

Logistics Outsourcing and the Future War Fighting Environment: Risk and Control

Advance Management Program

June 29, 2001



***Tench Francis
School of Business***

Team 4

**Bob Bestercy
Karen Collier
Jack Davidson
Steve Lee
Glenn Robillard
Dave Smith**

Introduction

The purpose of this paper is to explore issues of risk and control associated with current logistics “outsourcing” initiatives as part of the Navy’s business strategy for reducing costs and promoting efficiency. The critical issue to examine is the impact of these initiatives on future operational plans. Discussion will be limited to several Department of the Navy logistics initiatives, although these ideas could easily be extended to other areas within the Department of Defense. Examples of outsourcing initiatives to be explored include Direct Vendor Delivery (DVD), Performance Based Logistics (PBL), Competitive Sourcing and full Contractor Logistics Support (CLS). The paper addresses how changes in environment lead to revised strategies and in turn, changes in logistics plans. More specifically, it addresses risks that arise from these changes, and how logisticians can assess and mitigate these risks.

Strategy and the Environment

Development of any successful long-term business strategy must consider many factors. Two of the most important factors are the environment and the customer. For the military logistics provider, the national military strategy provides a planning framework for the near term security environment. Other documents, like the Chairman of Joint Chiefs of Staff’s *Joint Vision 2020* provide an extended outlook. The customer affected by these business strategies is the warfighter. Operationally, as the environment evolves, the warfighter changes and adapts to it, in turn revising strategies for a force capable of meeting the expected future environment. These revisions provide significant challenges for maintaining a successful long-term business strategy that is responsive to strategic changes. During periods of relatively rapid change in the security environment, military logisticians risk developing business strategies that may fall short of customer’s expectations, or warfighter’s requirements.

A Period of Change: Understanding the Environment and Customer of Tomorrow

The end of the Cold War marked the most significant change in the national security environment in the last fifty years. During the Cold War our enemies were known and the operational environment was predictable and quantifiable. Military strategy was based on size and overwhelming force. Strategic risk was very high. This drove logistic support concepts that

were based on large investments in organic support structures, mitigating risk by providing nearly absolute control of the logistics pipeline. Naval forces operated with large shipboard stocks supplemented by a large organic support network, including forward support ships, global support bases, dedicated transportation channels, and large retail and wholesale supply stocks. Government owned and managed inventories and maintenance activities not only provided a high level of operational readiness, they also provided a significant surge capability. Logistics support of the period can best be characterized as one of providing high readiness at any cost.

The 1990's were a period of significant transition in the security environment, resulting in a revised national military strategy that focused less on high risk Cold War adversaries, and more on low risk small scale conflicts, interventions, and operations other than war. These changes led to reduced budgets and force structure. Fueled by successes in private industry, reengineering and "best business practices" were instituted throughout the armed forces. Logistics was viewed as an area ripe for cost savings. Inventory reductions, acquisition reform, and outsourcing were enacted in the name of efficiency.

As we enter the next millennium, strategists now question what the security environment of the next decade will bring. Although no one can accurately predict the future, national security strategists believe the environment will be one of increased strategic risk. New regional powers will rise, threatening global stability. Terrorism and weapons of mass destruction (WMD) will threaten national interest at home and abroad. Rogue nations will continue to disrupt stability in fragile regions. Although the adversaries of tomorrow will most likely be smaller than those of the past, they will also be much less predictable. Forces must be lighter, more mobile, yet more lethal. Information superiority and near perfect knowledge will replace the need for size and overwhelming force. Precision strike and effects based operations will supplant the need for large land based operations. Enemy theater ballistic missile, WMD and other asymmetric threats will present formidable access denial challenges. Force protection will be paramount. Although predicting just how logistics support will differ with any certainty is impossible, the *JV 2020* operational concept of *Focused Logistics* provides a clear conceptual framework. The implications of *Focused Logistics* for the Navy are significant and far-reaching. No longer will the Navy be able to rely on a large logistics footprint and an expensive network of support activities. Future logistics systems must be cheaper yet more responsive, and rely more on contractors as primary providers. Information technology will be the primary enabler.

Because future logistic support systems will operate on close margins, operational risk will be high. The Navy’s current outsourcing initiatives must be evaluated against this framework to determine if business efficiencies translate into effective logistics support concepts.

Outsourcing: Trading Efficiency for Risk

Navy logistics outsourcing as a means to business efficiency is rapidly expanding in the areas of spare parts, support activities, repair facilities, and engineering services. Today, many weapons systems are almost entirely contractor-supported, and total contractor logistics support is being considered for the next class of Amphibious Support Ship. The change in support philosophy has a basic guiding principle: better logistics performance at a reduced cost to the government. Table 1 delineates differences between traditional and future logistics support methods, and their relative levels of cost and risk. For example, cost decreases as a contractor provides spare parts at a cheaper price, but risk increases as the Navy relinquishes inventory control decisions. Conversely, if we outsource support functions, such as clerical or administrative services, costs savings can be obtained at very low risk, as these functions are generally not considered critical to the national defense. In general, risk is higher in areas of support that directly impact the war fighter’s ability to perform their mission, and risk is lower for indirect support functions. The following paragraphs outline in more detail the changes to Navy logistics support delineated in Table 1.

Table 1

Function	Traditional Methods	Risk / Cost	Future Methods	Risk / Cost
Spare Parts	Navy, DLA Depots	Low/High	DVD/PBL- Contractor owned inventories	Moderate/Moderate
Repair of Components	Navy Organic Depot Repair	Low/High	Outsourcing	Moderate/Moderate
Support Functions	Civil Service/Military	Low/High	Outsource to private sector	Low/Low
Engineering Services	Navy Engineering Agency	Low/High	OEM/Contractor Engineering	Moderate/Moderate
Platform Logistics	Navy Program Management Office	Low/High	Total Contractor Support	High/Moderate

Spare Parts Support: Traditionally, spare parts have been procured by the Navy to stock and issue from DoD owned warehouses. To achieve efficiency, the Navy is increasingly entering into long-term contractual arrangements with distributors and original equipment manufacturers (OEMs) to push inventories to contractor owned-contractor operated facilities. The result is

reduced cost as the Navy reduces infrastructure, but increased risk in that the Navy relies on contractors to meet spare parts requirements. In the future environment, this can lead to increased operational risk if contractors are not able to deliver parts when and where they are needed.

Repair of Components: Outsourcing repair of equipment components and end items to OEMs and contractor operated facilities is on the rise, as the Navy looks to industry to provide repair capability at a cheaper price. In some cases this is accomplished through long-term agreements; in others, entire functions are outsourced as a result of competitive sourcing. Increased risk is due to potential loss of repair capability if a contractor defaults, and loss of organic repair skills over the long term. In the future, this loss of capability can be compounded by the potential denial of contractors into the battle space to perform mission critical repairs.

Support Functions: As the Navy looks to reduce end strength, more activities are contracting for support functions such as clerical services and administrative support. Costs are reduced, and risk remains low, as these functions generally are not considered critical to operational readiness.

Engineering Services: Similar to spare parts support and repair of components, the Navy is exploring relationships in which OEMs provide engineering design services, configuration control, technical assist visits and more. Risk increases as the Navy loses organic engineering skills over the long term and becomes more reliant on the private sector.

Platform Logistics: Planning for the logistics support of the LPD 17 Class includes options that all logistics support will be provided by the private sector. This includes not only all of the above listed functions, but additionally, all maintenance, warranty support, configuration control, modifications and upgrade will be provided by contractors. Risk is considerably higher than if these functions were performed by the Navy, as contractor default or access denial could result in a total loss of logistics support to the warfighter.

The above paragraphs illustrate that the more complex the tasks are that we delegate to the private sector, the greater the risk of failure of logistics support. How can we systematically

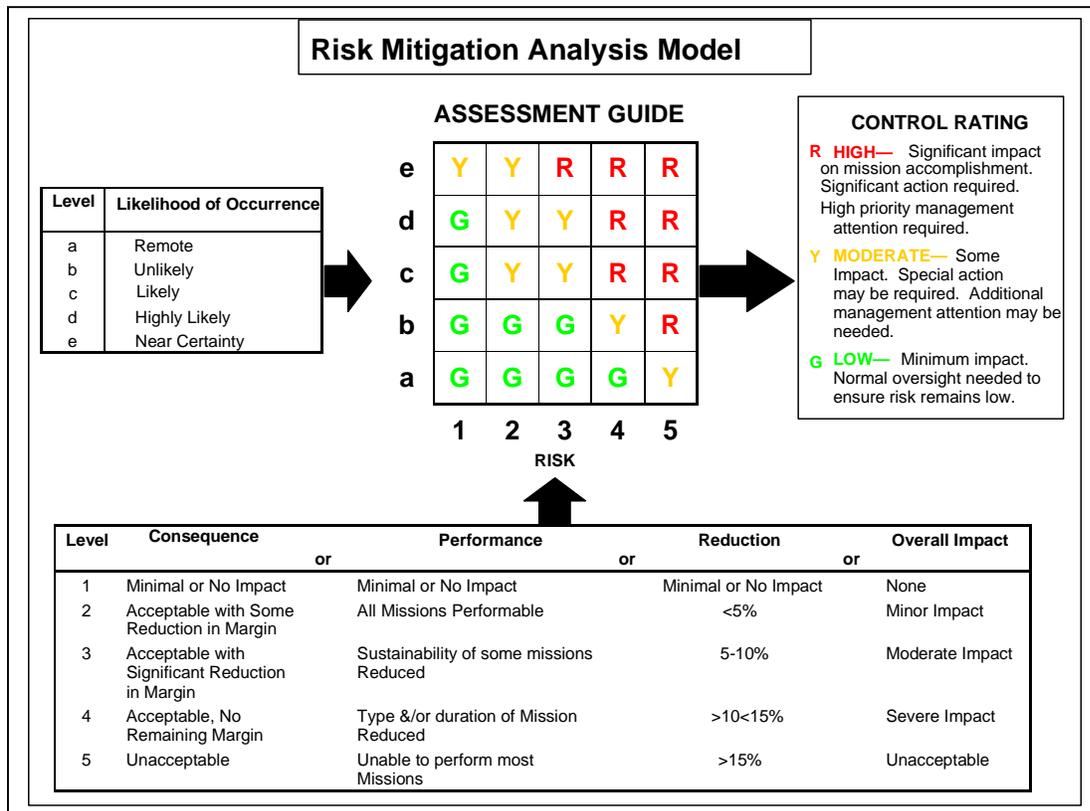
assess the level of risk involved, and in turn identify appropriate levels of management control? The next section presents one possible tool that can be used to assess a system to determine an appropriate level of control, given a corresponding level of operational risk.

Risks and Controls: A Basic Model

A basic tenet of management is that risks can be mitigated by controls. The greater the risk, the more stringent controls must be to avoid system failure. This section develops this simple concept and applies it to real life, understanding the risks of outsourcing logistics, and exploring the controls the Navy uses to mitigate those risks.

Defense Acquisition utilizes general Critical Process Risk Assessment (CPRA) models to assess contractor and process risks. Figure 1 suggests a similar model for assessing levels of logistics risk and management controls as they relate to operational readiness. This model can be a useful tool for planners to develop controls that can mitigate risks of logistics failure, and failure to support operational plans.

Figure 1



Applying the Model

The best way to demonstrate how the model can be applied is through an illustrative example. Suppose the Navy is considering outsourcing total logistics support for a critical component of the Aegis weapon system because of potential costs savings. Working closely with operators, the potential operational risk to the Navy is assessed (Level 1-5) and the likelihood that the systems would be employed in a future environment is determined (Level a-e). It is imperative that as outsourcing contracts are being developed, the customer (warfighter) plays a role in determining both the level of risk and the appropriate controls to be incorporated into the contract. Together, the two inputs, risk and likelihood, determine an appropriate control rating. In our case, the likely risk is high (5) and likely employment is certain (e), would result in a corresponding control rating of high (R). Consequently, either the potential outsourcing action is not recommended, or if the risk is acceptable, given the potential cost savings, appropriate management controls must be instituted. In this case controls might include in-house Defense Contract Management Agency (DCMA) oversight, tailored contract clauses, special warranty provisions, and other performance and inspection criteria. Table 2 provides additional examples to illustrate how controls could be utilized for each level of risk.

Table 2

Control Rating	Potential Management Control Actions
Low	No special provisions; standard contract requirements
Moderate	Potential outsource restrictions; surge provisions, performance incentives, product reliability incentives, product improvement incentives
High	Limited outsourcing; significant contract management control with increased Government oversight, validation, coordination, test/evaluation acceptance; in-plant DCMA presence.

Conclusion

Recognizing a changing environment and responding effectively is a challenge for any organization, but particularly challenging for a complex global system that the National Military Strategy attempts to predict and plan for. Further, as we develop business strategies to support changing military strategies, we must pay close attention to how business decisions effect the larger assumptions made in current and future war planning documents. If our business

strategies are causing increased risk of failure to meet the logistics needs of the warfighter, it follows that more stringent management controls must be levied to reduce the risk of failure.

The impact of decisions about logistics support on current and future war planning assumptions must be considered systematically. Using a model to assess risk and identify appropriate controls is one way to mitigate increased risk of failure. War planners must be able to carefully analyze assumptions that are made about organic logistics capabilities, and consider the overall impact business efficiencies may have. The model presented here can provide planners a useful tool in developing controls that are appropriate for an identified level of risk.