto manufacturers to integrate into a standard infrastructure—improving the quality and efficiency of the supply chain that ultimately lead to cost management. This common vocabulary eventually allowed Japanese and European manufacturers to also integrate into this standard infrastructure.

Appendix C. Acronyms

ACAT	Acquisition Category
AESIP	Army Enterprise Systems Integration Program
APIs	application programming interfaces
ASP	application service provider
BEA	Business Enterprise Architecture
BI	business intelligence
BPEL	Business Process Execution Language
BPM	Business Process Modeling/Management
BPMN	Business Process Modeling/Management Notation
BSIT Strategy	Army Business Systems Information Technology Strategy 2011
BYOD	bring your own device
COI	community of interest
COOP	continuity of operations
COTS	commercial-off-the-shelf
CRM	customer relationship management
DaaS	Data as a service
DEAMS	Defense Enterprise Accounting and Management System
DoD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
EBS	Enterprise Business System
ESB	enterprise service bus
ECSS	Expeditionary Combat Support System
EDI	Electronic data interchange
ERP	Enterprise Resource Planning
FASAB	Federal Accounting Standards Advisory Board
FIAR Plan	Financial Improvement and Audit Readiness Plan
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
FY	fiscal year
GB	gigabyte
GCSS-Air Force	Global Combat Support System-Air Force
GCSS-Army	Global Combat Support System-Army
GCSS-MC	Global Combat Support System-Marine Corps
GFEBS	General Fund Enterprise Business System
GPRA	Government Performance and Results Act of 1993
GSA	General Services Administration
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a service
ID	identification
IDA	Institute for Defense Analyses

ISO	International Organization for Standardization
IT	information technology
JIT	Just-In-Time (production)
LMP	Logistics Modernization Program
MOA	memorandum of agreement
MILDEPS	Military Departments
Navy ERP	Navy Enterprise Resource Planning Program
Navy SYSCOMS	Navy System Commands
NAVAIR	Naval Air Systems Command
NAVSEA	Naval Sea Systems Command
NAVSUP	Naval Supply Systems Command
NIST	National Institute of Standards and Technology
OMG	Object Management Group
PaaS	Platform as a service
RDBMS	relational database management system
RDF	Resource Description Framework
RIF	Rules Interchange Format
ROI	return on investment
S&T	science and technology
SaaS	Software as a Service
SFIS	Standard Financial Information Structure
SFTP	Secure File Transfer Protocol
SI	system integrator
SLA	service level agreement
STANFINS	Standard Finance System
SOA	service-oriented architecture
SOMARDS	Standard Operations and Maintenance Army Research and Development System
SPAWAR	Space and Naval Warfare Systems Command
TCO	total cost of ownership
TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP)
U.S.	United States
USD(AT&L)	Under Secretary of Defense (Acquisition, Technology and Logistics)
USD(C)	Under Secretary of Defense (Comptroller)
VOC	voice of the customer
W3C	World Wide Web Consortium
WCF	Working Capital Fund
XaaS	Everything as a service
XMI	XML Metadata Interchange

Appendix D. References

Army Chief Information Officer/G-6, *America's Army: Powered by a Networked Force*, http://ciog6.army.mil/EnterpriseNetworkUpdate/tabid/100/Default.aspx.

Business Transformation Agency, "Lesson 1 – Background and Challenge," *Service Oriented Architecture (SOA)*, Slide 8 ("BMA Transformation Principles – Platoon Sized/NOT Battalion Sized") last visited on January 18, 2012, http://www.bta.mil/products/training/SOA/index.html.

Business Transformation Agency, *Standard Financial Information Structure*, http://www.bta.mil/products/sfis.html.

CV-2 Capability Taxonomy (Business Capability),BEA Version 7.0, http://www.bta.mil/products/bea_7_0/BEA/iwp/bealist_businesscapability_na.htm

CV-2 Capability Taxonomy (Business Capability), BEA Version 8.0, http://www.bta.mil/products/BEA_8_0/index.htm.

Carr, Nicholas, *Does It Matter? Information Technology and the Corrosion of Competitive Advantage*, Boston, Mass.: Harvard Business School Publishing Corp., 2004.

Carter, Ashton B., USD(AT&L), *Implementation Directive for Better Buying Power—Obtaining Greater Efficiency and Productivity in Defense Spending*, Memorandum, November 3, 2010, http://www.ndia.org/Advocacy/Resources/Documents/LegislativeAlerts/Implementation_Directive_6Nov2010.pdf.

Carter, Ashton B., USD(AT&L), *Better Buying Power: Guidance for Obtaining Greater Efficiency and Productivity in Defense Spending,* Memorandum, September 14, 2010, 3, http://www.acq.osd.mil/docs/USD_ATL_Guidance_Memo_September_14_2010_FINAL.PDF

Chief Financial Officers Act of 1990, Public Law 101-576, Title II, November 15, 1990.

Clinger-Cohen Act (formerly the Information Technology Management Reform Act of 1996), National Defense Authorization Act, Division E, Public Law 104-106, February 10, 1996 .

CRM Magazine, *What is CRM*, Destination CRM.com, February 19, 2010, http://www.destinationcrm.com/Articles/CRM-News/Daily-News/What-Is-CRM-46033.aspx.

Defense Science Board, *Department of Defense Policies and Procedures for the Acquisition of Information Technology,* Report, March 2009, 1, http://www.acq.osd.mil/dsb/reports/ADA498375.pdf.

Defense Science Board, *Final Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for Acquisition of Information Technology*, March 2009, 67, http://www.acq.osd.mil/dsb/reports/ADA498375.pdf.

Department of Defense, *Final Report on Defense Business Operations to the Congressional Defense Committees*, March 15, 2009, http://dcmo.defense.gov/documents/March_2009_Congressional_Report%20.pdf.

Department of the Army, Office of Business Transformation, *Army Business Systems Information Technology Strategy 2011*, February 14, 2011, 8, http://www.armyobt.army.mil/downloads/sec-army-approved-bsit-strategy_final.pdf.

Deputy Secretary of Defense, *Department of Defense Reform Initiative Directive #46—Paperless Contracting,* December 9, 1998, http://www.defense.gov/dodreform/drids/drid46.html.

Deputy Secretary of Defense, *Department of Defense Reform Initiative Directive #47— End-to-End Procurement Process,* December 9, 1998, http://www.defense.gov/dodreform/drids/drid47.html.

DITPR data extracted on January 10, 2012.

FASAB, "Statement of Federal Financial Accounting Standards 6: Accounting for Property, Plant, and Equipment," *FASAB Handbook*, Version 10, June 2011, page 16, Footnote 27, http://www.fasab.gov/pdffiles/2011_fasab_handbook.pdf

FASAB, "Statement of Federal Financial Accounting Standards 10: Accounting for Internal Use Software," *FASAB Handbook*, Version 10, June 2011, page 2, http://www.fasab.gov/pdffiles/2011_fasab_handbook.pdf

Fielding, Roy T. and Richard N. Taylor, *Principled Design of the Modern Web Architecture* (22nd International Conference on Software Engineering 2000, Limerick, Ireland, June 9, 2000), 407, http://dl.acm.org/citation.cfm?doid=337180.

GAO, *Defense Management: Challenges Facing DOD in Implementing Defense Reform Initiatives*, (Testimony, Statement of David R. Warren, Director, Defense Management Issues, National Security and International Affairs Division, GAO/T-NSIAD/AIMD-98-122), March 13, 1998, http://www.gao.gov/assets/110/107264.pdf.

GAO, *DOD Business Systems Modernization: Billions Continue to Be Invested with Inadequate Management Oversight and Accountability* (GAO-04-615), May, 2004, 14, http://www.gao.gov/assets/250/242540.pdf

GAO, *DoD Financial Management: Reported Status of Department of Defense's Enterprise Resource Planning Systems* (GAO-12-565R), March 30, 2012, Enclosure III, http://www.gao.gov/assets/590/589796.pdf.

General Fund Enterprise Business System (GFEBS), http://www.gfebs.army.mil.

Goodson, John, *Data Virtualization Provides a Single View Into the Enterprise*, Data At Your Service blog, March 1, 2010, http://www.ebizq.net/blogs/dataservice/2010/03/data-virtualization-provides-a-single-view-into-the-enterprise.php.

Government Performance and Results Act (GPRA) of 1993, Public Law 103-62, August 3, 1993.

GPRA Modernization Act of 2010, Public Law 111-352, January 4, 2011.

GSA, News Release, "GSA Becomes First Federal Agency to Move Email to the Cloud Agencywide," (GSA # 10694) December 1, 2010, http://www.gsa.gov/portal/content/208417.

Hearing of the Military Readiness Subcommittee of the House National Security Committee, SUBJECT: FY 1999 Infrastructure Reduction and Military Readiness, 2212 Rayburn Building, Washington, DC, March 13, 1998, http://commdocs.house.gov/committees/security/has065030.000/has065030_3.HTM.

Heckman, Jory, *Kundra seeks broader vendor pool*, Federal News Radio, August 3, 2011, http://www.federalnewsradio.com/ nid=&sid=2460112.

Interface Details and Status (Interfaces v1.xlsx), document provided to IDA by the DEAMS Functional Management Office on June 21, 2011.

"Jevons Paradox," Webster's Online Dictionary, last visited on January 5, 2012, http://www.websters-online-dictionary.org/definitions/Jevons.

Johnson, Martha, *"GSA Is In The Cloud,"* The GSA Blog, July 26, 2011, http://gsablogs.gsa.gov/gsablog/2011/07/26/gsa-is-in-the-cloud/.

Jones, Capers and Olivier Bonsignour, *The Economics of Software Quality*, Boston, MA: Pearson Education Inc., 2011, 39 & 444.

Kundra, Vivek, *"Tight Budget? Look to the 'Cloud," New York Times*, Aug. 30, 2011, http://www.nytimes.com/2011/08/31/opinion/tight-budget-look-to-the-cloud.html?_r=1.

National Defense Authorization Act for Fiscal Year 2002, Public Law 107-107, Sections 1008-1009, December 28, 2001.

National Defense Authorization Act for Fiscal Year 2012, Sec. 901. REVISION OF DEFENSE BUSINESS SYSTEMS REQUIREMENTS. Public Law 112-81, December 31, 2011.

Navy ERP Program, "USD(AT&L) Signs Full Deployment Decision (FDD) Acquisition Decision for Navy ERP," News and Releases, July 11, 2011, http://www.erp.navy.mil/news_and_releases/news38.html.

Navy ERP Program, History, http://www.erp.navy.mil/history.html.

Navy ERP Program, Navy ERP Passes Release 1.1 Cycle 2 Test Readiness Review, http://www.erp.navy.mil/news_and_releases/news36.html.

NIST, U.S. Department of Commerce, *"The NIST Definition of Cloud Computing,"* Special Publication 800-145, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, *"Principles for Federal Engagement in Standards Activities to Address National Policies,"* M-12-08, 1, January 17, 2012, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08.pdf.

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, "FIAR Plan Overview," *Financial Improvement and Audit Readiness Website*, last visited on January 12, 2011, http://comptroller.defense.gov/fiar/overview.html.

Office of the USD(Comptroller)/CIO, *Financial Improvement and Audit Readiness (FIAR) Plan Status Report*, November 2011, IV-1, http://comptroller.defense.gov/fiar/documents/FIAR_Plan_November_2011.pdf.

Oracle, *Overview of Oracle Federal On Demand: Hosting and Infrastructure Support Services for Agencies of the U.S. Government*, version 2.0, July 2010, 3 (white paper provided to IDA by Oracle).

Oracle, "PL/SQL FAQ," *Oracle FAQ's*, last visited on January 12, 2012, http://www.orafaq.com/wiki/PL/SQL_FAQ.

Schmidt, Steve, Chief Information Security Officer, Amazon Web Services (AWS), interview with IDA on November 23, 2010. Additional information about AWS is available at http://aws.amazon.com/.

Shaul, Chris, "Top 10 ERP Solutions," *ERP Selection Help*, May 30, 2011, http://erpselectionhelp.com/top-10-erp-solutions/.

Singh, Anoop, et al., *Guide to Secure Web Services: Recommendations of the National Institute of Standards and Technology*, NIST, Special Publication 800-9, August 2007, C-4, C-5, http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf.

Slabodkin, Greg, "DISA makes headway on key enterprise initiatives," *Defense Systems*, December 5, 2011, http://defensesystems.com/articles/2011/12/13/cover-story-disa-enterprise-initiatives.aspx.

TechTarget, "RAID," last visited on January 4, 2011, http://searchstorage.techtarget.com/definition/RAID.

Under Secretary of Defense (Comptroller), *Management Reform Memorandum #2—Moving to a Paper-free Contracting Process by January 1, 2000*, Memorandum, May 21, 1997, http://www.defense.gov/dodreform/mrms/mrm2.html.

Under Secretary of Defense (Comptroller), *Standard Financial Information Structure (SFIS) Implementation Policy*, Memorandum, August 4, 2005, http://dcmo.defense.gov/products-and-services/standard-financial-information-structure/SFIS/SFIS_Policy_Memorandum.pdf.

Wardley, Simon, *"Cloud Computing—Why It Matters,"* presentation at O'Reilly OSCON (Open Source Convention 2009," July 23, 2009, http://www.youtube.com/watch?v=okqLxzWS5R4.

Wardley, Simon, *"Future Costs and Cloud," Bits or pieces?*, blog post, December 7, 2011, http://blog.gardeviance.org/.

Wardley, Simon, *"Here comes the farmer...," Bits or pieces?*, blog post, April 19, 2008, http://blog.gardeviance.org/2008/04/here-comes-farmer.html.

Yasin, Rutrell, "All of GSA's e-mail now in Google Cloud," *Government Computer News*, July 26, 2011, http://gcn.com/articles/2011/07/26/gsa-email-google-apps-cloud.aspx?sc_lang=en.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-02-2012	Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Beyond Enterprise Resource Planning (ERP): The Next Generation Enterprise Resource Planning Environment	DASW01-04-C-0003
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Laura A. Odell Brendan T. Farrar-Foley John R. Kinkel Rama S. Moorthy Jennifer A. Schultz	5e. TASK NUMBER AO-5-3446
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	IDA Paper P-4852 H 12-000323

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
OSD(AT&L) 3020 Defense Pentagon, room C3949A Washington, DC 20301-3020	OSD(AT&L)
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT.

Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

Project Leader: Laura A. Odell

14. ABSTRACT

The Department of Defense (DoD) has invested billions of dollars in business enterprise resource planning (ERP) systems. However, they are not meeting schedules, cost, or performance expectations. Senior Defense leaders are increasingly aware that the economic environment demands the DoD move from "defense readiness at any cost" to "defense readiness at the best value." The Institute for Defense Analyses (IDA) reviewed the ERP systems to: (1) identify the best way to leverage current DoD systems that are meeting objectives (2) explore potential alternatives or add-ons to ERPs (e.g., Business Process Modeling/Management (BPM) solutions, Software as a Service (SaaS)). Situational agility, or predicting how future pipeline technologies and analytic techniques may improve on or replace current methods, must be an enabler of innovation, not a compliance enforcer, to fulfill needed capabilities. ERPs must provide a jumping-off point for integrating other beneficial technologies in the portfolio (e.g., cloud computing, mobile applications, and business intelligence).

15. SUBJECT TERMS

Enterprise Resource System (ERP), Situational Agility, Software As A Service (SaaS), Information Technology (IT), Business Process Modeling/Management (BPM)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
Unclassified					Dr. Nancy L. Spruill
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include Area Code)
Unclassified	Unclassified	Unclassified	Unlimited	122	(703) 695-4060