This product is part of the RAND Corporation documented briefing series. RAND documented briefings are based on research briefed to a client, sponsor, or targeted audience and provide additional information on a specific topic. Although documented briefings have been peer reviewed, they are not expected to be comprehensive and may present preliminary findings.
DOCUMENTED BRIEFING

Identifying and Managing Air Force Sustainment Supply Chain Risks

Nancy Y. Moore • Elvira N. Loredo
Identifying and Managing Air Force Sustainment Supply Chain Risks

Nancy Y. Moore • Elvira N. Loredo

Prepared for the United States Air Force
Approved for public release; distribution unlimited
The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND’s publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

© Copyright 2013 RAND Corporation

Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Copies may not be duplicated for commercial purposes. Unauthorized posting of RAND documents to a non-RAND website is prohibited. RAND documents are protected under copyright law. For information on reprint and linking permissions, please visit the RAND permissions page (http://www.rand.org/publications/permissions.html).

Published 2013 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Library of Congress Control Number: 2013941129
ISBN: 978-0-8330-7655-7
Preface

In recent years, the Air Force and, particularly, its suppliers have pursued various means to improve performance, reduce costs, and otherwise adopt best industry practices. Such practices include outsourcing, global sourcing, supply-base rationalization, single sourcing, just-in-time deliveries, and lean inventories. While these practices offer many benefits in efficiency and effectiveness, they can also make supply chains more brittle and increase risks of supply disruptions.

This work examines supply chain risk management, including evolving commercial and Air Force practices. It was part of a project on “Identifying and Managing Risks Associated with Agile Supply Chains,” conducted in RAND Project AIR FORCE’s Resource Management Program and sponsored by the Air Force Deputy Chief of Staff for Logistics, Installations, and Mission Support. Since this research was completed, the Air Force proposed a reorganization of Air Force Materiel Command. The new structure took effect in October 2012 and established an Air Force Life Cycle Management Center (AFLCMC) and an Air Force Sustainment Center (AFSC). The AFLCMC consolidates product development and support system design. The AFSC integrates depot maintenance and Air Force supply chain activities. The findings and recommendations presented in this report are relevant to how the Air Force will identify and manage supply chain risk under the new organizational structure.

This report should be of interest to those purchasing and providing goods and services to the Air Force.

RAND Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the U.S. Air Force’s federally funded research and development center for studies and analyses. PAF provides the Air Force with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. Research is conducted in four programs: Force Modernization and Employment; Manpower, Personnel, and Training; Resource Management; and Strategy and Doctrine.

Additional information about PAF is available on our website:
http://www.rand.org/paf/
In recent years, the Air Force and, particularly, its suppliers have pursued various means to improve performance, reduce costs, and otherwise adopt best industry practices. Such practices include outsourcing, global sourcing, supply-base rationalization, single sourcing, just-in-time deliveries, and lean inventories.

While these practices offer many benefits in efficiency and effectiveness, they can also make supply chains more brittle and increase risks of supply disruption. For example, having fewer sources of supply means a disruption at any one of them is more likely to affect overall performance. Similarly, just-in-time deliveries and lean inventories mean fewer days of operating capacity should a supply disruption halt deliveries of raw materials or components.

To help the Air Force better identify and manage supply chain risks, the Deputy Chief of Staff for Logistics, Installations, and Mission Support asked RAND Project AIR FORCE to develop a strategy for managing supply chain risks during sustainment. The Air Force also requested a follow-on project focused on the manufacturing supply chain. This documented briefing focuses on the supply chain risks during sustainment. To do this, RAND researchers reviewed literature on supply chain risk management (SCRM) and interviewed Air Force personnel in the sustainment and acquisition communities and supply chain managers from commercial firms responsible for managing supply chain risks. The RAND team identified risks that are and are not being managed and developed recommendations for future risk management. We summarize below our key findings on prevailing practices, current Air Force and Department of Defense (DoD) guidance, and risks the Air Force may wish to address.

Supply Chain Risks Vary by Industry

There are many events that, if realized, could lead to a disruption of a company’s supply chain, such as earthquakes and floods; see Appendix E for a comprehensive list of supply chain risks. The significance of the risk varies by industry. For example, “supplier failure” and “strategic risk” were among the greatest reported concerns of “high-tech” and “aerospace and defense” firms.¹ Natural disasters and other singular events were of lesser concern. Nevertheless, recent events—such as the March 2011 earthquake, tsunami, and radiation leaks in Japan, which affected automotive and electronics supply chains throughout the globe, and Hurricanes Katrina and Rita in 2005, which disrupted petroleum production—have raised awareness of how disruptive and costly such events can be. In light of the unpredictability of such events,

¹ Examples of strategic risk include loss of manufacturing capacity or overreliance on one supplier.
some leading firms are recognizing the importance of responding quickly; while many events cannot be foreseen or avoided, their effect on the bottom line can be mitigated.

**Prevailing Practices in Supply Chain Risk Management**

We define supply chain risk as the effect of uncertainty at any point in the end-to-end supply chain on its objectives. The magnitude of supply chain risk may be measured along three dimensions: likelihood of occurrence, expected consequences, and duration. Risks of the highest likelihood, greatest consequence, and greatest duration would require first attention.

Traditional approaches to SCRM have included such strategies as multiple sources of supply, extensive competition, expediting, increased order quantities, development of inventory safety stocks, and well-stocked supply pipelines. Each of these strategies has its own risks. For instance, expediting orders, developing inventory safety stocks, and having a well-stocked supply pipeline can increase total costs. Qualifying and managing multiple sources of supply increases complexity. There are often limits on the number of capable suppliers, and the benefits of multiple supply sources can be outweighed by limited price leverage and increased variance in quality and delivery for the same good or service.

Even with the growing realization of supply chain vulnerability, few managers report they are well prepared for supply chain disruptions; SCRM is an emerging discipline.

**Emerging Best Practices in Supply Chain Risk Management**

We concluded from our company interviews and review of the literature that proactive SCRM requires the development of guidance and policies for identifying and managing supply chain risks. Some firms place less emphasis on calculating the probability of an event and more on reducing the response time to the realization of an event. That is, while one particular event may have a low probability of occurrence, if all the potential risks are examined as a whole, there is a good likelihood that one will occur; which one is not as important as having a strategy in place to detect and react. For example, Cisco Corporation lists four key elements in its SCRM program:

1. **Business Continuity Planning**, which works closely with internal and external partners “to document recovery plans and times and drive resiliency standards.”
2. **Crisis Management**, which is responsible for continuous global monitoring of and response to disruptions.
3. **Product Resiliency**, which helps Cisco’s business units address supply chain vulnerabilities during product design and to prioritize and reduce the costs of risk mitigation strategies.
4. **Supply Chain Resiliency**, which identifies points in the supply chain where time to recovery would be unacceptably high and develops resiliency plans for them.

Proactive SCRM also requires that an enterprise have a supply chain risk assessment and management process. Often supporting the process are tools for supply chain risk identifica-
tion, assessment, and monitoring. From a review of the relevant literature, we compiled a list of processes commonly involved in SCRM. We combine these into a proposed nine-step process:

Step 1: Recognize the existence of a potential risk.
Step 2: Identify the exposure of the supply base to the risk.
Step 3: Estimate the likelihood.
Step 4: Estimate the severity of realization of the risk.
Step 5: Prioritize risks by potential costs to allocate scarce resources appropriately.
Step 6: Develop, assess, and execute a risk management strategy for the prioritized list.
Step 7: Develop contingency plans.
Step 8: Monitor the risk environment to respond to changes and re-prioritize responses to risk.
Step 9: Continuously integrate lessons learned and improve risk and supplier management policies.

**Current Department of Defense and Air Force Guidance**

Several DoD and Air Force documents, including the *Defense Acquisition Handbook*, cite the need to deal with risk. However, risk identification and mitigation strategies in these documents primarily focus on the acquisition phase and risks in reference to cost, technical performance, or schedule of a weapon-system acquisition program. Altogether, DoD guidance identifies some, but not all, of the risks identified in the business literature.

The Air Force commodity councils have a process for managing risk, but it is geared toward managing contract risk, not supply chain risk.

One prominent category of supply chain risks identified in the business literature but not DoD guidance is natural disasters. The Federal Acquisition Regulation, through a force majeure clause, absolves suppliers of risks associated with natural disasters or with “acts of God or the public enemy.” This clause transfers these risks from many suppliers, especially those located in high-risk areas, to the Air Force. Force majeure clauses are also prevalent in commercial contracts and are necessary to ensure that suppliers are not unduly penalized for acts they cannot control. Awareness of the force majeure assignment of certain risks to the Air Force is critical to managing those risks.

**Interviews of Air Force Supply Management Personnel Reveal Gaps in Supply Chain Risk Management**

We interviewed a cross-section of representatives from organizations involved with managing suppliers or who are affected by supply chain disruptions during sustainment.

A questionnaire listing supply chain risks and asking how often they were considered was administered to each group. Commodity council members that we interviewed reported considering many of the same supply chain risks identified in DoD guidance. They often or always consider a relatively small number of risks, such as those related to supplier certification or qualification, demand uncertainty, overall quality, and technical competency. They consider about half the time such risks as long cycle times, poor training of supplier personnel,
and insufficient equipment and personnel at supplier facilities; risks resulting from uncertain demand and poor communications; and internal risks, such as poor forecasting and inadequate availability of resources. They rarely or never consider risks whose investigation would require investment in a supply chain risk assessment program or force majeure events for which the Federal Acquisition Regulation absolves suppliers. It may be logical for Air Force personnel not to consider these risks if they believe that the Federal Acquisition Regulation leaves them little leverage over suppliers regarding them. Nevertheless, the effects of such events could be catastrophic. Consequently, even if the Air Force cannot change the likelihood of a risk, it should take steps to minimize its consequence and duration.

We examined sustainment approaches for two Air Force weapon systems to determine when and how supply chain risks were managed. We found that the F-16 sustainment approach lacks a comprehensive process for SCRM, raising the question of whether organic weapon support more generally may lack an SCRM process. Boeing management of C-17 aircraft sustainment has some elements of SCRM based on corporate policies, but it is not clear whether these policies are meant to identify risks beyond those relating to financial, quality, or timeliness issues.

Implications

The results of this research suggest that many supply chain risks are not considered directly within the Air Force sustainment community and that, while others are acknowledged, there is little or no strategy in place to mitigate them. The primary recommendation from this research is that the Air Force establish an enterprise-level SCRM organization. This organization should oversee supply chain risk as part of supplier relationship management and should set policy on how to manage supply chain risk for both organic and contractor-managed sustainment, develop standard processes and metrics for risk management, expand the types of risk managed, develop tools for risk assessment, and establish metrics and incentives for mitigating risk. Commercial practices offer some guidance on this, but the Air Force will need to develop practices that reflect the Air Force’s unique requirements and organization. For example, one challenge for the Air Force is managing risk over the entire life cycle of the weapon system. The Air Force Materiel Command’s recent reorganization created an Air Force Life Cycle Management Center (AFLCMC) and an Air Force Sustainment Center (AFSC). This new structure consolidates product development and support system design under AFLCMC and integrates depot maintenance and Air Force supply chain activities under AFSC. Supply chain risk cuts across these areas. In this document, we do not explicitly address SCRM during acquisition, but we contend that many supply chain risks are common to acquisition and sustainment and are often shaped by decisions made during acquisition. At the time of this writing, the new structure is taking shape, but it is too early to determine how the Air Force intends to conduct SCRM or supplier relationship management. We recommend that the new organizational structure provide a mechanism to integrate supplier relationship management and SCRM across AFLCMC and AFSC.
We particularly thank Mr. Grover Dunn, then Director of Transformation, Deputy Chief of Staff for Logistics, Installations and Mission Support (AF/A4I), for supporting this project. We also wish to thank F-16 supply chain management personnel, Boeing personnel, Defense Logistics Agency personnel, and personnel at several leading companies for taking time from their busy schedules to answer our interview questions. We are grateful to the reviewers, Ellen Pint, Sarah Nowak, and Stanley Griffis, for their thoughtful comments. Lastly, we wish to thank Clifford Grammich for helping us revise this draft and Donna Mead and Jane Siegel for formatting it.
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFGLSC</td>
<td>Air Force Global Logistics Support Center</td>
</tr>
<tr>
<td>AFLCMC</td>
<td>Air Force Life Cycle Management Center</td>
</tr>
<tr>
<td>AFSC</td>
<td>Air Force Sustainment Center</td>
</tr>
<tr>
<td>ALC</td>
<td>air logistics center</td>
</tr>
<tr>
<td>CAMP</td>
<td>commodity acquisition management plan</td>
</tr>
<tr>
<td>CEO</td>
<td>chief executive officer</td>
</tr>
<tr>
<td>CFO</td>
<td>chief financial officer</td>
</tr>
<tr>
<td>CMP</td>
<td>commodity management plan</td>
</tr>
<tr>
<td>CVCM</td>
<td>customer value chain management</td>
</tr>
<tr>
<td>DCMA</td>
<td>Defense Contract Management Agency</td>
</tr>
<tr>
<td>DFARS</td>
<td>Defense Federal Acquisition Regulation Supplement</td>
</tr>
<tr>
<td>DLA</td>
<td>Defense Logistics Agency</td>
</tr>
<tr>
<td>DMS</td>
<td>Diminished Manufacturing Source</td>
</tr>
<tr>
<td>DMSMS</td>
<td>diminishing manufacturing sources and material shortages</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DoDI</td>
<td>Department of Defense Instruction</td>
</tr>
<tr>
<td>DSCR</td>
<td>Defense Supply Center, Richmond</td>
</tr>
<tr>
<td>FAR</td>
<td>Federal Acquisition Regulation</td>
</tr>
<tr>
<td>FY</td>
<td>fiscal year</td>
</tr>
<tr>
<td>GIG</td>
<td>Global Information Grid</td>
</tr>
<tr>
<td>GSM</td>
<td>Global Supplier Management</td>
</tr>
<tr>
<td>HSI</td>
<td>human systems integration</td>
</tr>
<tr>
<td>IPT</td>
<td>Integrated Process Team</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>LCL</td>
<td>life-cycle logistics</td>
</tr>
<tr>
<td>LGCC</td>
<td>Landing Gear Commodity Council</td>
</tr>
<tr>
<td>N/A</td>
<td>not applicable</td>
</tr>
<tr>
<td>OEM</td>
<td>original equipment manufacturer</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>OSS&amp;E</td>
<td>operational safety, suitability, or effectiveness</td>
</tr>
<tr>
<td>PAF</td>
<td>RAND Project AIR FORCE</td>
</tr>
<tr>
<td>PBL</td>
<td>performance-based logistics</td>
</tr>
<tr>
<td>SAF/AQ</td>
<td>Assistant Secretary of the Air Force (Acquisition)</td>
</tr>
<tr>
<td>SBU</td>
<td>strategic business unit</td>
</tr>
<tr>
<td>SCRM</td>
<td>supply chain risk management</td>
</tr>
<tr>
<td>T&amp;E</td>
<td>test and evaluation</td>
</tr>
</tbody>
</table>
In recent years, the Air Force and, particularly, its suppliers have pursued various means to improve performance, reduce costs, and otherwise adopt best industry practices. Such practices include outsourcing, global sourcing, supply-base rationalization, single sourcing, just-in-time deliveries, and lean inventories. Many new practices to improve the efficiency and effectiveness of supply chains are increasing their “brittleness” and, consequently, an enterprise’s exposure to supply disruptions (Griffin, 2008).

Such challenges increase the importance of securing supply; indeed, in the view of some analysts (e.g., Steele and Court, 1996), securing supply regardless of broader forces in the purchasing environment is the prime task for an effective purchasing organization. Risk management for such organizations consists of examining the entire supply chain for a good or service.

---

1 Many of these practices came into being in response to the theories of management experts, such as W. Edwards Deming, Joseph M. Juran, and Philip B. Crosby, and the success of Japanese manufacturers, such as Toyota, which put these theories into practice. For example, just-in-time manufacturing had great success in reducing the amount of work in progress on manufacturing lines and thereby reducing costs. However, this method depends on reliable supply and short lead times. Likewise, outsourcing and global sourcing were largely a reaction to comparatively lower costs of labor and materials available from outside the United States. These methods, while reducing some costs, extend transportation time and increase vulnerability to supply chain disruptions.
This should include both upstream to identify future supply problems and downstream to identify future distribution and customer problems.

Developing additional sources of supply can help reduce risks, but having them does not necessarily reduce supply chain vulnerabilities. Better options to reduce vulnerabilities may be available by working with existing suppliers, e.g., using dual sites to assure supply at one site should a disaster strike the other, or making sure suppliers have plans to address a wide variety of contingencies.

---

2 For example, to reduce single-source risk to its just-in-time processes, Honda of America requires dual capability (i.e., more than one production site) among its suppliers (Nelson, Mayo, and Moody, 1998). In addition, after temporarily shutting down all 12 of its Japanese plants because a key supplier’s plant (Riken Corp.), which produces $1.50 piston rings, was damaged by a 6.8-magnitude earthquake on July 16, 2007, Toyota president Katsuaki Watanabe said, “the company will examine its risk management and risk control and look for ways to become less dependent on single suppliers. [But it] won’t change its kanban, or just-in-time, strategy of keeping as little inventory as possible on hand, which reduces warehouse costs and ensures quality” (Chozick, 2007). For more on supply vulnerability and competitive advantage, see Sheffi, 2005; and Sheffi and Rice, 2005.
Motivation and Methodology

The supply chain challenges the Air Force faces are complicated by its changing missions, operations, and requirements for support. With the rise of smaller, regional conflicts and antiterrorist operations has come much more uncertainty regarding Air Force deployments, including their timing, location, and intensity. In response, the Air Force has developed plans and policies that require a very responsive, flexible, and resilient sustainment supply chain for its forces. Furthermore, the rising costs of sophisticated new technologies to counter new threats have driven up the real costs of weapons over time, reducing the numbers that the Air Force can acquire and increasing the consequences of supply chain disruptions.3

Fewer weapons and more deployments often lead to much lower densities of weapons at home stations and deployed. These lower densities, in turn, make cannibalization more costly and supply chains for weapon parts more important.4

---

3 For example, the Air Force initially sought to purchase nearly 650 F-22 aircraft to replace the F-15 and other aircraft. By 2009, however, Secretary of Defense Robert Gates, citing the need to shift from “big-ticket” items to programs for waging campaigns against terrorists and extremists in multiple regions, sought to cap the number of F-22 aircraft at 187 (“Gates Announces Major Pentagon Priority Shifts,” 2009). As he wrote in Foreign Affairs, weapons “have grown ever more baroque, have become costly, are taking longer to build, and are being fielded in ever dwindling quantities” (as quoted in Thompson, 2009).

4 Cannibalization is the removal of a currently functioning serviceable part from a weapon system that cannot currently perform its mission (because it is awaiting one or more parts or repair) and using it in an aircraft that needs the part to make it fully mission capable. The costs of cannibalization are twofold. First, cannibalization carries costs in lost aircraft owing to the possibility of collateral damage during the part removal and replacement process. Second, cannibalization requires additional maintenance man-hours to remove and then eventually replace the serviceable part.
The increasingly sophisticated technology and integration of Air Force weapon systems, coupled with outsourcing by original equipment manufacturers, further underscores the importance of the supply chain and reducing risks to it. Integrated weapon systems can complicate support because they require more sophisticated testing to ensure that all systems interfaces are properly functioning. For example, Deputy Secretary of Defense for Acquisition, Technology, and Logistics John Young said of the F-22, “The airplane is proving very expensive to operate, not seeing the mission-capable rates we expected, and it’s complex to maintain . . .” (as quoted in Thompson, 2009). In response to the estimated $1.5 trillion 55-year life cycle operating and support costs (Pocock, 2012), Vice Admiral David Venlet, the F-35 Program Executive Officer, is working with Lockheed Martin to reduce projected sustainment costs. Among other strategies, the Air Force is trying to balance performance-based logistics support provided by the original equipment manufacturer (OEM) with organic maintenance (Trimble, 2011); this underscores the complexity of the challenges and potential risks involved in the acquisition and sustainment of advanced weapon systems.

Projected reductions in defense spending, coupled with increasing costs of new weapons and personnel, are increasing pressure to reduce the physical size of and budgets for support infrastructure. This has included Office of Secretary of Defense policies for outsourcing the support of some old and many new weapons in so-called performance-based logistics (PBL) contracts “that optimize total system availability while minimizing cost and logistics footprint” (Defense Acquisition University, undated). Reducing the budget for support infrastructure is likely to lead to consolidation of suppliers and organic facilities as well as possibly more outsourcing. Consolidation reduces redundancies and means; if a disaster were to strike a consolidated site, the consequences would be greater.

---

5 Boeing’s experience with its “Dreamliner” 787 aircraft underscores the importance of some supply chain issues and risks in aircraft manufacturing. Its initial test voyage of the aircraft and subsequent delivery to customers were delayed by supply chain problems, specifically those in a shortage of fasteners (Holmes, 2007). Later, to gain greater control over its global supply chain, Boeing purchased a fuselage subassembly plant (“Boeing Acquires Stake in Plant,” 2009).

6 The F-22s currently in the inventory “are ready to fly only 62% of the time and haven’t met most of their performance goals” (Thompson, 2009). According to information from the Reliability and Maintainability Information System (REMIS) from fiscal year 2006 to 2010, F-22 mission capable rates have ranged between 61 and 63 percent.

7 Defense Secretary Gates, as quoted in Thompson, 2009, warned that “The spigot of defense spending that opened on 9/11 is closing.” Thompson further observes that “the military’s annual budget has finished growing, and the billions it once imagined it might spend on future weapons have evaporated. So cuts—and big ones—are coming.” In addition, the “average military service member is about 45 percent more expensive, after adjusting for inflation, in fiscal year [FY] 2009 than in FY98 . . .” (Daggert as quoted in Waterman, 2009). In January 2011, Secretary Gates announced $78 billion in budget cuts over five years. President Obama has proposed cuts of more than $400 billion by 2023 (Shanker and Drew, 2011).

8 PBL is the DoD-preferred approach for implementing product support. PBL is a strategy for weapon system product support that employs the purchase of support as an integrated performance package designed to bring higher levels of system readiness. PBL delineates outcome performance goals of weapon systems; ensures that responsibilities are assigned; and provides incentives for attaining those goals for the overall life-cycle management of system reliability, supportability, and total ownership cost. DoD Directive 5000.01, The Defense Acquisition System, provides policies that apply to all acquisition programs. According to the directive, program managers are required to develop and implement PBL strategies that optimize total system availability while minimizing cost and logistics footprint. The directive also requires that program managers become the single point of accountability for accomplishing program objectives for total life-cycle systems management, including sustainment. The Fiscal Year 2003–07 Defense Planning Guidance requires that each military department submit a plan that identifies its implementation schedule for applying PBL to all new weapon systems and all Acquisition Category I and II fielded systems (Office of the Inspector General, 2004).
Furthermore, Air Force customer expectations for responsiveness, resiliency, and cost effectiveness, based on their needs and experience in the commercial sector, are rising. Indeed, customer frustration with expensive, slow, and unreliable support had, in part, been driving policy to outsource more weapon system support to the private sector, particularly to OEMs through PBL contracts. More recently, the Air Force has retreated somewhat from outsourcing due to higher-than-expected costs of outsourced maintenance and repair as well as breaching of the “50/50 rule,” requiring that at least half of maintenance be performed at a public depot.

As we discuss, the total magnitude, or measure, of risk is a function of likelihood, consequence, and duration of an event. Uncertain deployment timing and destination, lower density of aircraft, and higher technological requirements, combined with pressures to make the support system more efficient and effective, can increase the likelihood, consequence, or duration of supply chain risks if they are not concurrently addressed. Such increased sustainment risks adversely impact the Air Force’s ability to respond quickly and to sustain agile operations.

---
9 “PBL strategies may be applied at the system, subsystem, or major assembly level depending upon program unique circumstances and appropriate business case analysis” (Wynne, 2004).
Over time, the Air Force has increasingly relied on contract rather than solely organic support for its weapon systems; an important implication is that the Air Force must work with external partners to make its supply chains resilient and responsive and to mitigate risk in them. The above table shows the evolution of Air Force weapon system maintenance support in recent and coming years. The top row lists major weapon systems by year of introduction. Each subsequent row in the table lists major support components (e.g., airframe, engines, landing gear) and support functions (i.e., engineering, supply chain management, distribution) for each system. The colors in each cell note the status of support.

This table shows the Air Force’s shift over time from organic-provided (i.e., internal) to contractor-provided (i.e., external) maintenance services. A significant amount of product support and depot maintenance is being performed through contracts on existing weapon systems, with more planned for future systems (Mulligan, 2007). While some elements of this strategy are being reviewed—for example, maintenance strategies for the C-17 and F-22 aircraft will use more organic support in coming years—it is unlikely that the Air Force will return, or even want to return, to 100 percent organic maintenance. Regardless of the contract strategy, both contractor and organic support have supply chain risks. What can vary are the types and dimensions of the risks as well as the access Air Force managers have to the information needed to adequately identify, assess, and manage them.
The Air Force asked RAND to help it develop an enterprise-wide strategy for proactively managing supply chain risks. Because supply chain risks span the life of a weapon system, we conducted the study in two phases: Phase one examined Air Force management of supply chain risks associated with sustainment of legacy or near-legacy systems (that is, those systems whose production has ended or will soon end), and phase two focused on managing supply chain risks during acquisition.

This document describes our findings for phase one on sustainment. Our goal for this phase was to identify those risks the Air Force is currently managing, those it is not currently managing, and those it should manage.
We began by reviewing the academic and business literature on supply chain risk management (SCRM). Because this is an emerging field, the literature is fairly recent and much less developed than literature on other risks or supply chain management generally. We also reviewed Air Force and Department of Defense (DoD) guidance regarding sustainment supply chain risk identification and management.

We developed, based on our reviews of the literature and policy guidance, interview protocols for Air Force and DoD personnel involved in supply chain, contracting, and commodity management (Appendix A) as well as for industry personnel involved in SCRM (Appendix B). We selected two weapon systems for case studies: the F-16, a legacy weapon system, which primarily has organic support and has transitioned from acquisition to sustainment, and the C-17, a newer system that is contractor-supported and is currently transitioning from acquisition to sustainment.

Because commodity councils are responsible for writing many sustainment contracts we also interviewed commodity council representatives at each air logistics center (ALC) regarding their management of supply chain risks. These included the Landing Gear Commodity Council at the Ogden Air Logistics Center, the Communications and Electronics Commodity Council at the Warner Robins Air Logistics Center, and the Propulsion, Instruments, and Accessories Commodity Council at the Oklahoma City Air Logistics Center. During these interviews, we learned of the importance of the Defense Logistics Agency (DLA) in managing Air Force supply chain risk; consequently, we also interviewed DLA personnel at the Defense Supply Center, Richmond, and DLA Headquarters.

**Methodology**

- **Review supply chain risk management (SCRM) literature**
  - Academic and business journals
  - Air Force and DoD guidance
- **Conduct interviews**
  - Weapon system managers (C-17 and F-16)
  - Defense Logistics Agency (DLA)
  - Commodity councils
  - High-tech companies
- **Identify risks managed and not managed**
- **Develop recommendations**
We also interviewed representatives of high-technology companies known for their innovative supply chain risk practices to learn more about their SCRM organizations, practices, and resources.

Throughout this research, we identified a comprehensive list of supply chain risks and examined which are managed. We later summarize these findings and develop recommendations based on them for the Air Force.
SECTION 2
Introduction and Background

Outline

• Introduction/background
  • Evolving commercial practices in SCRM
  • DoD and Air Force guidance on SCRM
  • Summary of Air Force SCRM case studies
    – Commodity councils
    – Weapon systems
      • F-16
      • C-17
    – DLA’s role in Air Force SCRM
  • Summary and recommendations

We present our research in the five sections listed above. We begin this section with an introduction to risk and its three dimensions as well as background on recent trends that affect supply chain risks. In the next section, we summarize our review of the literature and interviews with selected high-technology firms on current SCRM practices and outline a process for SCRM. In the third section, we summarize our review of DoD and Air Force guidance regarding sustainment SCRM. In the fourth section, we present our findings from our interviews with Air Force and contractor personnel involved in sustainment contracting and supply chain management, as well as findings from interviews with DLA personnel. Lastly, we summarize our findings and present recommendations for the Air Force to improve its SCRM.
We begin with definitions of supply chain risk and SCRM. The International Organization for Standardization (ISO) defines risk as the “effect of uncertainty on objectives” (2009b, p. 1). While there is no current ISO definition for supply chain risk, applying the ISO definition of risk to supply chain would yield the following: Supply chain risk is the effect of uncertainty at any point in the end-to-end supply chain on its objectives. Uncertainties, in turn, can lead to disruptions in the supply chain.

Similarly, there is no current ISO definition of SCRM. Applying the ISO (2009b, p. 2) definition of risk management—“coordinated activities to direct and control an organization’s end-to-end supply chain with regard to supply chain risks”

## Notes

1. Enslow (2008, p. 3) describes the supply chain as including “all processes involved in making, moving, storing, or servicing physical goods . . . from raw material producers through to the end customer. . . . Supply chain activities [may include] manufacturing, purchasing, warehousing, transportation, and inventory management as well as external activities performed on [an enterprise’s] behalf by suppliers, logistics partners, transportation carriers, distributors, co-packers, service and repair organizations. . . .”

2. “Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequences, or likelihood” (ISO, 2009b, p. 2). “An effect is a deviation from the expected—positive and/or negative” and “Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process)” (ISO, 2009b, p. 1).

3. The Council of Supply Chain Management Professionals (2009) developed the following definition of supply chain management: “Supply chain management encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third party service providers, and customers. In essence, supply chain management integrates supply and demand management within and across companies.”
with regard to risk”—to supply chain would yield the following: SCRM is the coordination of activities to direct and control an enterprise’s end-to-end supply chain with regard to supply chain risks. ISO further defines a risk management framework as the “set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization” (ISO, 2009b, p. 2).
There are three dimensions to measuring the total magnitude of risk. The first is the likelihood or probability of an event that could cause adverse effects (i.e., produce harm or loss) occurring. The likelihood of occurrence is much higher for some risks than others.

The second risk dimension is the expected consequence, that is, what will happen to the enterprise in the event that the risk occurs. An example of a harm or loss of low consequence resulting from a risk would be short delays in fulfillment of customer orders. An example of a high consequence (indeed, one that could destroy the enterprise) would be the release of a highly toxic substance harming or killing a large number of individuals.

The third dimension of measuring the total magnitude of risk is duration—how long the risk event causes loss or harm to the enterprise. Events can vary in their immediate and subsequent effects. A short event, such as a power outage lasting less than an hour, is likely to have little lasting impact on an enterprise. A more significant event, requiring more than a year to replace facilities, equipment, or personnel, would obviously have a longer-lasting impact. The longer the duration of the consequence, the greater the harm or loss is to an enterprise. If a risk cannot be avoided, then enterprises will focus on reducing its duration and consequences so as to reduce total harm or losses.

---

4 “Risk is often expressed in terms of the consequences of an event (including changes in circumstances) and the associated likelihood . . . of occurrence” (ISO, 2009b, p. 2).

5 “Risk is often characterized by reference to potential events . . . and consequences . . . or a combination of these” (ISO, 2009b, p. 2).
Deputy Secretary of Defense John J. Hamre (1998) commented that “[R]adical new business practices . . . have revolutionized American industry and have fueled American productivity in the last ten years.” Seeking similar productivity improvements, DoD and the Air Force have been implementing many of these new industry practices, which have changed some supply chain risks.

Two major commercial trends that DoD and the Air Force have been adopting, inventory reductions and outsourcing, can make supply chains more productive but also riskier. High inventory levels can buffer an organization against internal and external supply disruptions. Minimal inventory levels resulting from “lean” and other initiatives provide no such buffer.

---

6 “In May 1990 the Under Secretary of Defense for Acquisition established a 10-point inventory reduction plan” (GAO, 1994, p. 38).

7 The Federal Activities Inventory Reform Act (FAIR) of 1998 (P.L. 105-270) directs federal executive agencies, including DoD, to submit to the Office of Management and Budget inventories of activities that are “inherently governmental” and commercial activities (i.e., activities that are not “inherently governmental”) performed by federal employees every year by June 30. Activities identified as commercial may be competed against private-sector bidders using Office of Management and Budget (OMB) Circular A-76, Performance of Commercial Activities. If a private-sector bid is deemed cheaper, the activity is outsourced. In August 2001, President Bush announced the President’s Management Agenda, which included competitive sourcing as one of five initiatives to enhance government’s effectiveness (OMB, 2001). More recently, the Obama administration and Congress have introduced legislation to limit the “inherently governmental” functions that can be outsourced. The political pressure to limit outsourcing has been met with equally strong arguments to continue this practice.
Similarly, internal production gives an enterprise control over use and scheduling of its production assets. Outsourced production often requires an enterprise to share production assets with other customers of the supplier, giving the enterprise little or no control over use and scheduling assets. Consequently, outsourcing assembly, manufacturing, or production inputs can lead to more frequent disruptions, particularly when inventory buffers have also been reduced.

Other commercial-sector trends being adopted in the DoD and Air Force affecting its supply chain risks include supply-base rationalization,8 industry consolidations,9 globalization,10 and virtual integration.11

To reduce costs and improve supplier performance, many enterprises have analyzed their spending and supplier performance and rationalized their supply base. This often leads to a significant reduction in the number of suppliers. In response to a 2005 OMB memorandum (Johnson, 2005) that calls for “leveraging spending to the maximum extent possible,” DoD and the Air Force have been analyzing their contracts, spending, and supplier performance via strategic sourcing initiatives, which have often led to the use of fewer suppliers. Using fewer suppliers can increase supply risks because a larger percentage of inputs will be affected by a single supplier’s performance.

Over time, as industries mature, they tend to consolidate as a result of mergers, acquisitions, and bankruptcies (Deans, Kroeger, Zeisel, 2002). In the early 1990s, DoD leadership became concerned that excess capacity in defense firms, resulting from a sharp decrease in defense spending from its peak in 1985 (Office of the Under Secretary of Defense, Comptroller, Comptroller, 2009), would lead to higher weapon-system costs. Consequently, DoD actively encouraged defense industry consolidation through mergers, acquisitions, and restructuring (Perry, 1996). These efforts resulted in “a dramatic decline in prime contractors in 10 of the 12 markets DoD identified as important to national security” (GAO, 1998, p. 2) and raised concerns about preserving competition with fewer choices for defense aerospace products and suppliers. Such reductions in the number of suppliers could, as noted, increase supply chain risks.

Another trend that affects supply chain risk is globalization. Seeking to lower total costs, broaden their customer base, and diversify risks, many enterprises have actively sought suppliers in low-cost countries, moved production there, and expanded marketing and sales beyond their traditional markets. These actions have led to longer and more complex supply chains as products are customized to local markets and move through varying political, cultural, economic, and geographic environments as well as multiple distribution channels and transportation modes. The globalization of American business led the Deputy Secretary of Defense to remark that “I am not sure what an American company is anymore. I am not sure what

8 Supply-base rationalization is based on “The idea that an appropriate (often fewer) number of suppliers . . . will reap lower prices through leveraged volume, standardized service, and lower costs to manage transactions and the supply base. . . [I]t will also be easier to monitor supplier performance, and because these suppliers have been identified as ‘key’ or the ‘best fit’ for the required goods and services, the relationship can grow, fostering integration, trust, value-added services, and integration” (Duffy, 2005, p. 3).

9 See Deans, Kroeger, and Zeisel (2002) for trends in industry consolidations.

10 For more on trends in globalization see World Trade Organization (2008).

11 Virtual integration is the blurring of the traditional boundaries between supply chain partners through the use of technology and information (Magretta, 1998).
an American product is anymore” (Hamre, 1998). He noted further that DoD “want[s] very much to eliminate a defense industrial base and to adopt, in essence, just an industrial base.” As a consequence, as DoD moves away from its traditional defense industrial base, it will be tapping into the supply chains of enterprises that are often more global in nature.

The traditional lines between supply chain partners have also been blurring through the use of technology such as e-commerce to exchange information throughout the end-to-end supply chain; this phenomenon has been called virtual integration (Margretta, 1998). Activities that enterprises used to do internally, such as ordering, configuring, and delivery, are now being done by customers, suppliers, or logistics providers. Enterprises are developing multiple channels for serving customers. This makes tracking and managing supply chains, and risks to them, more complex. Such complexity requires sophisticated information systems for operations, management, and information sharing, which adds new costs and introduces additional risks to supply chains while managing others.

Lastly, buyer and societal concerns regarding environmental, fair labor, health and safety, and financial issues throughout the end-to-end supply chain broaden requirements for risk management beyond traditional categories. Such issues can cause dramatic changes in customer demand or even boycotts in the commercial sector and changes in policies in government as well as political pressures regarding supplier selection, particularly in response to negative announcements.

---

12 Deputy Defense Secretary John Hamre (1998) noted that “[d]uring the last 10 years, American businesses pioneered some startling relationships that effectively blur the distinction between customer and provider.”
Traditional approaches to supply chain risks were to buffer them with multiple suppliers, extensive frequent competition, expediting, increased order quantities, inventory safety stocks, and other stocks throughout the end-to-end supply chain (Giunipero and Eltantawy, 2004). Nevertheless, these buffering strategies also have risks and costs associated with them, including limited price leverage; increased variance in supply orders, quality, and delivery; limited opportunities for collaboration and continuous improvement; and having too much, too little, or the wrong inventory. All of these can lead to increased total costs. Inventory buffer stocks throughout the supply chain can also hide problems that enterprises should fix (Cordon, 1995).

Overall, the benefits realized in lower total costs and improved quality, delivery, and reliability from new supply chain management practices, though carrying new and different risks, increase the importance of shifting from reactive supply chain risk buffering to proactively identifying, understanding, and effectively managing end-to-end supply chain risks and vulnerabilities (Zsidisin, Ragatz, and Melnyk, 2003). Enterprises need to identify prospective risks and vulnerabilities that could affect the end-to-end supply chain, determine their probability, and assess the likely consequence of such events. Once prospective risks are identified, enterprises need to prioritize them and develop ways to prevent harmful events from occurring and mitigate and manage them should they occur (Steele and Court, 1996; LCP Consulting in conjunction with the Centre for Logistics and Supply Chain Management, 2003; and Zsidisin, Ragatz, and Melnyk, 2005).

---

13 Indeed, Zsidisin, Panelli, and Upton (2000) claim that “buffer strategies . . . are generally more expensive to maintain and usually do not reduce the chance of detrimental events from occurring in the supply base,” though they sometimes can help “‘buy time’ for the purchasing firm to come up with a solution to their incoming supply problem.”

### Traditional Supply Risk Buffering Strategies Also Have Risks

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple sources of supply</td>
<td>Limits price leverage and increases variance in quality and delivery</td>
</tr>
<tr>
<td>Frequent and extensive</td>
<td>Limits opportunities for collaboration and continuous improvement</td>
</tr>
<tr>
<td>competition</td>
<td></td>
</tr>
<tr>
<td>Expediting</td>
<td>Increases total costs</td>
</tr>
<tr>
<td>Increased order quantities</td>
<td>Increases bullwhip effect</td>
</tr>
<tr>
<td>Inventory safety stocks</td>
<td>Increases total costs</td>
</tr>
<tr>
<td>Well-stocked supply</td>
<td>Increases total costs and hides supply chain problems</td>
</tr>
<tr>
<td>pipeline</td>
<td></td>
</tr>
</tbody>
</table>
It is to be expected that the perception of what constitutes a risk and the severity of the risk will vary by industry and business; there can be differences in risk assessment within organizations as well. Risk managers (i.e., persons responsible for assessing and managing supply chain risks) and supply chain managers were recently surveyed regarding the types of risks that concern them (Enslow, 2008; Hillman and Keltz, 2007). Overlapping risks from the two separate surveys included:

- supplier delays/quality/disruptions
- logistics delays and disruptions
- natural disasters

The survey results were for risks beyond the risk manager’s traditional concerns with property and casualty insurance. Survey questions are tailored to represent the concerns of different segments of the organization. For example, supply chain managers may have different perceptions of risk than do financial managers or insurance risk assessors.

These can be caused by supplier shortages/constraints of labor, equipment, facilities, and/or inputs (goods and services) to their production processes, poor and/or variable inputs to production or production processes, or fires, explosions, structural failures, hazardous spills, financial problems, or labor strikes or slowdowns.

These include events that delay, disrupt, or affect the safety and security of road, rail, air, and ocean movements of inputs to and outputs from production.

These include earthquakes, floods, hurricanes, tornados, tsunamis, and volcanic eruptions.
• intellectual property theft, counterfeiting, or “gray market” (e.g., distribution of products through unauthorized, unintended, or unofficial channels) issues. These are highlighted in the figure. Enterprise risk managers were also surveyed regarding

- price
- internal buying enterprise operations/infrastructure
- demand volatility
- brand reputation (i.e., recalls, fair labor). (This risk was not asked of supply chain managers.)

Whereas supply chain managers were also surveyed regarding

- strategic risk
- geopolitical events
- regulatory risks
- other risks for which enterprise risk managers were not surveyed.

The results of these surveys show the relative importance of different supply chain risks from an enterprise and supply chain perspective. These differences highlight the gap between risk visibility within organizations and the need to manage risk specific to each operation.

---

19 These include internal employee or supply chain partner intellectual property theft, substituting of deceitful imitation of key inputs to production or deceitful imitation of final products, and the distribution of products through unofficial, unauthorized, or unintended channels.

20 Price risk involves the variability of raw materials costs.

21 These risks can be facility, labor, or equipment shortage/unavailability, or mechanical breakdowns. They can also be related to poor planning and management.

22 Demand variability/volatility can lead to surges or shortfalls in production, repair, or distribution.

23 Strategic risks represent a broader category of external risks than demand volatility (i.e., customer demand uncertainty), to include market conditions, financial stability, and the ability to successfully launch a new product or sell the right product in the right market. They are particularly challenging when demand and supply are highly variable and products have short life cycles.

24 These can include currency fluctuations, political unrest, and changes in trade policies.

25 These include changes in taxes, customs, tariffs, and other restrictions on imports and exports.
The above table is from Hillman and Keltz’s (2007) survey of supply chain managers and ranks relative concern for seven risks in eight industries. Not surprisingly, concerns about supply chain risks vary by industry. Of these industries, “high-tech” and “aero and defense” are perhaps most relevant to the Air Force. In both industries, both “supplier failure” and “strategic risk” are among the greatest concerns. Other risks of great concern among aerospace and defense supply chain managers but of less concern to those in “high-tech” industries include geopolitical events, regulatory risks, and logistics failures. Supply chain managers in the aerospace and defense industries reported that natural disaster risks are not applicable to them. We will discuss later what may be driving this lack of concern.

When we compare the results of the survey of supply chain managers by industry (shown in the slide) to those of the survey of supply chain managers (Enslow, 2008), we see that there are differences even within the same functional area across industries. Therefore, if one company relies on another to perform risk mitigation, it is important to understand any differences in each company’s (or industry’s) perception of risk.

26 Examples of strategic risk include loss of manufacturing capacity or overreliance on one supplier.
Evolving Commercial Practices in Supply Chain Risk Management

Outline

• Introduction/background
• Evolving commercial practices in SCRM
• DoD and Air Force guidance on SCRM
• Summary of Air Force SCRM case studies
  – Commodity councils
  – Weapon systems
    • F-16
    • C-17
  – DLA’s role in Air Force SCRM
• Summary and recommendations

SCRM is challenging for several reasons. Often, risk mitigation strategies are costly, may involve procuring backup systems, or may involve establishing alternative sources of supply. The return on investment from mitigation strategies may be difficult to quantify and justify to management, and this may be especially true for investments to mitigate risks with high impact but low likelihood. Business environments are very dynamic, and an inventory of the risks that cause concern will change as the business environment evolves, new competitors and suppliers enter or leave the market, governments and regulations change, etc. There may be limited visibility of upstream supply risks, making it difficult to assess and communicate the exposure to risks to upper management. SCRM requires balancing and communicating the uncertainty that an event will happen, the costs of preparing for the event, and the costs of paying for the consequences. We turn next to some of the best commercial practices for SCRM.
The table above lists several risk categories, significant events within those categories that have occurred in the past decade, and their consequences to the supply chain. These events also reveal that low-probability, high-consequence events may be difficult to predict at the event level, but, when grouped together, they happen more often than might be suspected.

Among these events were the September 11, 2001, terrorist attacks on the United States, which led to a shutdown of U.S. borders for days and grounding of nearly all flights. They also include natural disasters, such as hurricanes Katrina (August 2005), Rita (September 2005), and Ike (September 2008), which devastated several regions of the United States, including oil production facilities; the 2008 earthquake in Chengdu, China, which killed more than 80,000 people and disrupted manufacturing there1; and the 2011 earthquake and tsunami in Japan, which also killed thousands and caused supply disruptions that reverberated throughout the global supply chain. Even events such as the volcanic eruption in Iceland, which are peripherally connected to the global supply network, can also create disruptions that require management attention.

Other risk categories, such as strikes and changes in the law or regulations, have also occurred within the past decade. A ten-day West Coast port lockout (September and October, 2002)2 led to shipping backlogs of more than 100 days that took almost two months to clear.

---

1 Because they have robust business continuity and SCRM plans, both Cisco and Intel, who had suppliers in Chengdu, were able to smoothly transfer operations to other sources (Dornfeld, 2008; Solomon and McMorrow, 2008).

2 The Pacific Maritime Association, which represents major shipping lines and terminal operators at 29 West Coast ports, “locked out 10,500 members of the International Longshore and Warehouse Union, charging the union was engaged in a slowdown of work that amounted to a strike with pay.” (Isidore, 2002).
and is estimated to have cost the U.S. economy $1 billion to $2 billion per day (Isidore, 2002; McKenna, 2007; and Hannon, 2008). Such events caused many enterprises with lean supply chains to realize they needed to improve their risk management practices.

Federal legislation has also prompted concerns with business disruption and continuity planning. The Sarbanes-Oxley Act of 2002 “mandates that organizations . . . understand the risks that may impact their financial reporting processes and requires them to put in place the proper controls” (Berman, 2004); that is, management processes and practices to manage risks that may affect financial performance of the enterprise. While Sarbanes-Oxley does not specifically address business continuity planning, complying with it requires companies to establish controls, engage in risk assessment, implement control activities, create effective communication and information flows, and monitor their control processes. This has led many enterprises to establish or strengthen business continuity plans and programs. Because outsourced processes (i.e., the performance of external supply chain partners) can have a direct impact on an enterprise’s financial statements, those that report to the U.S. Securities and Exchange Commission are required to assess the effectiveness of their suppliers’ internal control structures pertinent to their contractual agreements. Some enterprises are beginning to require their suppliers to develop and share their business continuity plans. This has led to the establishment of SCRM organizations and their placement within business continuity programs.
According to two recent surveys, risk managers and supply chain managers do not appear to be well prepared for events that impact their supply chains.³ Virtually no risk managers reported that their SCRM was highly effective, while just over one-third reported that theirs was moderately effective. Among supply chain managers, only 11 percent reported that they were actively managing supply chain risk. This is not surprising given the relatively recent awareness of increasing supply chain risks and establishment of business continuity and SCRM organizations.

³ Enslow, 2008, summarizes an online survey of 110 risk managers located predominantly in North America, which was done in cooperation with Risk & Insurance magazine. The author does not give a response rate. Fifty-one percent of survey respondents were from large enterprises ($1 billion or more in annual revenue), 30 percent were from midsize enterprises ($50 million–$999 million), and 19 percent were from small enterprises (less than $50 million).

Hillman and Ketz, 2007, report results from a survey of 89 supply chain managers at U.S. manufacturing and retail companies. Respondents were qualified and only eligible to participate in the study if they were part of an evaluation for SCRM technology and services purchases. 52 percent of respondents were from discrete manufacturing, 36 percent were from process manufacturing, with the remainder from retail with 40 percent having 15,000 or more employees and 33 percent having fewer than 5,000 employees. The authors do not give a response rate.
The figure above, adapted from Verstrate (2008), illustrates how a lack of proactive SCRM delays recovery and increases the magnitude of the consequences of an event. The horizontal axis denotes time, and the vertical axis represents a change in the business or environment. The black line tracks how the business environment is changing, while the enterprise’s reaction to that change is shown by the red line. Enterprises that are adept at adapting to change reduce latency, so the red line and black line are very close. When there are no plans for quickly identifying events that could impact an enterprise’s supply chain, there can be a delay in recognizing such events—*decision latency*. Once an event has been recognized, if there are no plans for managing or mitigating the specific type of event that has occurred, response delays—*change design latency*—will increase while an enterprise determines the best response. Once a response has been designed, it needs to be implemented, which further delays an enterprise’s response—*change implementation latency*. Finally, after implementation, an enterprise needs to determine whether its response to the supply chain disruption was effective—*validation latency*. If not effective, the implementation may need to be modified, further delaying the enterprise’s return to normal operations.

A well-publicized example of the costs of delay in responding to a supply chain disruption was a brief fire caused by lightning at a Phillips Electronics semiconductor plant in Albuquerque, New Mexico (Latour, 2001). The fire adversely impacted the supply of critical computer chips for both Nokia and Ericsson cell phones. Nokia noticed a problem with its chip supply before Phillips notified it of the fire. As soon as it realized chip production would not be resumed quickly, Nokia “redesigned chips on the fly, sped up a project to boost production,
and flexed the company’s muscle to squeeze more out of other suppliers” (Latour, 2001). Ericsson did not have other chip suppliers and was slow to react, failing to find alternative sources of supply. As a result of its ability to detect the problem faster than Ericsson and execute a response, Nokia gained market share at the expense of Ericsson, which soon exited cell phone production.⁴

⁴ Ericsson eventually developed a proactive SCRM approach (Norrman and Jansson, 2004) but too late to prevent the large losses associated with the fire at the Phillips plant.
We conclude from our company interviews and review of the literature that proactive SCRM requires an organization that develops guidance and policies for identifying and managing supply chain risks. It must develop the capability to target critical risks and develop and execute risk management plans.

Proactive SCRM also requires that an enterprise have a supply chain risk assessment and management process. Often supporting the process are tools for supply chain risk identification, assessment, and monitoring. Along with those tools are strategies for mitigating and managing many supply chain disruptions. Strategies may include identifying or developing a second source or site for manufacture, holding inventory to cover requirements for the duration of the disruption, and, in the long term, designing future products and selecting suppliers to reduce overall supply chain risks.
**SCRM Organization**

- **Enterprise-wide SCRM organization**
  - Develop policy, processes, tools, and metrics (e.g., suppliers with business continuity plans, time to recovery)
  - Institutionalize reporting requirements (e.g., board of directors level)

- **Strategic business units**
  - Identify, assess, and prioritize risks
  - Develop and implement specific plans
  - Request and review supplier business continuity plans
  - Monitor and report risks

The enterprises most successful at SCRM have a formal SCRM program (Enslow, 2008). They create a partnership of corporate risk managers and supply chain operations. The risk manager mobilizes the enterprise against supply chain risks, while supply chain operations work to ensure that risk processes are designed cross-functionally and end-to-end and embedded into current activities. For example, cross-functional SCRM might include representatives from procurement, manufacturing, and sales. An end-to-end perspective would identify supply chain risk along all the points of the supply chain, including subtier suppliers.

We asked representatives from three companies how they were organized for SCRM. All reported that they had an enterprise-wide SCRM organization that develops policies, processes, tools, internal metrics (such as number of suppliers with business continuity plans), and supplier time to recovery commitments. These centralized organizations also institutionalize reporting requirements for SCRM, which can include regular reports to the enterprise’s board of directors.

One company reported that strategic business units (SBUs) do the actual identifying, assessing, and prioritization of supply chain risks for their products and services. The SBUs also develop and implement specific risk management plans, request and review supplier business continuity plans, and monitor and report supply chain risk up to SBU and enterprise management.

The Cisco SCRM team is part of its Customer Value Chain Management (CVCM) organization (Harrington and O’Connor, 2009). Within the CVCM organization, it partners with Global Supplier Management (GSM), which is responsible for sourcing decisions and manag-
ing relationships; Product Operations, which is responsible for developing products from engineering innovations, and Global Manufacturing Operations, which is responsible for global manufacturing and logistics. CVCM also partners with Cisco engineers to assess the resiliency of new products. Lastly, CVCM partners with Cisco’s suppliers, manufacturing partners, and transportation and logistics providers to continuously manage supply chain risks.

The four key elements of Cisco’s program are as follows:

1. The Business Continuity Planning Program, which works closely with internal and external partners “to document recovery plans and times and drive resiliency standards.”
2. Crisis Management, which is responsible for continuous global monitoring of and response to disruptions.
3. Product Resiliency, which helps Cisco’s business units address supply chain vulnerabilities during product design as well as to prioritize and reduce the costs of risk mitigation strategies.
4. Supply Chain Resiliency, which identifies points in the supply chain where time to recovery would be unacceptably high and develops resiliency plans for them.
In developing SCRM organizations, enterprises may seek to develop or impart certain skills. Survey responses of risk managers (Enslow, 2008) indicated that the following skills were very important for success:

- Strong networking and orchestration—79 percent
- Basic understanding of end-to-end supply chain process—77 percent
- Effectively articulate how risk initiatives deliver short-term operational or financial improvement—70 percent
- Talk the language of the CEO/CFO to gain support for initiatives—66 percent
- Effectively educate functional personnel on key risk areas and best practices—63 percent
- Adept at aggregating risks across functional silos and business units to monitor total enterprise risk—63 percent.

Strong networking and orchestration skills are particularly important because supply chain risks cut across different functions within the enterprise as well as suppliers external to the enterprise. While the goal of SCRM is to prevent adverse consequences (e.g., additional costs, short- and long-term loss of business) to the enterprise, it is often hard to justify expending scarce resources for SCRM initiatives to prevent loss. Therefore, articulating how risk initiatives deliver short-term operational or financial improvement is particularly important. In addition, supply chain risk managers need to speak the language of the CEO and CFO in
terms of enterprise-wide benefits or loss avoidance of SCRM initiatives in order to obtain the resources to develop and execute SCRM strategies.

The companies we interviewed also reported that supply chain risk managers needed to be able to effectively educate different functional personnel on key risk areas and best practices for managing those risks. Further, they need to be adept at aggregating risks across functional silos and enterprise business units to monitor total enterprise risk.

Representatives from one company we interviewed told us that they seek to hire persons knowledgeable in supply chain management, which they say is harder to teach, and then train them in SCRM.
The above figure outlines a composite, multistep process for supply chain risk assessment and management based on five proposed methods for analyzing supply vulnerabilities described in the literature. The nine-step process begins by recognizing the existence of a potential risk.

Yates and Stone (1992) suggest four elements for risk appraisal: existence, including awareness of the potential for possible loss; identity, including identification of specific losses that might occur; likelihood, including determination of the likelihood of a possible loss; and significance, including assessment of the significance of a possible loss.

Zsidisin, Ragatz, and Melnyk (2003) propose a second model based on awareness, prevention, remediation, and knowledge management. Awareness is both internal and external and may include financial reports, supply chain mapping, and use of audit instruments. Prevention includes identification, assessment, treatment, and monitoring of risks, and may include such actions as a risk register. Remediation includes planning how to minimize impact and duration of a risk and the resources required to address it. Knowledge management includes tracking results and actions for continuous improvement.

Zsidisin, Ragatz, and Melnyk (2003) also suggest a model adapted to the strategic sourcing process. Its first step is analyzing internal requirements and understanding risk tolerance. Its second step is analyzing the supply market to understand market risks. Its third step is to determine the approach to risk management and relationship types to reduce and buffer risks. Its fourth step is to identify and evaluate suppliers, including assessing the risks of each. Its fifth step is to build and manage relationships, including monitoring risks in them.

Ziegenbein and Nienhaus (2004) suggest a four-part continuous SCRM process. Its elements include identification of risks, including a structured documentation of risks and their sources; assessment of risks, including measuring their probability and impact; controlling risks, including evaluating risks and deciding how to cope with them; and monitoring risks, including a transparent overview of supply chain risks at all times.

LCP Consulting in conjunction with the Centre for Logistics and Supply Chain Management (2003) proposed an SCRM flow beginning with a description of the supply chain. An enterprise may then use vulnerability self-assessment templates to document risks in such areas as demand, supply, environment contingency, process, and control. Once the self-assessment is complete, an enterprise may evaluate the implications of the risks they face, including their scale, duration,
(step 1), identifying the exposure of the supply base to the risk (step 2), estimating the likelihood and severity of realization of the risk (step 3 and 4), prioritizing risks by potential costs to allocate scarce resources appropriately (step 5), developing, assessing, and executing a risk management strategy for the prioritized list (step 6), developing contingency plans (step 7), monitoring the risk environment to respond to changes and re-prioritize responses to risk (step 8), and, finally, continuously integrating lessons learned and improving risk and supplier management policies (step 9).

We define each step and provide additional details on identifying risk (step 2), prioritizing risk (step 5), developing assessing and executing management strategies (step 6), and capturing lessons learned to improve risk management (step 9).

**Step 1: Recognizing Risk.** Before a risk can be addressed, there must be an awareness that supply vulnerabilities exist (Zsidisin, Ragatz, and Melnyk, 2003). Enterprises need to be aware that their actions or lack of action creates various supply chain risks.
Step 2: Identifying Risks. This step of risk management and assessment requires identification of supply vulnerabilities. Enterprises need to identify the possible risks associated with a prospective supply strategy. An example of a supply chain risk may be disruptions due to natural disasters. One way to visualize these risks, which are related to location, is to map them, as we illustrate later. The figure above shows the locations of hurricanes, earthquakes by magnitude, and tornados by damage for the 48 contiguous states.\(^6\)

Other methods for identifying risks include brainstorming, interviews, workshops, supply chain mapping/description,\(^7\) the Delphi Method,\(^8\) fault or event tree analysis\(^9\) (Ziegenbein and Nienhaus, 2004), and Nominal Group Technique, or NGT (Zsidisin, Panelli, and Upton, 2000).\(^10\) Some authors recommend assessing vulnerabilities by categories of external risks, such

---

\(^6\) Data for earthquakes are for 1789 to 2004; those for tornados and hurricanes are for 1995 to 2000.

\(^7\) Supply chain mapping identifies all members, facilities, linkages, and flows of goods, information, and money in the end-to-end supply chain from upstream raw materials suppliers through manufacture to downstream delivery to the final customer, use, and then disposal (Gardner and Cooper, 2003).

\(^8\) The Delphi Method relies on a series of questionnaires among a group of experts to discern a consensus as well as reasons for disagreement. For further information, see Linstone and Turoff, 2002.

\(^9\) Fault or event tree analysis breaks down a system risk event into component failures step by step by linking failure events with their causes. Because fault tree analysis is used for qualitative and quantitative analysis of systems, it is essential that for a risk every cause is considered in the fault tree and conversely that every mentioned cause is actually needed to trigger the event (Schellhorn, Thums, and Reif, 2002, p. 1).

\(^10\) NGT involves individuals first generating their own ideas, then sharing them with a group, before ranking each. For more information, see Van De Ven and Delbecq, 1974.
as demand, supply (e.g., supplier failure, interruption in inbound shipments) and environment (e.g., natural disasters, accidents, terrorism/sabotage, and business environment), and of internal risks, such as control, process, and contingency (i.e., plans to mitigate and manage the impact of a risk) (Peck et al., 2003). (See Appendix E for a list of categories of supply chain risks.) Others recommend a less structured approach so as not to inhibit thinking (e.g., Steele and Court, 1996).11

Supplier participation is necessary for undertaking a vulnerability analysis (Steele and Court, 1996). While few organizations have the resources needed to eliminate all vulnerabilities and those that do may choose to employ them elsewhere, identifying vulnerabilities is an essential step in risk management.

**Step 3: Estimating Likelihood of Occurrence.** This step of the risk assessment and management process calls for enterprises to estimate the likelihood of occurrence of the prospective vulnerability. Some authors (e.g., Steele and Court, 1996) assign a relative weight to the probability of occurrence while others (Ziegenbein and Nienhaus, 2004) classify the possibility of occurrence into unlikely, possible, likely and very likely.

**Step 4: Estimate the Total Impact if Realized.** In this step, the organization needs to assess the relative impact or significance of the prospective loss (i.e., to calibrate the exposure of the business). The impact of a given risk is a function of its scale, scope, duration, recovery time, and total cost. A risk’s total impact to the enterprise can be ranked as low or high (Steele and Court, 1996) or as low, medium, significant, or fatal (Ziegenbein and Nienhaus, 2004).

**Step 5: Prioritize Risks.** Rather than addressing all vulnerable areas at once, enterprises can focus on those events that are likely to bring the greatest relief (Steele and Court, 1996). This step prioritizes risks by their significance to the enterprise so as to focus available resources for risk elimination, mitigation, and management efforts on the most important risks. Because each commodity, product, or service exhibits a different risk profile (Giunipero and Eltantawy, 2004) and identifying, assessing, and planning for supply chain risks requires considerable time and resources, enterprises need a way to prioritize SCRM efforts. The next three charts provide examples of alternative methods to prioritize risks.

---

11 “When working through the vulnerability analysis there will be a temptation to make use of some form of checklist. This should be avoided, since experience has shown that checklists seem to inhibit entrepreneurial thinking, so essential in this exercise” (Steele and Court, 1996, p. 89).
One proposed way to prioritize risks is to plot risks by probability of occurrence from low to high and consequence of event (interruption time or cost) from minor to major and identify the acceptable risk frontier above which risks are unacceptable to the enterprise and must be managed (Zsidisin, Ragatz, and Melnyk, 2003). The figure above notionally depicts this approach.
Steel and Court (1996) prioritize supply risks for management action based on the risks’ three dimensions: probability of occurrence (i.e., high, medium, and low likelihood), duration (i.e., short and long), and impact (i.e., high and low consequence). The above chart summarizes one way of prioritizing risks based on assessments of their priority, duration, and impact.

Steel and Court’s Prioritization of Supply Risks

<table>
<thead>
<tr>
<th>Priority</th>
<th>Likelihood</th>
<th>Duration</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>High</td>
<td>Long</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>Medium</td>
<td>Long</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>High</td>
<td>Short</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Medium</td>
<td>Short</td>
<td>High</td>
</tr>
<tr>
<td>5</td>
<td>High</td>
<td>Long</td>
<td>Low</td>
</tr>
<tr>
<td>6</td>
<td>Low</td>
<td>Long</td>
<td>High</td>
</tr>
<tr>
<td>7</td>
<td>Medium</td>
<td>Long</td>
<td>Low</td>
</tr>
<tr>
<td>8</td>
<td>Low</td>
<td>Short</td>
<td>High</td>
</tr>
<tr>
<td>9</td>
<td>Low</td>
<td>Long</td>
<td>Low</td>
</tr>
<tr>
<td>10</td>
<td>High</td>
<td>Short</td>
<td>Low</td>
</tr>
<tr>
<td>11</td>
<td>Medium</td>
<td>Short</td>
<td>Low</td>
</tr>
<tr>
<td>12</td>
<td>Low</td>
<td>Short</td>
<td>Low</td>
</tr>
</tbody>
</table>

SOURCE: Adapted from Steele and Court, 1996.
Another way to prioritize risks is to map their probability and their consequence (Ziegenbein and Nienhaus, 2004). The Air Force has recently standardized a 5×5 map for assessing risks during weapon system acquisition (Peyton, 2008), as shown above. It establishes as A-Risk those with the highest likelihood and severity, while giving lower priority to those with lesser consequence or probability of occurrence.
Step 6: Developing a Risk Management Strategy. This step of the SCRM process involves developing, assessing, and executing strategies for reducing the likelihood or mitigating the consequence or duration of prospective risks (Zsidisin, Ragatz, and Melnyk, 2003). For low-priority risks (i.e., those with low likelihood of occurrence and low consequence), an enterprise may want to ignore or accept the risk. For high-priority risks, (i.e., those with high likelihood of occurrence and high consequence) an enterprise may try to avoid12 the loss occurrence. To avoid supplier disruptions, enterprises can rigorously assess suppliers, carefully select them (using certification and pre-qualification), and frequently monitor or audit them for viability, quality (using statistical process control), reliability, and dependency (i.e., enterprise’s percentage of supplier’s total business). They can also establish multiple two-way communication channels for sharing forecasts and plans. They can gain or maintain visibility into the supplier’s operations and require a quality management program and contingency plan. They can also align the supplier’s incentives with theirs, penalize poor performance (using fines or reduced business), reward good performance (using gain sharing, increased business, and supplier recognition), and share financial risks. Lastly they can encourage joint improvement initiatives and direct access to knowledge workers. To prevent demand (volatility) risk, enterprises can develop industry standards, common product “building blocks,” or collaborative forecasting. Process risk prevention includes using ISO 9000 standards for process control, increasing supply chain visibility, and reducing lead times.

12 To avoid supplier disruptions, enterprises can rigorously assess suppliers, carefully select them (using certification and pre-qualification), and frequently monitor or audit them for viability, quality (using statistical process control), reliability, and dependency (i.e., enterprise’s percentage of supplier’s total business). They can also establish multiple two-way communication channels for sharing forecasts and plans. They can gain or maintain visibility into the supplier’s operations and require a quality management program and contingency plan. They can also align the supplier’s incentives with theirs, penalize poor performance (using fines or reduced business), reward good performance (using gain sharing, increased business, and supplier recognition), and share financial risks. Lastly they can encourage joint improvement initiatives and direct access to knowledge workers. To prevent demand (volatility) risk, enterprises can develop industry standards, common product “building blocks,” or collaborative forecasting. Process risk prevention includes using ISO 9000 standards for process control, increasing supply chain visibility, and reducing lead times.
altogether or accept and reduce its likelihood,\textsuperscript{13} consequence, or duration.\textsuperscript{14} If the likelihood, consequence, or duration of a risk cannot be reduced, then an enterprise needs to identify prospective operational or risk-sharing or transfer measures to mitigate the risk (Ziegenbein and Nienhaus, 2004).

\textsuperscript{13} To \textit{mitigate supplier risks}, enterprises can work with the supplier to improve its performance. They can also hold inventory (e.g., emergency supplies), obtain design specifications (i.e., technical data enabling them to develop supplier products internally or purchase them from another source), require the supplier to develop alternative sites, use dual or multiple sourcing, develop an alternative source, and move special tooling. To \textit{mitigate demand risk}, enterprises can hold safety stock inventory or develop multiple sources. \textit{Process risk mitigation} also includes holding safety stock inventory and using multiple sourcing.

\textsuperscript{14} To develop \textit{contingency options to reduce supplier risks}, enterprises can establish a second source contract or identify and introduce alternative sources. \textit{Contingency options for demand (volatility) risk} include identifying strategies to ration supply or reduce inventory and plans for their introduction. \textit{Process risk contingency options include} identifying strategies to shift production or flow and plans for their execution.
The above chart is an example from Ziegenbein and Nienhaus (2004) of short-, medium-, and long-term supply risk management strategies for both occurrence-oriented and impact-oriented supply events. For example, a long-term strategy for avoiding or reducing supplier problems is to have a rigorous supplier selection process followed by regular audits of supplier facilities, processes, and finances. Another strategy to reduce supply risks is to have multiple sources, if feasible. A third long-term strategy is to share or transfer the risk by including penalties in contracts for unreliable supply. A short-term strategy is to monitor supplier delivery dates and quantities (as we noted Nokia did for its chip supply) to quickly detect emerging problems at suppliers. A medium-term strategy could be to have extra inventory or safety stock, but many enterprises prefer not to do this because of the added costs and risk of obsolescence or eventual disposal due to excess inventory.

Prospective actions, depending on probability of risk, consequence, and duration, can range from eliminating the need or finding alternatives for a commodity to taking no immedi-

---

15 In the chart, the terms strategic, tactical, and operational are meant to distinguish between different business planning horizons. Strategic refers to long-term, tactical to midterm, and operational to short-term time frames. This differs from the way these terms are used by the Air Force and explained in Air Force Doctrine Document 2 (2007). Under Air Force doctrine, tactics define actions and how forces are employed, while strategy and operations define desired effects; strategic effects are focused on the desired national-level outcomes, while operations detail the plans needed to achieve strategic goals.

16 Transferring risk does not necessarily mean transferring costs or consequences. For example, BP may have thought they were transferring risks to subtier suppliers, but the consequences and costs from the Deepwater Horizon oil spill in the Gulf of Mexico were heavily borne by BP.
ate action. Because some prospective risk prevention or mitigation efforts can be quite costly, enterprises need to evaluate each prospective strategy’s costs and benefits. They should then gain management support and implement those strategies that are cost-effective (Kiser and Cantrell, 2006).\textsuperscript{17}

\textsuperscript{17} Cost-effective is not defined by Kiser and Cantrell, but will likely depend on the level of risk aversion and the available resources to mitigate risks that may be seen as having low likelihoods but catastrophic consequences.
For example, the figure above outlines different strategies for two prevalent supply chain improvement strategies: The upper right-hand quadrant indicates that a combination of outsourcing and reducing internal inventory buffers could reduce costs but increase the risk of supply chain disruptions, which in turn can decrease revenue due to lost sales. The arrows point to potential risk mitigation strategies that could be either external (work with suppliers to improve responsiveness, reduce lead time variability) or internal (increase inventory buffers). The lower right-hand quadrant shows the tradeoff of decreased risk of supply chain disruption at the cost of increased inventory and forgoing of potential savings from outsourcing. The risk of holding inventory can be mitigated if the accuracy of demand forecasts is improved, however, this is difficult to achieve. An alternative strategy is to hold fewer inventories but improve the responsiveness of the supply chain, which reduces the need for inventory and increases risk protection through risk transfer or insurance.

**Step 7: Developing Contingency Plans.** This step is focused on developing contingency plans for when disruptions occur because not all risks can be cost effectively avoided, adequately mitigated, or even identified. For example, while it may have been unlikely that anyone would have identified the radiation risk that resulted after the March 2011 earthquake and tsunami in Japan, contingency plans can be designed to quickly respond to unforeseen disruptions. These are detailed recovery or remediation plans for shortening the duration of a disruption, minimizing its consequence, and identifying the resources to execute the plan (Zsidisin, Ragatz, and Melnyk, 2003). As discussed earlier, the duration of a risk can be reduced by developing proactive risk management plans that reduce the decision latency to react to an
event, reduce the reaction plan design latency, reduce the implementation latency, and reduce the execution time of a recovery plan.

**Step 8: Continuous Monitoring.** Organizations should continuously monitor the environment after a supply strategy and associated risk management plan is in place for any increases or decreases in prospective supply chain risks that warrant changing the supply strategy or risk management plan (Zsidisin, Ragatz, and Melnyk, 2003).

**Step 9: Conduct Post-Incident Audits.** This step is focused on continuous learning and knowledge management. When a supply disruption occurs, an enterprise needs to conduct post-incident audits to determine its root cause and document any lessons learned for better management of future events. The audits should also address any deficiencies identified in past risk assessments, mitigation strategies, and contingency plans (Zsidisin, Ragatz, and Melnyk, 2003).
Example of How Hewlett-Packard Manages Risk

<table>
<thead>
<tr>
<th>Supply Chain Management Strategy</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Natural/man-made hazards</td>
</tr>
<tr>
<td></td>
<td>Country</td>
</tr>
<tr>
<td></td>
<td>Supplier</td>
</tr>
<tr>
<td></td>
<td>Bankruptcy</td>
</tr>
<tr>
<td></td>
<td>Network/soft-ware outage</td>
</tr>
<tr>
<td></td>
<td>Internet provider</td>
</tr>
<tr>
<td></td>
<td>Regulatory</td>
</tr>
<tr>
<td></td>
<td>Commodity price</td>
</tr>
<tr>
<td></td>
<td>Workforce practices</td>
</tr>
<tr>
<td></td>
<td>Logistics</td>
</tr>
<tr>
<td></td>
<td>Failure</td>
</tr>
<tr>
<td></td>
<td>Inventory</td>
</tr>
<tr>
<td></td>
<td>Quality</td>
</tr>
<tr>
<td>Globalization and outsourcing</td>
<td>High impact</td>
</tr>
<tr>
<td>Sole sourcing</td>
<td>Moderate impact</td>
</tr>
<tr>
<td>Lean practices</td>
<td>High impact</td>
</tr>
<tr>
<td>Distribution hubs</td>
<td>Moderate impact</td>
</tr>
<tr>
<td>Commodity dependency</td>
<td></td>
</tr>
<tr>
<td>Demand visibility/variability</td>
<td></td>
</tr>
<tr>
<td>Supply tiering</td>
<td>High impact</td>
</tr>
<tr>
<td>Returns management</td>
<td>Moderate impact</td>
</tr>
</tbody>
</table>

Exposure and risk to the bottom line are key criteria for ranking high impact areas.

The above table summarizes how Hewlett-Packard identifies the impact of differing risks on its supply chain management strategies (Verstrate, 2008). For example, the country where a supplier is located has a high impact on risks for HP’s globalization and outsourcing strategy, as can the supplier’s Internet provider, regulations, workforce practices, and quality. Note particularly that natural and man-made hazards have a high impact when enterprises use sole sourcing, lean practices, and distribution hubs. Note further that the risks to quality are high when using globalization and outsourcing, sole sourcing, supply tiering, and returns management.

---

18 “Distribution hubs” are regional centers of a physical distribution system into which goods flow for collection, sorting, transshipment, and distribution to a particular area of dispersed locations. “Commodity dependency” is the extent to which an enterprise depends on a particular commodity. “Demand visibility/variability” reflects the ability to see undistorted and accurate demands for a good or service within the time necessary to respond to it and the extent to which such demands vary over time. A “returns management” system is a system that manages returns of faulty products for businesses, sometimes also called the reverse supply chain.

19 Supply tiering refers to disaggregated or multitier supply chains where a number of different suppliers add value at different points along the supply chain (e.g., from raw materials, to subcomponents, to subassemblies, to assemblies, to assembled final product, to delivered final product).
Summary of Emerging Practices

- Quantifying the impact of disruptions on the enterprise, products, and customers
- Establishing sense-and-respond mechanisms to immediately identify supply chain disruptions, assess their consequence, and initiate recovery plans
- Assessing units and personnel on their SCRM plans
- Requiring key suppliers to:
  - Develop business continuity plans that are regularly reviewed
  - Commit to a time-to-recovery
- Developing standard metrics for SCRM

We end this section on best commercial practices with a reminder that SCRM is an emerging practice. Most enterprises have only recently begun to quantify the consequences of supply disruptions on the enterprise, its products, and its customers. Because resource commitments to SCRM initiatives need to be justified, quantifying the prospective consequences is important to the success of SCRM within an enterprise. They are also establishing sense-and-respond mechanisms to immediately identify prospective supply chain disruptions, assess their consequences, and initiate recovery plans.

Some enterprises have begun to assess the SCRM plans of SBUs and their key personnel. They are also requiring key suppliers to develop business continuity plans, which they regularly review.\(^{20}\) Cisco is requiring key suppliers to commit to a time to recovery, which helps it plan risk mitigation strategies, such as developing alternative sources of supply or inventory levels that can cover the expected duration of a disruption (Harrington and O’Connor, 2009).

Lastly, some forward-thinking enterprises have come together to begin developing metrics and ISO standards for SCRM through the Supply Chain Risk Leadership Council.

---

\(^{20}\) One company we interviewed said they review their most important suppliers’ business continuity plans every six months.
In this section, we examine the existing DoD and Air Force guidance on managing supply chain risk and compare it with commercial best practices, identifying gaps between commercial best practices and DoD and Air Force guidance.
**DoD and AF Risk Management Guidance Focuses on Acquisition**

- Selected DoD and AF Guidance on acquisition, sustainment, and risk
  - DoD 5000.1 and DoD 5000.2
  - Risk Management Guide for DoD Acquisition
  - Acquisition and Sustainment Lifecycle Management 63-101
  - DoD Supply Chain Materiel Management
  - Air Force Acquisition Quality Program 63-501
  - USAF Deficiency Reporting, Investigation and Resolution TO 00-35D-54
  - Guidance Memorandum: Life Cycle Risk Management

- Federal Acquisition Regulation (FAR)

| Key acquisition metrics are program cost, performance, and schedule |


We reviewed these documents for specific guidance on SCRM. We found that risk identification and mitigation strategies focus on activities during the acquisition phase and are related to risks in cost, technical performance, or schedule of the weapon-system acquisition program. We found no direct discussion in Air Force guidance of risk in sustainment or how decisions about supply chain risk and supplier relationship management made during the design phase could affect subsequent sustainment risks. We briefly describe each of these documents in Appendix C.
The FAR shapes approaches toward SCRM within DoD and among major OEMs. The FAR governs the acquisition of products and services by agents of the federal government. It provides a consistent set of guidelines and legal definitions for establishing the obligations and responsibilities of contractors. Yet its discussion of risk focuses on cost, technical performance, and schedule, with no general reference to supply chain risk or specific reference to risks noted in literature on commercial practices.

The approach of aeronautics and defense firms differs from other firms particularly in their consideration of natural disasters. Hillman and Keltz (2007) found that aerospace and defense firms did not consider natural disasters to be a major supply chain risk, in contrast to high-tech, chemical, and pharmaceutical firms, which all listed natural disasters as a serious supply chain risk.

One reason for this may be the force majeure clause, which the FAR makes common to federal contracts. As one aerospace SCRM official we interviewed told us, “One thing we look at is what is in the contract. If there is a force majeure clause, then the cost of realizing a supply chain disruption due to natural causes is passed on to the customer.” Such clauses mean suppliers are not held responsible for disruptions considered outside their control.

---

1 The Defense Federal Acquisition Regulation Supplement (DFARS) provides DoD implementation and supplementation of the FAR. The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public.
The only DoD or Air Force guidance specific to supply chain risk is DoD 4140.1-R, *DoD Supply Chain Materiel Management Regulation*. The scope of risks identified in that guidance is limited to such sustainment issues as stock outages, stockpile drawdowns, shelf-life expiration, supplier financial problems, long repair-cycle times, long order and shipping times, underestimation of the true maintenance replacement rate, resupply from external sources such as direct vendor deliveries, and deferred procurement (the practice of planning for unpredictable demands by having suppliers agree to stock spares of an item at their facilities until demand is realized by the Air Force). Moreover, while DoD 4140.1-R identifies some categories of risks (e.g., retail stock level) and lists factors that might contribute to increased risk, it does not discuss how to manage them in any detail.

We compare the supply chain risks found in DoD 4140.1-R with those listed in best practice literature (for a complete list of risks identified in the business literature, see Appendix E) and noted a match if there was a general agreement between the two (as indicated by colors on the above chart). While the list of business supply chain risks shown is not exhaustive, it represents the core of most commonly cited risks. There is a match between the DoD-identified risks “out of stock,” “draw down of stockpile,” and “shelf life expiration” with the general category of “demand uncertainty” in the business literature. The risks listed in DoD 4140.1-R also match other general categories of risk identified in the business literature, including such categories as “supplier risks,” “long lead times,” “inbound and outbound distribution,” “logistics delays/failures,” and “internal risks.”

### DoD 4140.1-R Risks

<table>
<thead>
<tr>
<th>DoD 4140.1-R Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out of stock</td>
</tr>
<tr>
<td>Draw down of the stockpile</td>
</tr>
<tr>
<td>Shelf life expiration</td>
</tr>
<tr>
<td>Supplier financial problems</td>
</tr>
<tr>
<td><strong>Exceeding:</strong></td>
</tr>
<tr>
<td>Repair cycle time</td>
</tr>
<tr>
<td>Order and shipping time</td>
</tr>
<tr>
<td>Maintenance replacement rate</td>
</tr>
<tr>
<td>Resupply from external sources (i.e., direct vendor delivery)</td>
</tr>
<tr>
<td>Deferred procurement</td>
</tr>
</tbody>
</table>

### Best Practice Literature

<table>
<thead>
<tr>
<th>Best Practice Literature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demand uncertainty/volatility</td>
</tr>
<tr>
<td><strong>Supplier risks</strong></td>
</tr>
<tr>
<td>Supplier risks</td>
</tr>
<tr>
<td>Long lead times</td>
</tr>
<tr>
<td>Inbound and outbound distribution</td>
</tr>
<tr>
<td>Logistics delays/failures</td>
</tr>
<tr>
<td>Internal risk (operations/infrastructure)</td>
</tr>
<tr>
<td>Environmental risks</td>
</tr>
<tr>
<td>Natural disasters</td>
</tr>
<tr>
<td>Pricing</td>
</tr>
<tr>
<td>Brand reputation</td>
</tr>
<tr>
<td>Strategic risk</td>
</tr>
<tr>
<td>Geopolitical event</td>
</tr>
<tr>
<td>Intellectual property infringement</td>
</tr>
<tr>
<td>Regulatory risk</td>
</tr>
</tbody>
</table>

Neither DoD nor its suppliers manage these risks.

**Sources:**
However, there are several categories of risks identified in the business literature that the DoD does not address. These include “environmental,” “natural disaster,” “pricing,” “brand reputation,” “strategic,” “geopolitical,” “intellectual property infringement,” and “regulatory risks.” Some of these risks, such as “brand reputation,” do not appear directly pertinent to the Air Force; nevertheless, the overall comparison reveals a substantial set of risks not addressed by DoD or the Air Force directly, the management of which, as we noted of the FAR, is not contractually the obligation of the supplier. (One risk, that of deferred procurement, is noted by DoD but does not appear to be discussed in the commercial literature.)

Two questions arise from this analysis. First, what is the potential impact to the Air Force’s supply chain from failing to manage these risks? Second, how does the Air Force currently implement the guidance in DoD 4140.1-R; that is, how does it manage the risks identified?
To understand the potential impact of failing to consider risks from natural disasters or environmental causes, we return to the map of natural disasters presented earlier in this documented briefing. This map highlights areas susceptible to hurricane, tornado, or earthquake damage. We use fiscal year 2007 data from the Federal Procurement Data System to identify the place of performance of suppliers of parts (manufacturing and repair) to Air Force weapon systems. We have circled clusters of suppliers with facilities in natural-disaster risk zones. The fact that a supplier is located in a risk zone does not necessarily mean that the Air Force’s supply chain is at risk. Nevertheless, such location indicates the extent to which natural disasters could affect the Air Force supply chain, which policymakers and sustainment managers should understand when developing appropriate mitigation plans.

For example, this map should lead policymakers and sustainment managers to consider the following questions:

- Which goods and services are produced by the suppliers at risk for natural disasters?
- Which weapon system do these goods and services impact?
- If a supplier experiences force majeure, what will be its time to recovery?
- Who in the Air Force has this information?
- Do the suppliers have business continuity plans in place, and has the Air Force reviewed the plans to determine their adequacy?
In this section, we explore the processes used by the Air Force to manage supply chain risk. We seek to identify which supply chain risks are known, how they are managed, and who in the Air Force is responsible for managing them.

To answer these questions, we interviewed subject-matter experts in the Air Force commodity councils, supply chain experts for the F-16 Maintenance organization, and managers of a system using Contractor Logistics Support, the C-17. We also later discuss the role of the DLA in Air Force SCRM.
At the time of this research, there were five commodity councils, organized to manage commodities used in aircraft structures, communication and electronics, support equipment, landing gear, secondary power, and engines (including propulsion, instruments and accessories). These five commodity councils were part of the Air Force Global Logistics Support Center (AFGLSC).¹

Commodity councils facilitate the establishment of contracts between the Air Force and its suppliers. Effective management of the contracting process is essential to reducing the administrative lead time required to initiate a contract. Long contract lead times have been a persistent problem leading to supply shortages.

We interviewed representatives at each of the three ALCs regarding the processes used by their commodity councils to manage risks.² We found each ALC had a slightly different approach to SCRM. These differences are a result of the type of commodities they manage, the amount of previous exposure to supply chain problems, and perceived reasons for those problems that each ALC has.

For example, the Landing Gear Commodity Council (LGCC) deals with many more competitively sourced parts than does the Aircraft Structures or Propulsion Commodity Council. Therefore, most of its SCRM focuses on mitigating risks in managing the deliverables

---

¹ Air Force Materiel Command recently stood down the AFGLSC as an organization and folded its activities into the new Air Force Sustainment Center.

² Interviews were conducted by telephone and followed a structured format. Questions were emailed to the commodity council representatives in advance of the interviews. Two to four representatives were involved in the interview; this varied by ALC. Following the interviews, we asked if the commodity council lead would be willing to examine and rank a list of risks based on his or her experience.
of multiple suppliers. In some cases, landing gear components were experiencing production lead times of 900 to 1,000 days, or nearly three years. Many landing-gear items are provided by small businesses; indeed, DoD met many small-business goals through purchase of these items. The effort required to manage all these small businesses is significant, especially in light of Air Force personnel reductions.

To mitigate the risk created by long lead times and difficulty of managing many small business suppliers, the LGCC has developed a prime vendor approach, in which the prime vendor is given the lead to manage deliverables of other suppliers. This strategy transfers responsibility and risk away from the Air Force and to a lead supplier or prime vendor. While many contractors are involved, a lead contractor is responsible for the final on-time or specified delivery of the item. This lets the Air Force consolidate contracts under one supplier, thereby permitting greater visibility on performance problems. Perhaps more importantly, the lead supplier integrator has strong incentives to act quickly to correct performance problems. Air Force representatives noted that the supplier integrator has more leeway in terminating contracts for lack of performance by individual suppliers than the Air Force would have. In this case, the Air Force has knowingly transferred responsibility for a critical supply chain performance criterion (delivery lead times) to an external supplier. The commodity councils have weighed the risk of transferring this responsibility against the benefits of the streamlined management structure it affords and have decided to assume the risk. In this case, the Air Force is aware of the transfer risk and has chosen to mitigate it, namely through incentives and penalties on the lead supplier based on performance of the subtier.

Representatives of the Aircraft Structures Commodity Council and the Communications and Electronics Commodity Council told us that they examined the financial status of suppliers, especially those that had previously done business with DoD. This included using records of the Defense Contract Audit Agency to verify contractor performance on previous government contracts but seldom included other financial rating systems, such as Dun and Bradstreet. High-value or competitive contracts typically had more thorough financial examinations, but for more than 95 percent of acquisitions financial checks ended with the Defense Contract Audit Agency clearance.

Overall, our conversations with the representatives of the commodity councils revealed an understanding and appreciation of the importance of SCRM. In addition to the risks already discussed, they mentioned other risks:

- cost tradeoffs between sole and multiple sources
- production quality
- not owning technical drawings
- ability to transition from first article test to production
- ability to manufacture, including tooling and personnel skills.

While the commodity councils recognize these risks, they do not mitigate them directly. The focus of the commodity councils remains with managing contracts. The commodity councils are aware of risk but have no systematic method for identifying, assessing, and mitigating risks other than contractual risk.³

³ The commodity councils use an eight-step process to develop their strategy for managing suppliers. This process has several steps that address risk, but these are limited in scope and require training to execute. For a more detailed explanation, see Appendix D.
We Developed a Risk Assessment Questionnaire and Obtained Selected Feedback

- Subject-matter experts were asked to:
  - List prevalent risks they considered
  - Review supply chain risks reported in business literature and rate how they applied to the Air Force
  - Rating scale:
    - 1 never considered
    - 2 rarely considered
    - 3 considered half the time
    - 4 often considered
    - 5 always considered (high-risk)

- Risks were grouped by risk category:
  - Environmental
  - Supplier
  - Demand
  - Inbound and outbound distribution
  - Internal (business risk)

Following our initial interviews, we developed and circulated among commodity council members a risk assessment questionnaire. The survey listed the prevalent supply chain risks reported in the business literature (see Appendix E) and asked Air Force personnel to rate these risks on a five-point scale and to categorize them in one of five groups. Many common risks are considered nearly always, while others are hardly ever considered. At each ALC, we identified and administered the survey to the one person, typically the head of the Acquisition Center of Excellence, who had the most knowledge on the process.4

---

4 Not all respondents agreed on the rating for every risk category. However, only a handful of categories generated responses that were opposed in the magnitude of the risk assessment. For example, one rater thought it was a 5, while the others considered it a 1. To obtain an overall rating, we combine the responses and take the maximum of the average and the mode for each risk. The effect biases the combined response toward higher risk concerns. For example, a risk rated 1, 1, and 5 would generate a combined rating of 2 (max of average and mode), while a risk rated 1, 5, and 5 would generate a risk rating of 5. This approach provides a “best case” for the ratings of which risks are considered by the Air Force.
Commodity council representatives said they consider only a relatively small number of risks often or always. These are listed in the chart above and cross the categories of environmental risks, demand risks, supplier risks, and internal risks. Note that respondents did not consider distribution risks "often" or "always," and they considered only one environmental risk (certification) "often." They also did not include environmental risks, such as bankruptcy, labor issues, and barriers to entry, “often” or “always.”

---

Note: No inbound/outbound distribution risks are considered always or often

---

5 “Environmental risk is the risk associated with external and, from the company’s perspective, uncontrollable events. The risks can impact the company directly or through its suppliers and customers.” See LCP Consulting in conjunction with the Centre for Logistics and Supply Chain Management, 2003.
Several risks were considered about half the time by commodity council personnel. Many of the risks listed above are identified as supplier risks in the business literature. These include long cycle times, poor training of the supplier’s personnel, and insufficient equipment and personnel at supplier facilities. Some of the risks identified above are portions of more general risks considered more often. For example, supplier quality was considered all the time, but lack of training of the supplier’s work force was only considered when it is relevant, i.e., when it was the identified cause of poor quality.

Among “demand” risks considered half the time were demand shortfalls, expedited jobs, and poor communication of job requirements or specifications. These risks are generated by the inherent uncertainty of the maintenance and repair environment. It is often difficult to predict drops or surges in demand. Because of this unpredictability, these risks were often considered to be beyond the control of the council. Improved modeling of demand, smoothing of demand by ordering more often, and writing of more flexible contracts with suppliers are possible ways to mitigate these risks.

Among “environmental” risks considered half the time were government restrictions or regulations, uncertain demand, diminishing competition, and obsolescence. These risks were the most mentioned environmental concerns and relate to the business environment rather than natural disasters, acts of God, acts of war, or other force majeure risks.
Risks mentioned about half the time that are internal to the Air Force included poor forecasting, inadequate availability of resources, and the number and experience of Air Force personnel. “Resources” need not be internal to the Air Force to pose an internal risk to it. For example, inadequate availability of Defense Contract Management Agency (DCMA) resources can pose an internal risk for the Air Force because the Air Force relies on DCMA resources to track quality of finished goods at manufacturing and repair facilities, and to monitor the implementation of corrective actions when quality problems are identified.
The list of risks that were rarely or never considered is instructive. It is not surprising to see that many environmental risks created by exposure to natural disasters were not considered if Air Force personnel believe that force majeure leaves them with little leverage or control over these risks. This may also be explained by lack of knowledge of the extent of risk exposure. Many of the events listed above are not common, but they could be catastrophic. Even if the Air Force cannot influence the probability of these or similar events, it can take steps to reduce their impact.
Other risks rarely or never considered fall within the categories of business environment, market environment, and technological uncertainty. While some risks listed here are not likely to be directly relevant to the Air Force (e.g., taxes, low profitability, currency devaluation), many others, such as issues related to labor, profitability, and technology, are relevant strategic supply chain risks.

### Some Other Environmental Risks Are Also Rarely or Never Considered

<table>
<thead>
<tr>
<th><strong>Business environment</strong></th>
<th><strong>Market environment</strong></th>
<th><strong>Technological uncertainty</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Government actions</td>
<td>Uncertain currency rates</td>
<td>Overall availability</td>
</tr>
<tr>
<td>–Taxes/tariffs</td>
<td>Entry barriers</td>
<td>Pace of change</td>
</tr>
<tr>
<td>–Customs</td>
<td>Specific assets</td>
<td>Direction of change</td>
</tr>
<tr>
<td>–Currency devaluations</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Lawsuits</strong></td>
<td><strong>Low profitability</strong></td>
<td></td>
</tr>
<tr>
<td>–Environmental</td>
<td>Geographic concentration of suppliers</td>
<td></td>
</tr>
<tr>
<td>–Health and safety</td>
<td></td>
<td></td>
</tr>
<tr>
<td>–Intellectual property</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Economic recessions/depressions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Labor</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>–Availability/shortages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>–Quality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>–Cost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>–Unrest</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Strikes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Work slowdowns</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Political unrest/instability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>–Boycotts</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>In the table:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Business environment</td>
</tr>
<tr>
<td>Government actions</td>
</tr>
<tr>
<td>–Taxes/tariffs</td>
</tr>
<tr>
<td>–Customs</td>
</tr>
<tr>
<td>–Currency devaluations</td>
</tr>
<tr>
<td>Lawsuits</td>
</tr>
<tr>
<td>–Environmental</td>
</tr>
<tr>
<td>–Health and safety</td>
</tr>
<tr>
<td>–Intellectual property</td>
</tr>
<tr>
<td>Economic recessions/depressions</td>
</tr>
<tr>
<td>Labor</td>
</tr>
<tr>
<td>–Availability/shortages</td>
</tr>
<tr>
<td>–Quality</td>
</tr>
<tr>
<td>–Cost</td>
</tr>
<tr>
<td>–Unrest</td>
</tr>
<tr>
<td>Strikes</td>
</tr>
<tr>
<td>Work slowdowns</td>
</tr>
<tr>
<td>Political unrest/instability</td>
</tr>
<tr>
<td>–Boycotts</td>
</tr>
</tbody>
</table>
Commodity council personnel reported rarely or never considering many “supplier” risks. Many of these risks reflect specific issues that require a considerable amount of knowledge about the supply base—for example, an ability to assess a supplier’s capability to sustain operations during a downturn in demand, its ability to maintain equipment, and its financial strength. Assessing these risks and their impact on the Air Force would require deliberate investment in a supply chain risk assessment program.

The force majeure clause in prime vendors’ contracts absolves them from most of these risks.
All our questionnaires indicated that distribution risks were rarely or never considered. One possible reason for this may be that many of these risks cut across the DoD and are perceived to be out of the scope of control of the commodity councils. These are higher-level risks that may not be specific to a supplier. Yet the Air Force should also evaluate these risks to determine its exposure regarding a particular supplier or across a group of suppliers (such as that a distribution strike crippling movement of goods and services could pose).

The force majeure clause in prime vendors’ contracts absolves them from some of these risks.
Some prospective risks that were rarely or never considered stem from internal business risks that are not applicable to the Air Force—for example, impact on liability and value of the enterprise are not risks that necessarily concern a military branch. Nevertheless, these risks are applicable to the Air Force’s prime contractors, so the Air Force needs to be aware of them and make sure that its prime contractors are managing them when they are relevant.

Other risks listed above, such as uniqueness of the item, knowledge of supplier costs, work scope creep, and program maturity, are relevant to the Air Force and would require a concerted effort to assess and mitigate.
In this section, we examine supply chain risks for two weapon systems. We selected the F-16 because it is a legacy system with a large inventory and sustainment managed organically by the Air Force. We selected the C-17 because its sustainment is managed under a PBL contract. As we noted earlier, the Air Force already outsources a large number of maintenance tasks and expects to outsource more. The Boeing Company manages C-17 maintenance under a multiyear contract. Because Boeing is also currently one of only two suppliers of large commercial aircraft (Airbus is the other), it has considerable influence within the aerospace industry. Consequently, the supply chain risk assessment and mitigation strategies it uses are likely to be good indicators of what is done across the aerospace industry and what the Air Force is likely to see from other aerospace contractors.

---

6 According to the U.S. Census Bureau (2008), sales of aircraft and aircraft engines to DoD were less than half of total industry sales minus National Aeronautics and Space Administration (NASA) sales (i.e., commercial sales) through 2003. Recently, DoD sales have been slightly larger than half, but not by a wide margin (U.S. Census Bureau, 2008).
For this portion of the research, we spoke with representatives of the F-16 sustainment organization and of Boeing’s C-17 PBL management office. We also visited the C-17 sustainment wing in Warner Robins, Georgia, and spoke to representatives there about C-17 sustainment activities and their relationship with Boeing. We interviewed DLA representatives by phone. We used the interview protocol shown in Appendix A as a guide for our discussion; we did not strictly adhere to the question format if it was not relevant to the interviewees. The interviews helped us answer the following questions about F-16 and C-17 SCRM:

1. Is there a clearly discernible SCRM process?
2. Which supply chain risks are considered, and how are they prioritized?
3. What are some of the factors that may impede a robust SCRM process?

The table above summarizes the findings resulting from our interviews of the F-16 and the C-17 weapon system sustainment groups. The table also includes our findings from interviews with DLA. We will first discuss our findings from our F-16 and C-17 interviews, then discuss our interviews with DLA later in the text.

### F-16 Supply Chain Risk Management

The F-16 sustainment group relies on the organic depots, ALC inventory management, and DLA to supply the parts and services needed to maintain the F-16 fleet. The depots repair items such as engines, landing gear, and avionics. The depots also provide periodic inspections and overhaul of aircraft to maintain or extend their operational life. The inventory of parts used on
an F-16 is managed by either the Air Force or DLA, depending on the part. The ALCs develop supply strategies and purchase repair services from outside suppliers. They also manage repairs performed by depots and by outside contractors. DLA manages contracts with commercial sources of supply and procures the inventory of spare parts (both depot-level reparable spares and consumables used in the overhaul and repair). These primary suppliers in turn each deal with a supply chain of their own. Under this arrangement, the F-16’s supply chain risks can be effectively managed if one assumes that each stakeholder will adequately manage the supply chain risks associated with its own operation, that all risks are known to all key stakeholders, and that the assessment and priority given to risk mitigation is focused on improving the reliability of the F-16’s supply chain. If any of these assumptions are false, then supply chain risk for the F-16 is ineffective. In other words, multiple organizations involved in managing supply chain risks may not have the same incentives or priorities for doing so. Later, for example, we will discuss how DLA is concerned about excess inventory and is willing to increase the risk of not having a low-demand part available, while the Air Force is willing to pay the cost for holding slow-moving inventory if it reduces the risk of stock outages.

**SCRM Process**

The F-16 sustainment branch participates in quarterly Integrated Process Team (IPT) meetings to discuss concerns and issues with F-16 sustainment. However, there are no IPTs specifically discussing supply chain risks. The F-16 team works with suppliers to develop and maintain supplier relations, but limitations on manpower availability and data at the sustainment-wing level restrict the amount of proactive SCRM that can take place.

**Risk Considered**

For the most part, SCRM is reactive; if an event such as a wildfire is threatening a supplier, Air Force managers will call the supplier to assess the level of threat. But we could discern no strategic level supply chain risk assessment or mitigation. The concerns at the wing level are with quality of the repair or manufacture, existence of a contract or financial arrangement to obtain the needed part, and delivery lead times. We saw very little evidence of a purposely designed and implemented SCRM process.

**Compounding Factors**

Implementing such a process at this level of the Air Force organizational structure is challenging. The sustainment wing does not have the personnel, training, or access to data needed to implement an SCRM process. It would also likely lack the leverage necessary to work with suppliers and change existing supply chain management processes at the supplier. There are two reasons for this. First, wing-level maintenance often does not have the volume of demand that can influence suppliers. Second, many supply decisions are made in the acquisition phase, meaning they cannot be easily changed in the sustainment phase.

**Boeing C-17 Supply Chain Management**

At the time of this research, the C-17 supply chain was managed by the Boeing Company, which served as the lead system integrator and was responsible for all decisions regarding C-17 sustainment. The performance expectations and compensation for Boeing’s role as the lead

---

7 This includes the Aircraft Sustainment Wing at the Ogden Air Logistics Center and the 416 Supply Chain Management Squadron.
system integrator were guided by a PBL contract between the Air Force and Boeing. Under this agreement, Boeing entered into contracts with the Air Force’s organic depots, commercial suppliers, and DLA. The effectiveness of the lead system integrator arrangement was judged by performance metrics. Boeing took full responsibility for supplier selection, inventory levels of all C-17 unique parts, and the distribution of parts. Boeing owns the demand history and the forecast method for the C-17 parts it manages. SCRM was conducted by Boeing and was based on its judgment and prioritization of risk. Data on system performance was managed and owned by Boeing. Boeing, and not the Air Force depot, had the direct relationships with the subtier suppliers. When we interviewed the C-17 sustainment wing at Warner Robins Air Force Base, it reported difficulties establishing relationships with Boeing’s subtier suppliers for the maintenance workloads that were under depot management.

**SCRM Process**

Because the PBL contract granted Boeing full responsibility over C-17 sustainment decisions, it also granted responsibility over SCRM. We interviewed members of Boeing’s C-17 Sustainment Support Team and asked how they conducted SCRM. We did not have visibility into the existence of a discrete process for assessing and mitigating the C-17’s supply chain risk. Boeing’s C-17 sustainment team indicated that they followed corporate guidelines for managing risk.

We also spoke with a Boeing corporate representative about supply chain management strategy. This representative reported that at the corporate level Boeing has a council on supply chain management across its major business units that reports to the CEO on supply chain matters. The council meets monthly and issues guidance on supplier selection and management. Supply chain risk is managed at the applicable program or business division level and is implicitly part of the supplier performance reports.

**Risk Considered**

Information about the supplier, including financial performance, quality, capacity, and past performance on cost, timeliness, and quality, is obtained and reviewed periodically to inform a risk assessment. Performance along these dimensions is tracked over time to provide an early indication of a problem. Suppliers are segregated by their strategic importance. Targets for key performance metrics vary by supplier. Risks are assessed as part of supplier selection and the ongoing supplier management process.

Boeing’s supplier selection process focuses on product quality and the company’s financial position. Boeing verifies that the supplier is ISO-certified and is technically capable of doing the work required; such certification indicates the supplier’s ability to deliver a quality product. Boeing also examines the supplier’s financial risk; if it is deemed to be high, then the supplier is critical. The supplier’s financial performance is tracked monthly or quarterly.

Once the supplier is selected, Boeing stresses the quality and timeliness of supplier performance. For example, Boeing looks at the number of parts returned to a supplier because of a quality deficiency or discrepancy. Boeing looks at turnaround times for repairs and manufacturing lead times. Supplier performance in quality and timeliness are aggregated across business units and reported enterprise-wide. Boeing’s defense unit (known as Boeing Integrated

---

8 Where possible, Boeing manages by commodity groups, such as aluminum goods used in both commercial and military applications, with supplier performance tracked at the corporate level.
Defense Systems at the time of our research, and later renamed to Boeing Defense, Space, and Security) knows how suppliers are performing on its commercial airplane contracts.

**Compounding Factors**

Boeing expects suppliers to be ISO-certified and assumes that they have business continuity plans in place in case of a disaster leading to work interruption. It does not ask to see or certify the business continuity plans. When we asked why Boeing does not put more emphasis on this risk, Boeing representatives responded that while they are concerned with work interruptions, they will work with suppliers to minimize their impact. If the work interruption was caused by a natural disaster, the force majeure clause in most contracts would exempt the supplier and Boeing from financial responsibility. This was an insurance policy against unpredictable events for which Boeing did not have to insure against.

The C-17 Sustainment office could not point to a product or report covering C-17 SCRM. We conclude, based on other interviews, that Boeing does have an SCRM process, but that it is not described or implemented as a separate process and instead rather integrated into other processes such as supplier selection and management. Information about the performance of key suppliers is reported to the upper levels of management. When necessary, Boeing has on-site representation at the supplier facility to oversee supplier performance.

Next we discuss our interviews with DLA personnel.
DLA’s sustainment role varies by weapon-system support relationship. If weapon-system sustainment is managed by the Air Force (i.e., the ALCs and the depots), then DLA has a substantial role. Its role in the management of weapon systems such as the C-17, which are under sustainment contracts, is far less. For organically managed systems, DLA manages tens of thousands of parts from many vendors, and the Air Force is generally required to use its services. DLA also manages a few thousand parts for the C-17, parts that are common to other weapon systems, but Boeing is under no obligation to use DLA to help store or manage these parts for the C-17 and reported that it does not do so. Altogether, DLA manages nearly 5 million items, providing nearly 100 percent of consumable items and 84 percent of all spare parts. Because DLA policies have a major impact on sustainment activities, it is important to understand how DLA manages supply chain risk.
DLA Risk Management Focuses on Inventory and Cost Reduction

- DLA has unilateral decision making power over DLA-managed, non-service-coded weapon system parts
- Risk is perceived in terms of inventory management
  - DLA concerned with reducing
    - Size of inventory footprint
    - Investment in inventory, particularly “low-demand” and “slow-moving” items
- Effort to reduce inventory driven by cost concerns—No evaluation of supply risk
  - DLA asked supply chain managers to review inventory levels for Air Force-coded weapon system national stock numbers with no demands for the past three years

SOURCE: Interviews with DLA headquarters and Defense Supply Center, Richmond, personnel.

From conversations with DLA personnel from the Defense Supply Center, Richmond (DSCR), we learned that DLA’s risk management is focused on managing excess inventory and reducing costs. DLA is concerned with reducing the size of the inventory footprint (i.e., the volume and floor space inventory occupies in a warehouse) and the investment in inventory particularly for “low-demand” and “slow-moving” items. Because DLA has unilateral decisionmaking power over DLA-managed parts for which the services have not requested a specific inventory level for a specific weapon system, it can take actions that impact the Air Force’s ability to sustain a weapon system without informing the Air Force beforehand.9

In addition, inventory levels of parts managed by the services but warehoused by DLA are also under review. DLA recently requested that the services review the inventory levels of service-coded national stock numbers with no demands in the past three years. Not having a demand in three years is common for many weapon system parts. Components with low failure rates may not have a demand in many years. It is difficult to predict which “low failure rate” part will fail next. However, if the part is not in stock when needed, the lead time and expense required to obtain the part from an outside supplier could be considerable. At the same

---

9 DLA is required to meet performance goals, such as 85 percent supply availability, but there are no penalties other than to its metrics if DLA does not meet its performance goals. It provides a very broad range of goods. Consequently, it can manage its performance metrics by providing high availability on very cheap items, such as nuts, washers, and screws, and lower availability on expensive critical weapon system parts. Thus, DLA can reduce inventory on expensive, high-volume weapon system parts and still maintain 85 percent availability. This has been the past experience of the services. See Chenoweth, Arkes, and Moore (2010) for DLA performance on Air Force weapon system items.
time, a reduction in the force structure for a weapon system could fully justify reducing the inventory of slow-moving parts. In other words, any policy to reduce cost and inventory, while often warranted, should consider all the costs and risks involved.
We conclude with a summary of our findings, their implications, and our recommendations.
Air Force Currently Takes a Limited Approach to Sustainment SCRM

• No identified process for comprehensive SCRM at the weapon system level

• Commodity councils have a process for SCRM, but lack experience in risk management and many risks are not considered
  – Risks considered mirror those listed in DoD sustainment guidance

In summary, we identified some DoD and Air Force guidance related to supply chain risks. The guidance does not incorporate many of the supply chain risks identified in the best-practice literature. We did not identify a comprehensive SCRM process for the F-16, suggesting that Air Force organic weapon support may more generally lack such processes. Boeing management of C-17 sustainment has some SCRM elements emerging from its corporate supply chain management policy, but it was not clear that this policy was used to identify supply chain risks beyond those relating to financial, quality, or timeliness risks. The Air Force’s commodity councils have an eight-step process that some members pointed to as their way of managing supply chain risk, but this process is geared toward managing contract risk. At the same time, the eight-step process could be expanded to focus on supply chain risk as part of a broader supplier relationship management policy. Further, the shift to PBL has been shifting sustainment management, including SCRM, to suppliers.
In the course of this study, we asked leading firms how they were organized to manage supply chain risks. The structures varied, but the companies that had a more clearly defined supply chain risk program also had a small organization (four or five people) that helped coordinate supply chain risk activities across business units and up to the corporate headquarters.

We envision a similar organization for the Air Force. This organization would communicate supply chain risk vulnerabilities to Air Force leadership and monitor and help Air Force commodity councils and sustainment wings react to supply chain risks both strategically and tactically. It would also establish SCRM policy and provide guidance to manage Air Force interactions with external and DoD suppliers (including DLA). The role and scope of this organization would need to be clearly defined, but it should provide an enterprise view of supply chain risks and help mitigate risks across weapon systems. This organization should

- set policy on how to manage supply chain risk under both organic and contractor-managed sustainment
- develop standard processes and metrics for risk management, including setting expectations for business continuity plans and time to recovery metrics
- expand the types of risks managed
- develop tools for risk assessment, including, for example, sense-and-respond processes to monitor disruptions and initiate contingency plans
- provide effective training in risk identification, assessment, and management
- establish metrics and incentives.

**An Enterprise-Wide SCRM Organization Would Ensure Integrity of SCRM Across the Air Force**

- Set policy and provide guidance for sustainment
  - Organic management
  - Contractor support (e.g., PBL, contractor logistics support)
- Develop standard processes
  - Require key suppliers
    - Develop business continuity plans
    - Commit to time to recovery
  - Expand types of risks managed
- Develop tools for risk assessment
  - Sense and respond process to monitor disruptions and initiate contingency plans
- Provide effective training in risk assessment
- Establish metrics and incentives
The Air Force Materiel Command’s recent reorganization created an Air Force Life Cycle Management Center (AFLCMC) and an Air Force Sustainment Center (AFSC). This new structure consolidates product development and support system design under AFLCMC and integrates depot maintenance and Air Force supply chain activities under AFSC. Supply chain risk cuts across these areas. In this document, we do not explicitly address SCRM during acquisition, but we contend that many supply chain risks are common to acquisition and sustainment and are often shaped by decisions made during acquisition. At the time of this writing, the new structure is taking shape, but it is too early to determine how the Air Force intends to conduct SCRM or supplier relationship management. We recommend that the new organizational structure provide a mechanism to integrate supplier relationship management and SCRM across AFLCMC and AFSC.
Questions Remain Regarding the Scope and Responsibility for SCRM Implementation

• Scope?
  – Acquisition and/or sustainment
  – Sources of weapon system support (e.g., DLA, organic, and contractor for PBLs or contractor logistics support)

• Where?
  – Development of SCRM policy and guidance
  – Execution of enterprise-wide sustainment SCRM through commodity councils and supplier relationship management

Our analyses raise some SCRM implementation questions for Air Force leadership, which we explore in the second phase of this analysis.

The first of these is the focus of Air Force SCRM, particularly on whether it should include acquisition or be limited to sustainment, which has much less influence over suppliers.

The second is its extent, specifically whether it should include organic suppliers, DLA, and contractors for PBL and contractor logistics support, as well as standard contractors.

The third is the location of Air Force SCRM activities, both development of policy and guidance and execution of enterprise-wide sustainment SCRM through commodity councils and supplier relationship management efforts.

We explore these and other questions in examining the scope and responsibility for SCRM implementation in the second phase of our analysis.
This appendix presents the protocol used for our interviews with DoD and Air Force personnel involved with supply chain, contracting, and commodity management for the F-16, a legacy weapon system, which primarily has organic support and has transitioned from acquisition to sustainment, and the C-17, a newer system that is contractor-supported and is currently transitioning from acquisition to sustainment.

Background
RAND is conducting a study, entitled *Identifying and Managing Risks Associated with Agile Supply Chains*, sponsored by the Air Force Director of Transformation within Logistics, Installations and Mission Support. Its objective is to assist the Air Force with development of an enterprise-wide strategy for proactively managing sustainment support supply chain risks across the Air Force’s portfolio of weapon systems. The current study seeks to identify important weapon system sustainment supply chain risks the Air Force is managing, those it is not managing, and those it should manage for legacy or near-legacy systems.

The result of this RAND effort will be a briefing and RAND report. We do not intend to identify anyone we interview in our briefing or report other than general offices or industries. If we receive any figures or tables during our interviews that we would like to use in our reports, we will seek permission to use them and guidance on how to properly acknowledge the source.

**BACKGROUND**

1. What is the role of your office in the Air Force weapon system sustainment support supply chain?

2. For respondents supporting weapon system sustainment, please describe your supply chain, including
   a. The part(s) or system(s) you manage
   b. Your major upstream suppliers for 2.a.
      i. The major suppliers to these suppliers
   c. Your major downstream customers for 2.a.
      i. Customers of your major customers, if applicable
   d. The annual volume managed including quantity and value by source of supply
   e. Number of single source suppliers
82 Identifying and Managing Air Force Sustainment Supply Chain Risks

f. Number of Diminished Manufacturing Source (DMS)\(^1\) suppliers

**TYPES OF SUSTAINMENT SUPPLY CHAIN RISKS**

3. The attached table presents many typical types of risks associated with managing different types of supply chains in the commercial sector.
   a. Which of these risks are actively managed by your office (or by another office that you can provide)?
   b. Are there risks that your office manages that are not represented in the table?

4. For each of the risks identified in question 1, can you provide
   a. Air Force policy, directive, or other documentation about how the risk is or should be managed
   b. Data and/or analyses used in the assessment of that risk, its likelihood, duration, and impact on your sustainment supply chain
   c. Data and/or analyses of the ranking of the importance of the risk to the Air Force based on its likelihood of occurrence, duration, and impact
   d. Plans for avoidance, mitigation, or management of that risk, its frequency and actual impact on your supply chain

5. For each risk you did not identify as actively managing in question 2:
   a. Are you aware of any of the risks applying to your sustainment supply chain or to other Air Force or DoD sustainment supply chains? If so, can you tell us or point us to where we can learn what happened, when it happened, what was the duration and impact, and what was done to shorten its duration?
   b. Could any other risks apply to your sustainment supply chain?
      i. Yes/No?
      ii. If yes, how would it be managed? (see question 2)

6. Using the attached graphic, the answer from 2.b., and the professional guidelines you use to perform your duties, which risks are most important to the Air Force and why are they important?
   a. Of these, what do you think is the likelihood of the risk to your sustainment supply chain?
      i. What is the likelihood of the risk to other Air Force or DoD sustainment supply chains?
   b. What do you think would be the impact of the risk to your sustainment supply chain?
      ii. What is the impact of the risk to other Air Force or DoD sustainment supply chains?

---

1 According to the DoD 4140.1-R, *DoD Supply Chain Materiel Management Regulation*, diminishing manufacturing sources and material shortages (DMSMS) is “the loss or impending loss of manufacturers of items or suppliers of items or raw materials may cause material shortages that endanger a weapon system’s or equipment’s development, production, or post-production support capability.” DMSMS directly impacts system readiness, system availability, and costs DoD hundreds of millions of dollars annually.
<table>
<thead>
<tr>
<th>Typical Supply Chain Risks</th>
<th>Does This Apply to the Air Force?</th>
<th>Is There a Plan to Prevent?</th>
<th>Plan ID</th>
<th>Date</th>
<th>Is There a Plan to Mitigate?</th>
<th>Plan ID</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shortage of supply</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Quality defects in manufactured product</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Diminishing source of manufacturing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Unplanned demand exceeds production/repair/transportation capacity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Price fluctuations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental: Natural or man made disasters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Distribution disruptions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Transportation network compromised</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Existing warehouse inaccessible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Production/repair capacity diminished</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- IT structure compromised</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Business sector shows signs of weakening (i.e., supplier failures on the rise)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Structural</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Single source suppliers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Diminishing manufacturing source suppliers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- No technical drawings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Funding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Underfunding supply requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PARTNERS IN SUSTAINMENT SUPPLY CHAIN RISKS

7. Which, if any, of the sustainment supply chain risks that you manage are affected by decisions made by someone else either earlier in the weapon system acquisition process or elsewhere in the sustainment supply chain?
   a. What were the decisions and how have they affected the risks you manage (e.g., the risk’s likelihood, duration, or impact or limited risk avoidance, mitigation, or contingency actions)?
   b. Are the risks that you manage in your sustainment supply chain affected by decisions or actions in the sustainment supply chain for other weapon systems (i.e., not the C-17 or F-16)?

8. What should we know about identifying, assessing, prioritizing, and managing sustainment supply chain risks in the Air Force that we have not asked you?
   a. Who else would you recommend we talk to about sustainment supply chain risks for your weapon system?
   b. Can you point us to data, tool, or Air Force and DoD literature to help us better understand how the Air Force is identifying, assessing, prioritizing, and managing its sustainment supply chains?
This appendix presents the protocol used for our interviews with industry personnel involved with SCRM.

Background
RAND, a non-profit corporation dedicated to objective analysis of important public policy questions, was asked by the U.S. Air Force to assess its ability to identify, evaluate, manage, and mitigate weapon system support supply chain risk. As part of this study, we are studying best commercial practices for supply chain risk management to learn the latest trends and corporate strategies for managing them. We are also interviewing Air Force personnel regarding how they identify supply chain risk, who is responsible for assessing and managing this risk, and how they mitigate supply chain risk.

RAND would like to understand how your company approaches supply chain risk management. Our project is particularly concerned with aftermarket supply chain risk.

QUESTIONS ON RISK MANAGEMENT

1. How did your company’s approach to supply chain risk management change after 9/11? Were there other events that had an impact on your company’s perception of supply chain risk management?
2. Which corporate areas conduct supply chain risk assessments (i.e., manufacturing, supplier relations, etc.)?
3. How are supply chain risk assessments and risk management strategies communicated throughout the enterprise? How often?
4. Is there a single organization for managing supply chain risks? Where does this organization fit in the org chart?
5. How is supply chain risk management organized?
   a. What type of experience and skills are required by your company to work in supply chain risk management?
   b. Are employees working in the supply chain risk organization promoted to other units within your company, or is this seen as a career position?
   c. What is the average tenure of someone working in this area?
   d. How many employees are directly involved in management of supply chain risk?
   e. Are these employees fully dedicated to this function or do they share their risk responsibility with other tasks?
f. What is the function of the supply chain risk management organization, i.e., does it facilitate, oversee, audit, or control supply chain risk management at your company?

6. How often is supply chain risk assessed? Does this vary by commodity or product?

7. Does your company have a written process for conducting supply chain risk assessments?

8. When assessing a supplier, what types of risks is your company concerned with?

9. Does your company start assessing supply chain risk during the product design phase? If so when in product design?

10. Once a product moves from prototype development to production is there a change in the responsibility for management supply chain risk?

11. Is the board of directors briefed on supply chain risk?
APPENDIX C

Description of Department of Defense and Air Force Guidance on Acquisition and Supply Chain Risk

Defense Acquisition Guidebook (Defense Acquisition University, undated)

The Defense Acquisition Guidebook is a reference document to help acquisition professionals understand and apply the material in DoD Directive 5000.01 and DoD Instruction 5000.2. The section most relevant to supply chain risk management is in Chapter 4 of the handbook. Below, we briefly describe the chapters.

A. Chapter 1: “Department of Defense Decision Support Systems”
   This chapter describes the context of acquisition at the Department of Defense. It looks specifically at the Planning, Programming, Budgeting, and Execution process for setting up an acquisition; at the Joint Capabilities Integration and Development System regarding needs; and at the Defense Acquisition System regarding procurement.

B. Chapter 2: “Defense Acquisition Program Goals and Strategy”
   This chapter describes the purpose and process of formulating goals for acquisition, looking at the Joint Capabilities Integration, the Technology Development Strategy, and the Acquisition Strategy as stages of that process.

C. Chapter 3: “Affordability and Life-Cycle Resource Estimates”
   This chapter describes how to determine affordability over the life cycle of an acquisition program and how to satisfy DoD policy requirements in estimating and reporting those estimates of affordability.

D. Chapter 4: “Systems Engineering”
   This chapter explains systems engineering procedures and how to use them in the acquisition process. It examines questions of system design and gives direction for carrying out a Systems Engineering Plan. In discussing how systems engineering is implemented, section 4.2.3.5, “Risk Management,” describes the requirements and process of risk management in acquisitions.

E. Chapter 5: “Life-Cycle Logistics”
   This chapter describes life-cycle logistics (LCL) and how it operates within the processes of acquisition and sustainment. It discusses how LCL operates within Systems Engineering to improve reliability and to lower the “logistics footprint,” places priority on the use of PBL for product support, and describes the essential LCL activities in all the phases of a weapon system’s life cycle.
F. Chapter 6: “Human Systems Integration (HSI)”
This chapter focuses on how best to use personnel resources in the acquisition process. It discusses each area of HSI: manpower, personnel, training, human factors, safety and occupational health, personnel survivability, and habitability.

G. Chapter 7: “Acquiring Information Technology and National Security Systems”
This chapter describes the “network-centric strategy” used by DoD, examining the Global Information Grid (GIG), how to make programs operable across the GIG, how to make data accessible and useful (including across the electromagnetic spectrum), and how and when to use commercial solutions to achieve these goals.

H. Chapter 8: “Intelligence, Counterintelligence, and Security Support”
This chapter examines the unintended loss of military technology and strategy through “inadvertent technology transfer.” It describes prevention and protection strategies.

I. Chapter 9: Integrated Test and Evaluation
This chapter addresses the test and evaluation (T&E) phase. It describes how to develop a T&E strategy that will provide necessary information for furthering the acquisition process.

This chapter describes the timeline of decisions and reviews for which program managers are responsible.

K. Chapter 11: “Program Management Activities”
This chapter describes the major management actions for which program managers are responsible. These include:

1. joint programs
2. international cooperation
3. integrated program management
4. earned value management
5. contract management reporting
6. risk management
7. knowledge-based acquisition
8. performance-based business environment
9. total life cycle systems management
10. integrated product and process development
11. technical representatives at contractor facilities
12. contractor councils
13. government property in the possession of contractors
14. integrated digital environment
15. simulation-based acquisition and modeling and simulation
16. independent expert review of software-intensive programs.
Risk Management Guide for DoD Acquisition (Department of Defense, 2006)

This guide gives specific directions for managing risk to program managers. It defines a risk event as having three distinct elements: a future root cause, the probability of that cause occurring, and the consequence or impact of the event. The guide emphasizes plans for risk mitigation and implementing those plans rather than simply relying on strategies to avoid risk. This is especially evident in its emphasis on future root causes. By describing how the chance of a risk occurring depends on the chance of the root cause, the focus shifts from simple attempts to minimize impact to more comprehensive efforts to understand and avoid the causes. The guide distinguishes between managing risks and issues: risks are future events with future consequences, whereas issues are current problems. Risk management thus involves the mitigation of possible future events, not solving current problems.

Acquisition and Sustainment Life Cycle Management
(Air Force Instruction 63-101, 2009)

This document establishes the integrated lifecycle management guidelines, policies, and procedures to be applied by Air Force personnel in managing systems and subsystems procured under DoD’s 5000.2 series directive. While this document does not mention sustainment risk explicitly, it lays out a requirement to manage and measure program life-cycle performance. This document attempts to integrate the acquisition and sustainment early in the life cycle of a program. Section 3.13 discusses the need to establish metrics to measure sustainment performance but gives no specific direction on assessing supply chain risk.


This guide provides the required procedures for managing DoD materiel. It defines and describes the supply chain, planning for materiel, the sourcing and acquisition of materiel, materiel production and maintenance, materiel delivery and return, technology that supports these processes, and logistics programs and systems that support these processes. It addresses but does not discuss in any detail the following risks: the proximate causes for the risk of an item being out of stock, draw-down of the stockpile, reducing the risk of shelf-life expiration, financial risks that may be associated with life-cycle support, exceeding repair cycle time, exceeding order and shipping time, exceeding the maintenance replacement rate, resupply from external sources, and security risks associated with particular weapons system categories.

USAF Deficiency Reporting, Investigation, and Resolution (TO 00-35D-54; Secretary of the Air Force, 2011)

This technical order implements the guidance of AFI 63-501, The Air Force Acquisition Quality Program. Its purpose is to establish product deficiency reporting procedures that will allow
the Air Force to track and correct product quality deficiencies before they adversely impact operational safety, suitability, or effectiveness (OSS&E). Table 1.1 of the technical order lists attributes that may impact OSS&E, including quality, reliability, maintainability, and logistics supportability. The deficiency reporting information system is a repository of deficiency reports that could be mined to reveal supply chain risks. The user reporting the deficiency must categorize the severity of the impact to OSS&E; Category I deficiencies are most serious and could lead to critical failures and loss of life. Table 1.2 describes the categories of deficiency severities.
Commodity Councils Manage Supply Chain Risk Within Their Eight-Step Process

**Step 1. Review Current Strategy:** Conduct analysis and research to understand how the commodity is fulfilled today to include: spend and forecast analysis, supplier analysis for current suppliers, inventory position and strategy, customer feedback, barriers and impediments, etc.

**Step 2. Evaluate/Assess Current Market:** Analyze market to assess trends, emerging or diminishing technologies, and suppliers. All associated tasks to be led by the Market Research Analyst in conjunction with the Central Market Research Team.

**Step 3. Analyze and Forecast Demands:** The goal of this step is to develop a validated supply plan detail and summary based on forecasted requirements from D200 and including additional concerns from customer input, engineering configuration, spend/forecast variances, supplier capabilities/capacities, and recent developments.

**Step 4. Create Future Strategy:** In this step, information from the discovery phase (Steps 1–3) is synthesized to develop potential strategies for the Material Governance Board to consider and approve in Step 5. The output from this step is a Commodity Management Plan (CMP) with recommendations for subcouncils and potential spiral strategies the council/subcouncils will pursue. Inputs to this step include existing inventory levels and material management and logistics plans. Outputs include key performance indicators and estimates on return on investment. Examples of return on investment include reduced cycle times or
improved quality. These outputs also include potential contracting strategies, key milestones, potential barriers, and mitigation plans. The process steps for Step 4 are accomplished at a high level for the CMP, and with greater detail in the Commodity Acquisition Management Plan (CAMP).

Step 5. Approve Strategy: The Material Governance Board considers CMP and CAMP documents and approves the commodity plan.

Step 6. Establish Contractual Instruments: This step includes the preparation and approval of a performance-based agreement, preparation of a source selection plan (for competitive contracts), and issuing of a request for proposal.

Step 7. Rollout Strategy: Develop the rules of engagement for the execution of the commodity/supplier strategy. This includes setting up a data gathering plan to track performance and issuing a user’s guide on how to place items on contract and award orders.

Step 8. Monitor and Continuously Improve Strategy and Performance: This step consists of 26 substeps leading to the generation of a variety of reports on compliance and performance. These reports are reviewed by the Materiel Governance Board and used to adjust the commodity strategy and improve supplier performance.
A risk assessment is prescribed under two of the steps. First, Substep 2.4 directs commodity councils to review the supplier’s capacity and capabilities. This is related to the supplier’s ability to meet the demand requirements for the commodity. Technological capability is also considered. The second place risk is considered is in Substep 4.6, which calls for a risk assessment of the proposed commodity council purchasing strategy, including risk of meeting the desired goals.

Certainly, many of the other steps detailed in the eight-step process are related to risk assessment. For example, Step 2 calls for a market analysis to assess trends, emerging and diminishing technologies and suppliers, etc. Step 2.1.2 calls for the commodity council to obtain industry research reports, including supplier financial data, watchdog reports, and publicly filed reports.
While the commodity councils’ members were aware of supply chain risks and sensitive to the issue, we do not see evidence of an integrated and systematic process for identifying, assessing, or mitigating supply chain risks. We believe the lack of an integrated approach is due to the commodity councils’ emphasis on contracts. However, it is also due to a lack of training on how to conduct a risk assessment and a belief that the commodity councils do not have enough leverage to change policy or influence supplier behavior. This leads to a narrowly focused approach to supply chain risk management.\(^1\)

\(^1\) Findings based on conversation with commodity council lead.
This appendix lists all the risks that were included in our risk questionnaire. Survey participants were asked to rank the frequency with which they considered each risk. The results of the survey are presented in the body of this document.

<table>
<thead>
<tr>
<th>Type of Risk</th>
<th>Frequency with which you consider this risk: 1 = never, 2 = rarely, 3 = half the time, 4 = often, 5 = always</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental risk</td>
<td></td>
</tr>
<tr>
<td>Natural disasters</td>
<td></td>
</tr>
<tr>
<td>Weather</td>
<td></td>
</tr>
<tr>
<td>Hurricanes</td>
<td></td>
</tr>
<tr>
<td>Tornados/cyclones</td>
<td></td>
</tr>
<tr>
<td>Blizzards/hailstorms/lightning</td>
<td></td>
</tr>
<tr>
<td>Floods/mudslides</td>
<td></td>
</tr>
<tr>
<td>Droughts</td>
<td></td>
</tr>
<tr>
<td>Earthquakes</td>
<td></td>
</tr>
<tr>
<td>Tsunamis</td>
<td></td>
</tr>
<tr>
<td>Volcanoes</td>
<td></td>
</tr>
<tr>
<td>Rogue waves</td>
<td></td>
</tr>
<tr>
<td>Epidemics</td>
<td></td>
</tr>
<tr>
<td>Infestations</td>
<td></td>
</tr>
<tr>
<td>Terrorist/sabotage</td>
<td></td>
</tr>
<tr>
<td>Bombings</td>
<td></td>
</tr>
<tr>
<td>Chemical/biological release</td>
<td></td>
</tr>
<tr>
<td>Blockades</td>
<td></td>
</tr>
<tr>
<td>Product tampering</td>
<td></td>
</tr>
<tr>
<td>Electronic intrusions</td>
<td></td>
</tr>
<tr>
<td>Viruses</td>
<td></td>
</tr>
<tr>
<td>Worms</td>
<td></td>
</tr>
</tbody>
</table>
Trojan horses
Denial of service
Property theft
  Physical
  Intellectual
Business environment
  Government actions
    Taxes/tariffs
    Regulations
    Customs
    Currency devaluations
Lawsuits
  Environmental
  Health and safety
  Intellectual property
Economic recessions/depressions
Labor
  Availability/shortages
  Quality
  Cost
  Unrest
Strikes
  Work slowdowns
  Political unrest/instability
  Boycotts
Market environment
  Capacity constraints
  Unstable prices
  Uncertain currency rates
  Little or no competition
Entry barriers
  Capital requirements
  Specific assets
Categories of Supply Chain Risks

Proprietary (i.e., patents)
Design
Processes
Low profitability
Certification/qualification
Raw materials
Availability
Cost trends
Geographic concentration of suppliers

Acts of War
Bombings
Blockades
Accidents
Fires
Explosions
Structural failures
Hazardous spills

Technological uncertainty
Overall availability
Obsolescence
Pace of change
Direction of change

Demand uncertainty/volatility
Surges
Shortfalls
Expedited jobs
Poor customer requirements/specifications
Product configuration changes
Changes in fleet life cycle (longer or shorter)

Supplier risks
Bankruptcy/financial failure
Withdrawal from the market
Inability to sustain during a downturn
Utilize slack
Reserve funds

Inadequate contingency/risk management planning

Poor quality/rework
- Failure to maintain equipment
- Lack of training/knowledge in principles and techniques

Constrained volume capacity
- Equipment, personnel, or facilities

Excess capacity
- Equipment, personnel, or facilities

Inflexible mix (i.e., production) capability

Shortage of inputs (materials and services)
- Poor forecasting
  - Long and/or variable purchasing cycle times

Long lead/order cycle times – unresponsive
- Backlogs

Variable lead/order cycle times – unreliable

Inability to control/reduce costs

Unwillingness/inability to continually improve

High management/personnel turnover

Slow adoption of technological changes

Incompatible information systems

Dependency on buyer, one, or a few large customers

Intellectual property theft

Critical technology disclosure (i.e., International Traffic in Army Regulations)

Downstream integration/direct competition

Substituting harmful/inferior/patent-violating materials or parts

Illegal/poor labor/environmental practices

Poor quality internal and external information flow

Inflating purchase costs

Opaque processes

Practices that threaten viability of key upstream suppliers

Opportunistic behavior

Security requirements/clearance for facilities/personnel

Certification (e.g., Federal Aviation Association)
Transition to new supplier (time, cost, quality)

Inbound and outbound distribution

Constraints

Infrastructure
  Ports
  Roads
  Rail
  Air

Assets
  Cargo aircraft
  Container ships
  Locomotives/rail cars
  Chassis
  Containers

Labor
  Truck Drivers
  Rail operators
  Longshoremen
  Pilots

Long distances
Longer lead times
Increased chance of disruption
Damage in transit
Many touch points

Security
  Theft
  Terrorism/tampering

Damage in transit
  Increased costs
  Incompatible information technology

Internal risks

Personnel
  Numbers and experience
Knowledge and skills

Design
  Lack of technological drawings/verification (product model/configuration) modifications

Complexity
  Validity of data

Manufacturability

Value to the enterprise
  Impact on customer satisfaction/loyalty
  Impact on liability
  Impact on costs/profits

Value to final product/application
  Customer demand
  Uniqueness
  Substitutability
  Systems integration

Availability of organic facilities

Plant breakdowns/mechanical failures

Reliability of test equipment

Inventory obsolescence

Forecast reliability/schedule availability

Knowledge of supplier costs

Defense Contract Management Agency availability

Work scope/plan creep

Competition/bid process

Poor communication
  Suppliers
  Customers

Acquisition strategy

Program maturity

Integration testing

Flight tests
  Qualifications
  Schedule

Funding availability

Subcontracting agreement
Bibliography

AFI—See Air Force Instruction.

http://www.fas.org/irp/doddir/usaf/afdd2.pdf


Chenoweth, Mary E., Jeremy Arkes, and Nancy Y. Moore, Best Practices in Developing Proactive Supply Strategies for Air Force Low-Demand Service Parts, Santa Monica, Calif.: RAND Corporation, MG-858-AF, 2010. As of June 24, 2012:
http://www.rand.org/pubs/monographs/MG858


Council of Supply Chain Management Professionals, “CSCMP Supply Chain Management Definitions,” undated. As of June 15, 2012:
http://cscmp.org/aboutcscmp/definitions.asp


Defense Acquisition University, Defense Acquisition Guidebook, undated. As of June 15, 2012:
https://acc.dau.mil/dag

Defense Federal Acquisition Regulation Supplement (DFARS), Part 201—Federal Acquisition Regulations System, Subpart 201.1—Purpose, Authority, Issuance, revised December 19, 2006. As of June 15, 2012:


DoDI—See Department of Defense Instruction.


GAO—See U.S. General Accounting Office.


http://www.uspto.gov/web/offices/ac/comp/proc/OMBmemo.pdf


LCP Consulting in conjunction with the Centre for Logistics and Supply Chain Management, Understanding Supply Chain Risk: A Self-Assessment Workbook, Bedford, UK: Cranfield University Centre for Logistics and Supply Chain Management, 2003.

http://is.njit.edu/pubs/delphibook/

http://www.economist.com/node/1378156


http://www.dodig.mil/Audit/reports/fy04/04-110.pdf

http://www.whitehouse.gov/sites/default/files/omb/assets/omb/circulars/a076/a76_incl_tech_correction.pdf


Identifying and Managing Air Force Sustainment Supply Chain Risks


http://www.ainonline.com/node/103396


http://www.wto.org/english/res_e/reser_e/wtr08_e.htm


