

How to fortify your supply chain through collaborative risk management*



*connectedthinking

Table of contents

The heart of the matter	2
Sharing risk information across the supply chain helps improve performance and reduce costs.	
<hr/>	
An in-depth discussion	4
Suppliers' new responsibilities in the supply chain require a new kind of coordinated risk management.	
Risk management must adapt to the new supply chain	5
Only coordinated action can mitigate interconnected risks	7
ITAR risks	13
New strategies can realize a major opportunity	15
<hr/>	
What this means for your business	20
Shared risk management can change the contractor/supplier relationship from transactional to strategic.	
Calculating risk	22
What is your framework?	23
What are your supply chain risks?	24
What do risks mean to your program?	26
How are you responding?	34
Is your response still effective?	36
Small steps yield big results	37

The heart of the matter

Sharing risk
information across the
supply chain helps
improve performance
and reduce costs.

“Radically changed” is the phrase that best describes the aerospace and defense supply chain today. Vertical integration has all but disappeared over the past 20 years, and the days when primes directly managed most of their suppliers are also gone. First- and second-tier suppliers now supervise a huge portion of subsystem integration, and, with it, a huge segment of the supply chain. Today, more than ever before, programs succeed or fail because of supply chain execution.

Many contractors have reaped financial and other rewards from the new supply chain model, but it has pushed current risk management systems past their limits. In recent years, the ineffective management of supply chain risks has caused cost overruns, production delays, quality failures, and program cancellations. And the increasing search for international partners and customers is creating ever more complicated risks.

Individual suppliers cannot respond to these risks alone, nor can the current processes and controls at prime contractors. Working in isolation, both primes and suppliers are blind to many emerging supply chain problems. As a result, they spend far too many program management resources addressing risks after they’ve blossomed into realized problems or even full-blown crises.

Successful companies are finding they can do better. By sharing risk information and developing coordinated risk responses, it is possible to minimize surprises and disruptions, improve program performance, and reduce costs. This is the key opportunity in program risk management today, around which three best practices are developing.

First, the number of program risk management participants is expanding to include more internal functions and more members of the supply chain. Programs can add lower-tier suppliers and a wider range of stakeholders into efforts to identify risk, understand it, respond to it, and then monitor the effectiveness of the response. Second, program executives are developing foresight by learning to recognize, interpret, and monitor the early warning signs of problems and changing risk profiles. Third, companies are changing their cultures. Training, new responsibilities, and new incentives for employees and suppliers weaken the “conspiracy of hope,” in which people avoid reporting risks until they have solutions, or see risks as someone else’s problem.

Executives can take action now. Opening communication lines, monitoring and reporting leading indicators, and clarifying roles, for example, all start with incremental adjustments. Over time, better risk identification and more comprehensive and efficient responses to risk produce a host of benefits. Penalty costs go down. Schedule and labor disruptions become less frequent. Rework shrinks. Return on invested capital grows. In other words, companies improve their track record of executing on budget, on time, and on spec. All of these add up to more programs won and fewer lost.

An in-depth discussion

Suppliers' new responsibilities in the supply chain require a new kind of coordinated risk management.

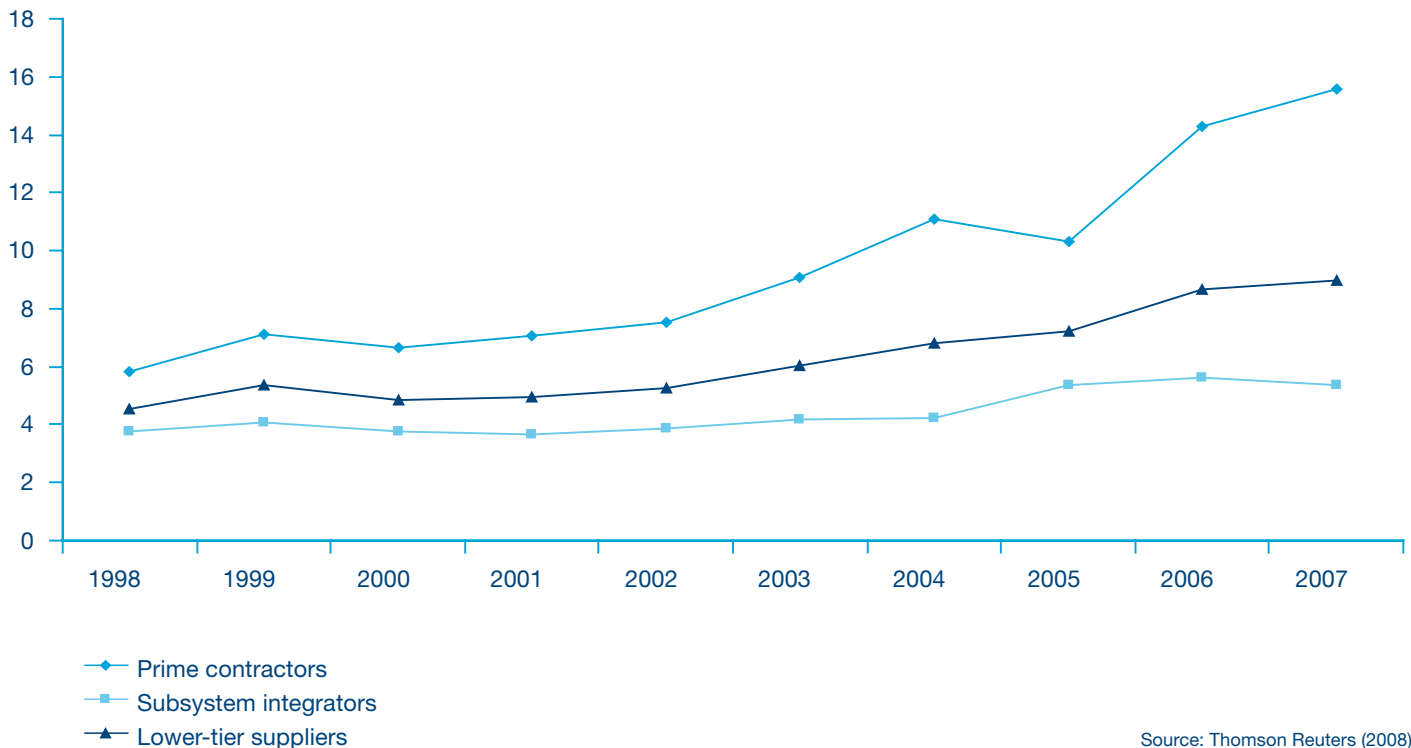
Risk management must adapt to the new supply chain

Four connected trends radically reshaped the aerospace and defense supply chain over the last 20 years.

First, outsourcing rose dramatically. Not long ago, prime contractors manufactured roughly 80 percent of deliverables in-house and outsourced 20 percent of production. Today, those percentages are reversed. Second, aerospace and defense companies pursued growth in foreign markets. Third, primes and governments reduced their number of direct suppliers. Finally, primes shifted costs and responsibilities to subsystem integrators and other suppliers.

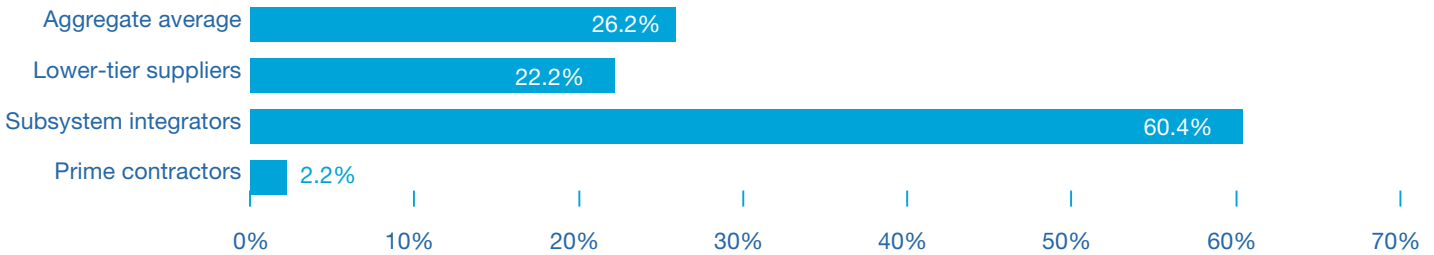
For primes, the payoff is clear. Ten years ago, they generated inventory turnover six times a year. Now the turnover is nearly 16 times a year. (See Figure 1.) Over the same ten years, primes increased their average margin and return on invested capital by 8 percent.¹

Figure 1. Inventory turnover: the number of times inventory is sold and replaced



In the supply chain, mid- and second-tier members took on more inventory and employees in order to develop new competencies, particularly for subsystem integration. Since 1998, staffing levels have grown only 2 percent at primes while the industry as a whole has increased staff by an average of 26.2 percent. (See Figure 2.)

Figure 2. Percent change in aerospace and defense employees, 1998 to 2007



Source: Thomson Reuters (2008)

Suppliers' new responsibilities and investments carry new program execution risks. These require a different kind of supply chain risk management than companies practiced in the past. As Dan Pleshko, Chief Supply Chain Officer at Goodrich, says, "We've moved up the value chain and the integration chain in the types of products and services we offer to customers. In doing so, we've moved from a purchasing/standard-procurement style to helping our supply base manage its outsourced operations. That's a major skill shift in people and core competencies, which brought new risks into play. Four types of risk came to light quickly. First, commodity pricing fluctuation. Before, we purchased many components and commodities directly. Now, that activity might be two to three steps removed from us. Second was supply chain capacity. How are suppliers ensuring they have capacity in place at the right time with the right technology? Third was supply chain interruption, which really includes all supply chain elements, such as logistics, administrative issues, and duties and customs. Fourth and last was political risk. As we entered different emerging economies to find a lower cost structure, we became susceptible to different kinds of political risk."

Companies that do not adapt to these new operating conditions can expect more severe and frequent cost overruns, schedule delays, and quality failures. According to testimony by the US Government Accountability Office (GAO) before the US Senate Armed Services Committee in June 2008 (published under the title *Better Weapon Program Outcomes Require Discipline, Accountability, and Fundamental Changes in the Acquisition Environment*), US defense acquisition costs in 2007 were 26 percent (\$295 billion) above first estimates, more than quadruple the overage in 2000. The average scheduling delay also reached a high point of 21 months, compared with 16 months in 2000.²

Only coordinated action can mitigate interconnected risks

No one link in the supply chain has all the information necessary to identify and monitor risk comprehensively. Still, many contractors and suppliers try to leave each other alone to manage “their own” risks. As a result, they cannot see many risks that are emerging and changing. Instead, risks go unnoticed until realized, and the supply chain ultimately spends too many program management resources resolving the resulting problems and crises.

The need for better cooperation becomes even clearer when individual risks are considered. Below are some examples in the areas of financial, geopolitical, regulatory, and operational risk. These complex and interconnected risks require a coordinated response by multiple levels of the supply chain.

Financial risk

The expansion of costs and responsibilities in the supply chain has created new financial risks for which new evaluation methods are needed. According to Janice Davis, VP of Global Sourcing at Bombardier, the company has “always done standard financial-risk analyses of our suppliers. But it was the same stuff everyone does—what’s their debt to equity, how are they doing with their bank covenants, etc. Today it’s a whole new world. We recognize that yesterday’s best practices are not adequate, and at Bombardier we’re committed to building a better approach.”

By concentrating on what they perceive as “their own” risks, suppliers and primes can become blind to emerging risks across the supply chain.

If contractors want suppliers to share program investments and rewards (for example, via sole-source contracts), they need to ensure that suppliers also have the experience and financial expertise necessary to manage a higher level of investment. Smaller suppliers in particular may feel they have no choice but to “bet the company” on a program investment or maintenance bid in order to stay competitive. Similarly, a supplier may have made a number of smaller commitments to different programs, which together add up to overcommitment.

Turmoil in the credit markets can also put smaller suppliers under financial strain. In October 2008, Louis Gallois, the CEO of EADS N.V., told *Aviation Week & Space Technology*, “We have ample cash flow to fund operations and have no near-term need to access the market. But many of our suppliers are not in the same position, and we might have to find a way to help some of them out.”³ In fact, that same month, EADS made an early research and development payment to Groupe Latécoère. Latécoère was in a liquidity crisis after it spent €100 million on research and development for the Airbus A380, and then had to wait through unexpected delays in the delivery of the final product to customers.⁴

Changes in the aftermarket are also fueling an increase in financial risk for contractors and suppliers. The aftermarket was once a stable, high-margin business, which compensated to some degree for the higher risk of investing in winning development contracts. Now, governments are trying to squeeze more out of every maintenance dollar—for instance, by turning to maintenance contracts that pay based on the performance of the final product. Generally referred to as performance-based logistics (PBL), this type of contract dramatically increases the prime’s risk of underestimating its costs. As an example, Lockheed Martin and Sikorsky Aircraft Corporation are being paid a fixed lump sum for tip-to-tail logistics on the Navy’s H-60 helicopters. They bear all the risks of providing the required parts and services and making a profit from the venture.⁵

Primes that enter into PBL contracts with governments naturally turn around and make PBL agreements with their supply chain partners. As much as primes have been challenged to accurately bid PBL, the challenge is even greater for smaller suppliers with fewer resources and less experience. A supplier with a great cost structure and lean operations might be an ideal development partner, but the strengths required to successfully supply PBL maintenance—engineering innovation, the ability to invest, and flexibility—are different from those required for development. If a supplier fails because it doesn’t have the skills for development and the aftermarket, the subcontractor or prime fails too.

Geopolitical risk

Aerospace and defense companies pursue global customers and partners in order to lower costs, generate international sales, qualify for business offsets, and share development costs. In pursuit of these benefits, supply chains are entering countries and regions where there is greater potential for political instability, which could impact program execution.

With Russia becoming more muscular in its attempts to reassert influence over its neighbors, Sage Newman, Associate, Corporate Advisory Services at Eurasia Group, believes that “political risks within the Caucasus will continue to increase, and the first- and second-order consequences of those risks will be felt well beyond the region, too.”

The 2008 Russia/Georgia conflict, for instance, “could negatively impact perceptions about the security of the [Georgian oil pipeline] and reduce the willingness to expand infrastructure to accommodate new oil from places such as Kazakhstan’s Kashagan field, which is due to be up-and-running in 2013,” explains Newman. “Kazakhstan’s alternative routes through Russia and China instead could absorb more Kashagan oil once it becomes online.”

Aerospace and defense companies need to cooperate in new ways in order to manage the complicated risks in supply chains that serve increasingly global programs. To develop the Joint Strike Fighter (JSF), for example, Lockheed Martin is working with Northrop Grumman and BAE Systems, with significant contributions from the United States, the United Kingdom, Italy, the Netherlands, Turkey, Canada, Australia, Denmark, and Norway.⁶ A major challenge faced by the JSF leadership team is maintaining political support in each member country. The program contractors cannot handle that challenge alone because foreign support usually depends on successful partnerships with foreign suppliers.

Aerospace and defense companies need to cooperate in new ways to manage the complicated risks in supply chains that serve increasingly global programs.

Qualifying for business offsets may force contractors into regions where they have little experience and where they must work with unknown suppliers that are new to the build experience. This intensifies the communication difficulties caused by geographical distance, language barriers, cultural differences, and inconsistent technical or quality standards. The supply of appropriately skilled labor is so tight in many regions that executives often refer to the worldwide “war for talent.” They also encounter difficulties enforcing contracts under certain legal regimes and where the rule of law is weak. Local business practices may also violate regulations or draw public criticism in the contractor’s home country.

According to an October 2008 *BusinessWeek* report, counterfeit microchips from rural China have entered the supply chains of US defense contractors, including Boeing Satellite Systems, Raytheon Missile Systems, Northrop Grumman Navigation Systems, Lockheed Martin Missiles and Fire Control, and BAE Systems. The risk to US weapons systems, planes, ships, and communications networks goes beyond schedule delays and cost overruns to potentially fatal equipment failure and even foreign espionage. The risks of reputational damage and lawsuits are also high.⁷

Regulatory risk

Complex international supply chains make it more difficult to know if suppliers are violating regulations, but primes and subcontractors remain responsible if they do—all while law enforcement is prosecuting more cases and assessing bigger penalties.

In October 2007, for example, a Munich court fined Siemens, Europe’s largest engineering company, €201 million after an investigation into payments made to secure contracts.⁸ Many of Siemens’ own employees acted illegally, but they also used middlemen as “consultants” in foreign countries in order to deliver illegal payments.⁹ That practice did nothing to reduce Siemens’ liability. In January 2008, Siemens reported that costs related to the German investigation and a US Department of Justice (DOJ) inquiry into the same activity had reached €1.6 billion.¹⁰

The DOJ is investigating Siemens under the US Foreign Corrupt Practices Act (FCPA), which outlaws bribery.¹¹ Over the last few years, prosecutions under the FCPA have become notably more frequent: In 2007, the total number of FCPA enforcement actions by DOJ and the Securities and Exchange Commission (SEC) reached 36, up from just 7 in 2004.¹² In the first three quarters of 2008, there were more FCPA prosecutions than in any other full year prior to 2007.¹³

The severe penalties applicable under the FCPA justify the investment in communicating and cooperating with suppliers and subsuppliers. The maximum fine for a company is at least \$2 million or twice the amount of its gain, and the SEC may also order disgorgement, “including reasonable interest.” Individuals, whom the DOJ and SEC are pursuing more regularly,¹⁴ can be sentenced to up to five years in prison and fined as much as \$100,000. Further plaintiff actions, competitor lawsuits, and actions under other federal or state laws are also risks. For example, a private cause of action can seek triple civil damages under the Racketeer Influenced and Corrupt Organizations Act (RICO).

In guidelines issued by the Office of Management and Budget, a person or firm found in violation of the FCPA may be:

- Barred from doing business with the federal government
- Ruled ineligible to receive export licenses
- Barred from securities business
- Suspended from agency programs of the Commodity Futures Trading Commission and the Overseas Private Investment Corporation

Improperly exporting technology to foreign countries is another practice for which prosecutions and penalties are rising—and again, the potential risk for contractors justifies the investment in gaining a reasonable level of assurance that suppliers and subsuppliers are adequately managing compliance. For fiscal year 2007, the US State Department’s Directorate of Defense Trade Controls (DDTC) reported a 50 percent increase in criminal indictments and convictions related to illegal technology export.

DDTC expects fiscal year 2008 to be another record year for criminal investigations related to violations of export regulations, especially the International Traffic in Arms Regulations (ITAR). The potential for suppliers to err in interpreting and complying with the ITAR and other export controls is a key risk area. (For more details, see “ITAR risks,” page 13.)

Small companies may find it particularly challenging to navigate regulations, especially if they have not had to do so before. In December 2007, hundreds of small businesses became subject to regulation when US ethics requirements were extended to all companies subject to the Defense Federal Acquisition Regulation Supplement (DFARS) and whose US government contracts were expected to exceed \$5 million and 120 days. Within 30 days of the contract award, companies must now create a written code of business ethics and begin enforcing it. At the time the requirement was first proposed, the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council estimated that the clause would apply to 1,800 contractors per year, “of which 700 companies are small business concerns.”¹⁵

A compliance failure at a supplier based anywhere in the world could become a major problem for a contractor. In 2007, reports of ethics violations at one of Lockheed Martin’s suppliers were at the heart of a US whistle-blower lawsuit that snowballed into a DOJ investigation.¹⁶ The government’s heightened scrutiny of compliance and the complexity of the aerospace and defense supply chain are here to stay. Contractors need to treat suppliers as compliance partners, but also follow the old adage “trust but verify.”

ITAR risks

Technologies move between civilian and military projects, and employees often work on both at the same time. In such conditions, it is difficult enough for prime contractors to identify an export-controlled item and continuously monitor its use and incorporation into other products. It is even more difficult for many suppliers, who may not have the necessary resources, level of expertise, and process sophistication. This challenge creates an opportunity for companies to differentiate themselves from the competition by better managing export controls.

Primes and their subcontractors regularly deal with suppliers who lack experience navigating the complicated US International Traffic in Arms Regulations (ITAR). The ITAR regulates any item “designed, developed, configured, adapted or modified” for military use (referred to as defense articles, technical data, and defense services). Any “tweak” to commercial off-the-shelf (COTS) equipment that is being incorporated into a military system, no matter how small, can subject the item and its associated technical information to the ITAR. When the ITAR-controlled component, subsystem, or system is incorporated into a higher-level item, it renders *the entire system* subject to ITAR control. This means that makers of both commercial and defense-related products must keep the commercial ones free of ITAR-controlled parts, components, subsystems, and/or technologies. And if they do put ITAR-controlled technology into a product, they must thoroughly investigate the implications for their market, customers, and supply chain.

Any US company (including any US subsidiary of a foreign company) that manufactures defense articles is required to register with the US State Department. This is true whether or not the company exports defense articles. Companies must also protect ITAR-controlled products and information from transfer to any foreign person or entity. Non-US persons (those individuals

who are not US citizens or lawful permanent-resident “green card” holders) are prohibited from having access to ITAR-controlled items unless specifically licensed by DDTTC. A national of a prohibited country, such as Iran, is not eligible to receive a license, no matter how dated or remote his or her connection with the country. Screening and hiring processes must apply these rules.

Companies that transmit controlled information to any supplier must mark the information as controlled and ensure the supplier and its subsuppliers have procedures that prevent foreign persons from having even the potential for access to the information. DDTTC considers *the potential for access to be the same as actually having access*. The entire supply chain must be prepared to demonstrate compliance in the case of an ITAR audit.

Tracking who is licensed to access what data (and from where) at any given point in time is a major challenge, particularly when data rests in so many locations, such as servers, desktop systems, and mobile devices and storage. Companies need information technology that securely grants and terminates virtual access as necessary, based on verified identities, citizenship, and licenses. No single access control software can achieve this today across all the applications and data repositories that contain export-controlled data. For example, simply applying for and keeping track of licenses requires its own software solution, which does not yet link to identity management.

Compliance requirements should be built into the early stages of business development and program management. Otherwise, business activities cease while the program obtains the appropriate license. Such delays reduce program performance and can reduce the operational readiness of US and allied forces.

Operational risk

As suppliers take on more program investments and more responsibility for integration, they become less interchangeable and more costly and risky to replace. Suppliers also continue to seek growth and market share through mergers and acquisitions. With less competition among suppliers, contractors depend more on existing suppliers and have more difficulty negotiating costs. At the same time, the concentration of resources and knowledge in fewer suppliers may reduce total capacity. It also leaves contractors with few or no alternative sources if a supplier fails or runs out of capacity.

If switching suppliers is less viable, it is important that contractors ensure suppliers have the additional technical personnel and different kinds of expertise needed to manage their own sub-suppliers. For example, in the past, component fabricators managed suppliers of raw stock. Now, component fabricators are becoming subsystem integrators, and subsystem integrators are becoming mini-primers. Both have to manage an additional tier in the supply chain.

To keep pace with the increase in responsibility, suppliers are hiring systems engineers, subcontract managers, more experienced quality assurance personnel, and so on. But new competencies take time to build, and, in some cases, talent is scarce. According to a recent *New York Times* report, the increased demand for systems engineers coincides with a brain drain in the US defense sector. As the current generation of systems engineers retires, most of the next generation is bypassing the defense sector in favor of finance, information technology, and management consulting.¹⁷

In 2008, the strain on small suppliers of galleys, lavatories, and business-class seats led to supply chain disruptions. The problems affected an estimated 8 percent of Airbus's widebody aircraft and contributed to a 19 percent drop in operating income at Boeing. According to *The Wall Street Journal*, "Most [suppliers] lack the resources to expand design departments and manufacturing quickly when business picks up rapidly, as it did over the past two years."¹⁸

After working with its own suppliers to help prioritize and improve production processes and generally improve their visibility, management processes, and controls, Boeing now feels those suppliers will be able to meet the revised production schedule. New information technology played an important role. In a quarterly conference call, Boeing CEO Jim McNerney explained, "It has to do with IT. It has to do with design responsibility. It has to do with visibility [into] supply and production through these IT environments.... We did not have the kind of controls that we now know we have to have—both management and IT to manage globally remote activity—and...we are fixing it."¹⁹

Boeing and Airbus are certainly not the only prime contractors addressing challenges communicating with lower-tier suppliers. Primes often do not realize that subsuppliers have performed to the wrong technical specifications until a delivered subsystem cannot be assembled properly. Not enough primes can map their entire program supply chain, and primes and subcontractors do not communicate enough about supply chain risks. In these conditions, it is impossible to identify all the potentially weak links.

Janice Davis, VP of Global Sourcing at Bombardier, explains: “As an industry, we need to recognize that we can no longer be focused only on the first-tier suppliers, but that we need to have better visibility into the value chain. It’s tough. It takes a lot of discipline and resources—and it will be a continual trade-off and balancing act on when to work only with the first tier, allowing them to manage the value chain, and knowing when to step in to support or directly manage ourselves.”

Silos and poor communication within the walls of the prime’s organization can lead to difficulties with supplier management. Recently, a prime contractor faced the collapse of a key component supplier due to an unexpected shortage of a rare metal. After an internal investigation, the company found that one of its own engineering procurement groups had predicted the shortage, but had not shared the prediction with the affected program team.

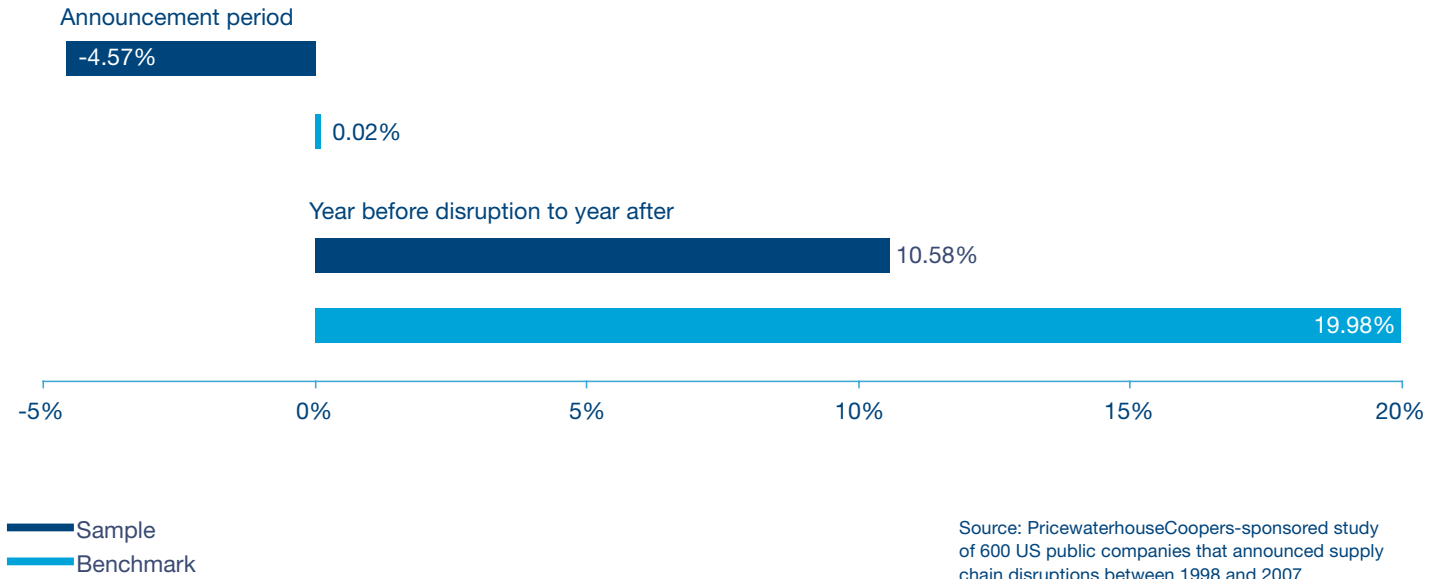
Avoiding such missteps is one way to win more programs and profits. The US government, for example, is increasingly sensitive to primes or higher-tier contractors that seem to “add no value.” One activity that adds a lot of value is managing risks in the program supply chain.

New strategies can realize a major opportunity

Improving supply chain risk management creates the opportunity to win market share and retain more programs. Returns are diminishing in other areas of supply chain optimization. Customers, however, continue to push for better program performance. In a recent competition for a maritime unmanned aerial vehicle, Lockheed Martin underbid the competition by \$5 billion but still lost. The GAO ruled that the US Navy fairly rejected the proposal based largely on perceived execution problems at Lockheed Martin’s principal subcontractor.²⁰

Investors are also focused on program execution. PricewaterhouseCoopers examined the stock values of 14 aerospace and defense companies that reported supply chain failures between 1998 and 2007. Compared to a benchmark group of unaffected firms, disruption-experiencing firms dropped 4.5 percent below the benchmark group during the two days when the disruption was announced. One year later, their shares were underperforming peers by 9 percent.²¹

Figure 3. Median change in stock price



If primes and suppliers can spend less time reworking problems and more time managing and mitigating (or, if appropriate, eliminating) risks, they will reduce costly schedule failures, labor disruptions, and penalties. One successful and stable production program estimated the ongoing cost of rework from late parts alone at \$250,000 per week in penalties and staff hours. And because staff engaged in rework cannot do their original jobs, much less focus on new development, efforts toward efficiency and innovation also suffer.

Investors will also see an improvement in financial metrics from better supply chain risk management. As rework, costs, and program disruptions decrease, margins and return on invested capital expand and companies are able to reduce working capital. In other words, the value generated from each dollar of program investment will increase.

To realize these benefits, companies are taking new actions to mitigate risks in the supply chain. The following are some of the best practices that are emerging.

- **Treat all suppliers as critical members of the program team.**

As Ian Stopps, Chief Executive of Lockheed Martin UK, said to *Aerospace International*, “I am certain that one thing in particular will play an increasingly important role—partnerships...We must encourage innovation across industry and we must be prepared to accept and share risk. Any prime contractor is only as good as its supply chain and each member in that chain is as important as the last.”²²

Some contractors recognize the critical role of suppliers by assigning them a subcontract project manager. But there is some way to go before the people managing subcontracts are appropriately valued according to their impacts on program execution. Many human resources functions still benchmark compensation for subcontract project managers against the traditional procurement or “buyer” role. This contributes to the idea that subcontract management is another buyer role—which, in turn, discourages employees who want to enter the traditional career path of project manager followed by program manager, and then a position at the corporate level. The lower pay and lack of advancement opportunity also make it difficult to attract talent with the engineering experience, graduate degrees, and specialized technical knowledge that is typical of aspiring program managers and also is required for effective subcontract management.

- **Bring the best minds to supply chain risk identification.**

Too many contractors do not know all the links in their supply chain, so how can they know where the risks lie? A logical first step is to map the entire supply chain, assess risk by supplier, and then start managing the risks that have been identified. This process is wholly different from simply procuring suppliers. It is a collaborative partnership with suppliers that involves personnel from many functions, such as finance, operations, compliance, and supply chain management. Every supplier has unique risks. A collaborative, cross-disciplinary team is best suited to identify them.

- **Seek out early warning signs.**

Supply chains contain a vast amount of qualitative and quantitative information about risk. If that information is systematically filtered and communicated, it can warn companies when risk profiles change or new risks appear. One systems integrator that recently won a firm-fixed-price subcontract might have benefited from an early warning system. The integrator subcontracted work to a metal fabricator that subsequently fell behind schedule, jeopardizing the integrator’s delivery schedule. In the end, the integrator paid significantly more for the metal fabrication to help the supplier avoid bankruptcy because it was less risky and expensive than switching suppliers. Better visibility into the fabricator’s levels of

resource allocation, numbers of internal corrective actions, and aging might have provided an early warning and allowed an earlier, less costly intervention.

- **Create a culture of proactive risk reporting.**

Open, cross-functional communication requires a patently different mindset from the old transactional model, which held sway when primes handled most manufacturing and integration internally. Primes took responsibility for paying, and subcontractors took responsibility for delivering according to price, quality, and schedule estimates. Each side tried to minimize its liability for execution failures, and subcontractors took sole responsibility for their own suppliers.

The notion of sole responsibility for supply chain risk is dated. Delays, cost overruns, and quality problems affect margins and profits in the entire supply chain, irrespective of where the root cause resides. Recognizing this, contractors have begun treating suppliers as partners in answering four questions: What are the risks to the program's supply chain? What are we doing about them? How are we making sure that what we're doing remains effective as conditions change? How do we know when conditions are changing inside our suppliers?

To succeed in the new role of risk management partner, suppliers need to be made aware of a program's risk management priorities and procedures during negotiations over costs, schedules, and the statement of work. If contractors wait until after the contract award to impose a risk methodology, suppliers will not be able to work the related costs and responsibilities into their initial bid.

Informed by suppliers' on-the-ground experience, contracts can spell out what and how information about risk and risk management practices should be reported (e.g., quality issues, personnel assignments, and regulatory compliance). For example, contractors can no longer rely on general export control clauses buried in the fine print of most supplier agreements. Contract language should be specific about the program's requirements. And the contractor and supplier should discuss what specialized personnel, information technology, and processes are in place to meet them.

Delays, cost overruns, and quality problems affect margins and profits in the entire supply chain, irrespective of where the root cause resides.

With solid policies and procedures established, the hard work of changing ingrained behavior begins. There is already a culture of accountability in aerospace and defense. Transparency about risks should be added to it. Employees and suppliers need to be convinced that they should report risks before the risks are resolved. Otherwise, companies cannot see risks emerge and change, and are left with only historical information. The corporate culture should encourage early collaboration on risks before they become problems. Training can help, and a positive attitude toward transparency on the part of management is vital.

- **Do not wait for new programs.**

The next unexpected problem may blow the budget or schedule, especially if an ongoing program has already used a portion of a program's contingency buffers. The path toward delivering on budget, on schedule, and on spec involves working with suppliers in four areas. First, contractors and suppliers can identify supply chain risks together. Second, they can understand them by assessing the impact and likelihood of each risk and determining what qualitative and quantitative information would indicate an important change in the impact or likelihood. Such information is called a leading risk indicator (LRI). Third, they can coordinate an appropriate response—for example, agreeing simply to keep an eye on an LRI by having the supplier gather certain data and then analyze it together with the contractor. Finally, whatever the response, indicators need to be continually monitored as operating conditions change. Yesterday's effective response may be obsolete tomorrow.

What this means for your business

Shared risk
management
can change the
contractor/supplier
relationship from
transactional to
strategic.

The supply chain strategy of outsourcing, globalization, and strategic supplier relationships has returned many benefits to the aerospace and defense industry. Prime contractors in particular have already reaped the financial rewards. Now, the industry faces turbulent global economic conditions while customers and stakeholders continue to push for better program performance. Where is the next opportunity?

Supply chain risk management is one area that remains largely untapped. Prime contractors have less visibility and control of supply chain risks than ever before. Suppliers have more risks but lack the resources to manage them alone. On the demand side of the industry, customers are becoming more aware of how costly it is to wait for risks to become problems before responding. The GAO has already recommended that the US Department of Defense (DOD) adopt a framework to better identify and manage supply chain risks. This may ultimately lead to regulation requiring primes to formally report supply chain weakness (or potential weakness) to the DOD.²³

Companies that improve supply chain risk management will deliver more projects according to their schedules, technical specifications, and cost estimates. This is a competitive advantage. The contractor with a better record of program performance wins more business and loses fewer contracts. The pages that follow summarize critical strategies and tools for building this advantage, organized under the basic questions that drive effective supply chain risk management.

Companies that improve supply chain risk management gain competitive advantage by delivering more projects to their schedules, technical specifications, and cost estimates.

Calculating risk

The size and frequency of program disruptions point clearly to an opportunity: Companies can make better-informed decisions about supplier risk as programs are initiated, and can monitor risks more effectively as they get underway. The following timeline of a recent supply chain breakdown illustrates how these opportunities can be realized.

Award

A prime awards a contract for developing space-quality parts at cost-plus-award-fee. In addition to the fee, there are four scheduling milestones for the subcontractor, each worth an additional \$125,000.

Supplier evaluation

The subcontractor asks for proposals from metal fabricators for the precise drilling of a titanium part. The fabricator needs to drill holes with a numerical control machine using a specially designed fixture. At this stage, the subcontractor has a minimum of \$500,000 (four milestones) riding on the supplier's ability to deliver quality work on schedule. The subcontractor chooses a reasonably priced proposal from a fabricator it has worked with before.

To better account for the sizable financial risk, the subcontractor could also assign risk-weighted values to the proposals. For example, fabricator Y's and fabricator Z's proposals are 25 percent lower than the rest, but what would they be if the risk factors were calculated? What is the probability the subcontractor will have to provide a cost escalation or "bailout" of \$20,000? What is the chance of having to rework product for \$100,000? Five percent? Ten? If Y and Z begin to look less attractive after these assessments, could a risk management scheme still make either a compelling proposal?

With so much at stake, the subcontractor could also mitigate key risks. It could send quality and engineering resources to the fabricator's premises to help it with the initial technical set-up and with quality assurance. It could also set up a process (such as regular reports or data from quality control) for gathering early warning signs of problems. If the milestones are met, the bonus payments alone will justify the expense.

Breakdown

Without an early warning system in place, however, the subcontractor has limited visibility into quality risks at the fabricator. Only during a periodic on-site inspection does the subcontractor find critical pieces have been ruined as a result of numerous quality escapes, such as oval holes and gouges.

Fallout for the . . .

Supplier. The fabricator goes well over budget because it has to stop work, participate in a root-cause analysis, improve quality control, and submit to additional inspections by the Defense Contract Management Agency.

Subcontractor. The subcontractor also exceeds its budget. It has to vet and pay another supplier to re-fabricate critical pieces that are ruined. It also needs more engineering time for daily on-site oversight of the original fabricator. The contingency fund is not enough to cover the costs. In addition, the subcontractor cannot complete the corrective actions in time to make any of the prime's milestones. It loses the \$500,000. Then, the prime reduces the award fee by \$175,000 as a result of the problems, which threatened the prime's critical flight date.

Prime. Nervous about the threat to the critical flight date, the government customer asks the prime to create a corrective action plan and present weekly briefings on the plan's progress.

When contractors outsource into the transformed aerospace and defense supply chain, they have a new level of fiduciary responsibility beyond total cost. Suppliers are investing heavily to win positions on major programs and build new business models as subsystem integrators. This increases the pressure on the subcontractors and causes them to take on additional risks, which must be managed.

What is your framework?

Adopting a common framework helps organizations understand and systematically apply supply chain risk management, so that potential events can be identified, responses developed, and surprises reduced. One effective framework is the *Enterprise Risk Management—Integrated Framework* produced by the Committee of Sponsoring Organizations of the Treadway Commission, known as COSO.²⁴

At a minimum, any framework should do the following:

- Create supply chain risk management objectives based on program objectives.
- Establish acceptable levels of risk, or “risk appetites.” While some degree of uncertainty is inherent in all business, it is critical for programs to accept a level of risk that is appropriate to the business opportunity at hand. The underlying premise of supply chain risk management is to ensure value for stakeholders.
- Determine appropriate strategy for each risk. For example, some risks will be controlled, others insured against, still others eliminated, and, finally, all should be monitored and managed to ensure they stay within tolerance levels.
- Treat risk as a portfolio across programs so that the interactions among multiple risks can be understood. This can reduce associated costs and losses throughout the supply chain and will allow companies to better identify and realize opportunities. For example, robust risk information can help management assess overall capital needs and enhance capital allocation.
- Help select and manage supply chain partners.

A framework suggests adjustments to business processes, people, and technology throughout the program cycle, from scoping a potential opportunity to delivering maintenance and logistics in the aftermarket. Some of these changes are incremental, particularly to business processes and existing technology. Casting off old cultures, on the other hand, is a much bigger transformation.

A common framework for supply chain risk management suggests adjustments to business processes, people, and technology—some incremental, some transformational.

One major contractor that was recently considering incremental changes to risk management procedures found it needed to change job descriptions and the employee reporting structure. This was a major transition for many employees. To help them adjust, the contractor is giving workshops aimed at opening minds to a new way of participating in supply chain risk management.

True cultural change will involve multiple functions within the prime's organization and its first-tier subcontractors, as well as the suppliers below the first tier. If people begin to communicate program status and supply chain risk information across programs, functions, and organizations, they can address risks before they become issues disrupting program operations and schedules.

What are your supply chain risks?

Every aerospace and defense company tries to identify risks at the beginning of a program. A common reference point is previous root causes of failure in a relevant program. This is a good first step, but it can benefit from refinement and enhancement. Companies can bring the future into sharper focus by thoughtfully considering new and potential sources of risk that are unique to a program or that spring from changes to operating conditions.

Effective due diligence comes from asking the right questions. Rather than looking to past failures as the primary indicators of potential future risks, adding a careful evaluation of the objectives of a specific program can focus the right minds on the right questions. Programs already have robust processes for establishing objectives. They consider high-level goals and how those align with their company's vision. Then, they establish a strategy for achieving those goals through related objectives by choosing among alternative strategies, which carry different levels of risk.

Rather than relying on past failures to predict future risks, a careful evaluation of program objectives can focus the right minds on the right questions.

When people think in these terms, they naturally look to the future and ask, “Based on all of our experience and the available information, what is likely to interfere with our objectives?” Other questions also arise: Does the program team understand its objectives and how they impact corporate strategy? Do key supply chain partners understand how their objectives affect the program strategy? Are supplier objectives aligned with prime contractor objectives? Do both of these groups have the tools and information necessary to prioritize supply chain risk management based on mutually understood risk impact and likelihood? Finally, do changing risk conditions create any opportunities?

Fundamentally, program risks and opportunities are events that may help or hurt the achievement of the program’s objectives. Sometimes a separate risk management function is responsible for identifying and evaluating those events. This function should not work alone, but instead bring in the people responsible for achieving the objectives, both internally and throughout the supply chain. These employees and suppliers (particularly lower-tier suppliers) are embedded in the operating environment and deal with impediments to objectives day in and day out. Therefore, they bring a frontline perspective to risk identification and evaluation.

Customers and outside experts may also have a vital point of view. Using radar as an analogy, contractors aim their “risk radars” at known supply chain risks, as well as areas where risks might appear. But every radar has blind spots. Suppliers and others can shrink those blind spots because they see risks the contractor does not. And because suppliers are on the front lines, they provide earlier warnings about changing risks. They help extend the risk radar over the horizon.

Sometimes the greatest challenge is communication within the organization. Program risks come from many different areas, so identification needs to be cross-functional and, ideally, stem from cross-program input. Finance, operations, compliance, and supply chain management may all have valuable information. Both the capture and execution teams should also be involved.

When a broad constituency focuses on objectives, it reduces the size and number of blind spots on the risk radar. And when risks are identified and evaluated based on program objectives, it reduces clutter on the radar screen by helping discriminate among low- and high-priority risks (since the significance of risks is related directly to the significance of the objectives which they may impact). Then, active maintenance and regular upgrades keep the radar in good condition through the life of a program. The identified risks, which form the baseline for the entire supply chain risk management system, should be re-evaluated as necessary. Many organizations find it logical to do this during financial and strategic planning. This creates a concept of operations (CONOPS) for risk management that is not treated as an add-on, but is built into the normal operating rhythms of the business and the program.

What do risks mean to your program?

Risk appetite

Once a program has defined its risk management framework and identified supply chain risks using that framework, it must determine its appetite for each risk. A contractor's risk appetite is central to effective supply chain risk management, but it can be lost in translation through the silos of large organizations and the layers of a supply chain. It is vital that contractors and suppliers agree on the acceptable risk level for their programs.

Risk-adjusted pricing is one formal and quantitative way to better calculate risk, thereby making sure that the risk of a particular business decision aligns with the company's appetite. The lowest bidder may not actually be the lowest bidder once the bid is adjusted for risk—i.e., how much risk the contractor is undertaking by collaborating with the supplier, and how much that risk could potentially add to the supplier's bid. Supply chain risk should be a component of best-value estimating.

When a broad constituency focuses on objectives, it reduces the size and number of blind spots on the risk radar.

A formal and qualitative way to align risk appetites is, once again, to ask the right questions. Figure 4 includes some key questions that should be answered before a contract is signed. If contractors and suppliers explore these questions before the contract award, they will be more certain of alignment in the way they prioritize risks, and better able to answer the fundamental question: Can the identified supply chain risks be eliminated, or, more likely, can their impact and likelihood be managed to a level that is within the appetites of both contractor and supplier?

Figure 4: Key risk-related questions to consider before entering an agreement

For contractors

Financial risk

What is the supplier's performance record? Has the supplier received any press lately? Is there any possibility it will be acquired or merged?

Can the supplier safely invest the amount of capital required to do the work?

Is the supplier flexible on contract type and award-fee type?

Geopolitical risk

How difficult is the travel to the supplier, and what are the geopolitical risks in the supplier's locations?

Regulatory risk

Does the supplier have specifically trained and experienced personnel, policies, and effective local procedures for handling regulatory compliance (e.g., ITAR, earned value, etc.)?

Is there an inventory of software applications and information systems to store or process export-controlled information?

Does the supplier plan to assign any foreign persons to my program? Do any foreign persons have the potential to access export-controlled information, either deliberately or through normal operations (for example, if an outsourcer handles backups for servers and work stations)? How is my supply chain managing that access? For example, is there a database that ties employee, contractor, and partner persons to their citizenship status and work location?

For suppliers

Financial risk

What is the contractor's performance record and recent press coverage?

Looking at all my investments, can I safely commit the amount of capital required?

How does contract type or award-fee type affect my financial and operational risk?

Geopolitical risk

How difficult is the travel to the point of delivery and what are the geopolitical risks associated with that location and mine?

Regulatory risk

What will be required to comply with applicable regulations, particularly export controls, ethics requirements, and earned value?

If I am a US company that will manufacture defense articles, has my compliance department registered with DDTTC?

Do my hiring practices identify foreign persons? How can I ensure any foreign persons in my company or among my own suppliers do not have the potential to access export-controlled information? For example, how is citizenship and location data maintained and how is it reviewed?

For contractors

Operational risk

Will the supplier have the estimated capacity, as well as the ability to expand or reduce the volume of orders or services?

Does the supplier have the right mix of people and competencies to fulfill my program requirements?

Will the supplier's other customers interfere with program execution? Is the supplier already slow to respond?

Does the supplier have formalized risk management, change management, and quality management systems?

How does the supplier handle sensitive intellectual property?

Which work will the supplier outsource, and to which suppliers in which locations?

For suppliers

Operational risk

How could changes in capacity affect the profitability or success of this contract opportunity?

Can I fill gaps in competencies by subcontracting or other means without destroying my margins?

Can I provide the priority the contractor demands without jeopardizing other work?

What resources are required to meet the contractor's standards of quality, change, and risk management?

What will be required to meet the contractor's policies and procedures for handling sensitive intellectual property?

With which of the contractor's other suppliers will I be required to work, and can I answer all of the questions "for contractors" about my own suppliers and partners?

Likelihood and impact

Assessing any supply chain risk is a function of appetite, likelihood, and potential impact. Aerospace and defense companies define likelihood and impact qualitatively (e.g., low, medium, and high) and quantitatively through a combination of decision science (such as Monte Carlo, Real Options Valuation, and Crystal Ball models), performance metrics (such as return on invested capital), and mathematical probabilities.²⁵

The data fed into these calculations is often historical. For example, if a supplier has a good track record of delivering on time to quality specifications, then it may be considered a low risk. Contractors should also consider what conditions in the program at hand might differ from the historical record because the same risks can be assessed differently from program to program. Is a good component supplier bidding to become a subsystem integrator? Does it have the additional expertise required?

Supplier capacity is another area of concern. When a supplier develops an excellent reputation, multiple contractors can “conspire” to create trouble by offering too much work, which the supplier “can’t refuse.” More open and regular communication about supply chain risk can provide a clearer picture of capacity and help avoid this destructive cycle. Then, the more accurate risk assessment can be compared to each party’s risk appetite as the program’s portfolio of risk is assembled. When appetite is aligned with likelihood and impact, companies make better decisions about how to respond to risks in order to meet reporting and regulatory objectives, and they have a more accurate understanding of how well the program is fulfilling its strategic and operational objectives.

Leading indicators

Returning to our “good” supplier and the adage “trust but verify,” what type of information would provide an early warning that the supplier might be headed for capacity problems? A traditional candidate is safety stock levels, but supply is often on the verge of disruption by the time safety stock levels are low. An earlier warning sign might be lead times from the supplier, or the number of expedited deliveries. These are qualitative indicators that can be further investigated through quantitative analysis. For example, a tolerance level might stipulate that the lead time could exceed the plan by as much as 10 percent, and that anything above this would trigger further investigation and possibly mitigation.

Figure 5, “Early warning signs,” has more examples of information that can indicate a change in the impact or likelihood of financial or operational supply chain risks. These leading indicators improve supply chain risk management in two ways. First, they allow companies much more time to respond to risks. Second, they allow responses to be adjusted as operating conditions change. Both of these increase the chance that a risk can be prevented from being realized—i.e., from becoming a program disruption.

The good news is that existing functions already have access to most leading risk indicators. Some likely candidates are program management, supply chain management, integrated product teams, finance, and contracts. What’s missing in most cases is a systematic approach to gathering, analyzing, and communicating this information.

Information technology can help. Aerospace and defense companies can focus on better utilizing their information technology at the business unit, group, or program level in order to monitor and communicate risk. To name a few examples, business intelligence software, enterprise resource planning (ERP) systems, and core functional process management technology can track risk information. This includes collecting, identifying, and systematically analyzing select leading indicators.

Executives can also work toward integrating risk information across their enterprises, but this is a long way off. Aerospace and defense companies tend to grow through acquisition and amass multiple IT platforms in which they have invested heavily. Scrapping some of these systems and merging others not only requires new investments but also abandoning existing ones, a scenario that is unlikely in a time when economic growth is trending down globally. There are reasonable, incremental investments companies can make to share risk information across internal silos, such as sales, sourcing, and engineering. There are also many leading indicators that only suppliers can provide, so companies need to add or improve connections with those suppliers.

Boeing, for example, is developing a platform for gathering, analyzing, and sharing quantitative risk indicators in cooperation with key suppliers, which it intends to implement in all four parts of its business: Integrated Defense Systems, Commercial Airplanes, Shared Services Group, and Phantom Works (Boeing’s research and development unit).

“What we’re trying to do is identify predictive indicators of problems in processes—not specific products—and correct these processes beforehand so that issues don’t materialize in the end delivery to Boeing or our customers,” explains John Harnagel, Director of Supplier Program Management at Boeing Integrated Defense Systems. “Ultimately, all our predictive indicators are targeted at one thing—a goal of 100 percent on-time delivery and zero defects.”

Figure 5. Early warning signs

Leading risk indicator	Sources of information about the indicator	Functions holding the information
Financial risk indicators		
Cash flow: Insufficient cash flow	<ul style="list-style-type: none"> • Industry reports (e.g., Dun & Bradstreet) • Conversations with suppliers 	<ul style="list-style-type: none"> • Finance • Supply chain management
Working capital: Decreasing inventory turns	<ul style="list-style-type: none"> • Supplier self-reporting • Supplier reviews and assessments 	<ul style="list-style-type: none"> • Finance • Program managers
Equity: Erosion of shareholder value or equity	<ul style="list-style-type: none"> • News and analyst reports • Public filings • Conversations with analysts 	<ul style="list-style-type: none"> • Finance • Corporate strategy
Operational risk indicators		
Management: Key management changes	<ul style="list-style-type: none"> • Supplier reviews and supplier self-reporting • Conversations with supplier contacts • News reports/releases 	<ul style="list-style-type: none"> • Program manager • Supply chain management • Finance and contracting • Operations
Supply chain: Supply chain instability	<ul style="list-style-type: none"> • ERP system data • Supply chain management metrics (delivery schedules, lead times) • Supplier scorecards and self-reporting 	<ul style="list-style-type: none"> • Supply chain managers • Program managers
Process/quality: Process instability	<ul style="list-style-type: none"> • Operations meetings • Quality management system • Supplier reviews and self-reporting 	<ul style="list-style-type: none"> • Operations • Quality control • Supply chain management

Examples of qualitative indicators

Examples of quantitative indicators

-
- | | |
|--|---|
| <ul style="list-style-type: none">• Complaints about supplier from other suppliers | <ul style="list-style-type: none">• Supplier has non-recurring engineering investment requirements exceeding forecast cash flow |
| <ul style="list-style-type: none">• Supplier reports build-up of work in progress and accelerating material reimbursements | <ul style="list-style-type: none">• Supplier's sub-tier supplier inventory levels exceed plan by 15%• Material buffers exceed material requirements planning (MRP) standards by 25%• Progress payments invoiced 15 days earlier than expected |
| <ul style="list-style-type: none">• Announced or rumored takeover of supplier | <ul style="list-style-type: none">• Price-to-earnings ratio or market is more than 25% below industry comparables• Market capitalization dropped 25% in one year |
| <ul style="list-style-type: none">• Key supplier contacts change• Announcement of reduction in force or plants | <ul style="list-style-type: none">• Supplier's attrition rate exceeds 9%• Supplier's sub-tier supplier base forecasts reach 75% of capacity |
| <ul style="list-style-type: none">• Inability to get lead times from suppliers• Increasing amount of expedited material• Increasing changes in delivery plans | <ul style="list-style-type: none">• Lead times exceed plans by 10%• Supplier's sub-tier supplier forecasts exceed plans by more than two weeks for two months running |
| <ul style="list-style-type: none">• Variable production outcomes (e.g., some lots integrate well and some do not)• Unpredictable schedules and deliveries• Increased communication between supplier and quality control• Manner in which the sub responds to purchase orders is significantly different from past | <ul style="list-style-type: none">• Actual to schedule is inconsistent by more than two weeks for two months running• Increase in the number of outstanding quality corrective actions and average age increase of greater than 30%• Sub-tier supplier production yield rates are more than 10% below targets |
-

How are you responding?

Today

One response to an identified supply chain risk is to monitor it, ideally, with leading indicators. Then, a company can see as early as possible when the likelihood or impact of a risk evolves outside of the company's risk appetite. If quality corrections trend upward, a program manager may need to work with the supplier to find and fix the cause. In general terms, a new response is required in order to bring the risk level back in line with the contractor's appetite.

It is simple to say "Fix the cause." But in practice, programs may not have owners with express responsibility for responding to supply chain risks. They may also lack a structured process delineating what to do, which functions will do it, and when those functions will communicate. For example, procurement managers are accountable for the information they send to suppliers. In an export-controlled environment, the procurement manager is responsible for contacting internal trade compliance professionals, who have the authority to assign the appropriate jurisdiction and classification to information. The procurement manager is then responsible for clearly marking all export-controlled information before giving it to any supplier, foreign or domestic. All employees of the supplier are accountable for the information they accept. They have the responsibility and need the authority to refuse any information without a specified export control status. For risks such as these throughout the supply chain, companies need to determine responsibility, accountability, and authority.

The main challenge is not finding people—it's connecting them. Internal silos and the distance (and barriers) between contractors and subcontractors need to be overcome. As Greg Archer, Director of Procurement at Northrop Grumman, puts it, "The engineering and global supply chain (GSC) communities must act as one. The stove-piped silos of the past won't work. GSC needs to be part of the process from the very beginning so we can get our product to our customers on time."²⁶ Furthermore, supply chain risk management is a continuous process. The connections between risk information and those with the ability to respond to it need to be kept active.

Tomorrow

Aerospace and defense companies need to change their cultures of supply chain risk management. Many people have been conditioned by long experience to avoid reporting problems as long as possible. There is a “conspiracy of hope” that problems will solve themselves because people have become accustomed to raising issues only when they know the solution. This cultural norm impedes proactive supply chain risk management, which seeks to address risks sufficiently early so as to avoid the risks becoming problems.

This is why the current trend is for primes to deploy tremendous resources to solve program disruptions. The future is to do less expensive monitoring all the time, followed by less expensive mitigation of risks, and to address interrelated risks across a portfolio of programs. However, mitigation is still a capacity challenge. Program managers need to build in the flexibility necessary to take on risk monitoring and control tasks outside the normal operations of the program.

For example, a systems integrator was recently operating under a firm-fixed-price contract. It subcontracted the production of cases under another firm-fixed-price agreement. However, when the case maker fell behind schedule, the systems integrator started weekly teleconferences and on-site reviews to help find a solution. Capacity was a problem, so the case maker developed an outside machine source. To return to schedule, it also began working overtime and weekends, air-shipping components, and paying premiums for expedited work from its own suppliers.

By improving supply chain risk management, the systems integrator may be able to anticipate the next emerging problem involving capacity constraints, and shift work before the supplier falls behind schedule. The supplier may also have a formal process to raise capacity concerns early and to raise concerns about common risks, such as the late release of drawings and specifications. Once the alarm is sounded, the integrator and supplier could cooperate on work-arounds to avoid schedule disruptions.

Program partners need to discuss risk management systems and processes as part of submitting initial proposals. Contract negotiations are an opportunity to specify supply chain risk management protocols and create incentives. Part of a supplier’s compensation, for example, could be based on how well it reports on key risk areas. Once the contract is signed, the subcontractor should be managed by someone with the same skills as an experienced program manager, who is empowered to treat the supplier as a partner in program execution. This manager should use criteria for ongoing supplier evaluation (e.g., scorecards) that include clear expectations for risk reporting.

Sometimes the contractor is uneasy with the program's risk baseline, but suppliers need a working example of how early reporting and action can be a positive for everyone. In this case, the contractor should consider independent non-advocate reviews (INARs) or a technical assessment to investigate the concerning risks and to demonstrate that suppliers will not be penalized for reporting risks.

Training is the other good method of changing behavior, when it is properly supported by executive attitudes (i.e., the "tone at the top"). The aerospace and defense sector has become effective at training employees and key partners on elements of enterprise risk management and program management. This same effort should be applied to supply chain risk management.

In PricewaterhouseCoopers' 2008 anti-corruption survey, only 40 percent of respondents felt their current controls were effective at identifying high-risk business partners or suspect disbursements.²⁷ One way to strengthen these controls is through anti-corruption training. Both employees and supply chain partners need to be aware of the risks of corruption and their responsibilities *across all of the jurisdictions they are likely to encounter*. In general, primes can sponsor forums at suppliers or invite key suppliers to in-house universities for specialized education about supply chain risk management. Online training can also be used to reach a geographically dispersed audience in a cost-effective manner.

Is your response still effective?

In the aerospace and defense industry, companies already monitor many key performance indicators to measure outcomes. The great step forward for most companies would be identifying and understanding risks throughout each program's complete supply chain and adding forward-looking indicators related to those risks. Leading indicators help companies better manage program execution so they can meet their objectives. One well-known public dashboard of leading indicators is the National Hurricane Center of the US National Weather Service.²⁸

When a hurricane forms, the center issues predictions about the likelihood of the hurricane making landfall and its severity if or when it does. As the hurricane moves across the ocean, these early predictions are updated regularly. The center provides forecast advisories every six hours, along with other leading indicators such as wind speed probabilities and "cones" of potential movements, plus historical indicators such as the hurricane's path to date.

Businesses, governments, and individuals use this dashboard because they cannot keep the resources necessary to deal with hurricanes on constant standby—and they also need to know when to evacuate. Effective supply chain risk management follows a similar pattern, using leading indicators to adjust investments and responses over time as operating environments change.

Returning to the aerospace and defense industry, a program objective might be achieving the highest possible quality, as measured using the key performance indicator Six Sigma. A leading indicator, on the other hand, would be monitored while the part was still being manufactured.

An integrator responsible for a navigation system might monitor the yield rates in the manufacturing process for navigation chips. If the yield rates fell below a pre-designated threshold, this might indicate a risk that the navigation system could be delivered with less than 3.4 defects per million opportunities (i.e., Six Sigma quality), at which point the integrator would need to do more than monitor. It might conduct a health check. If the yield rates were low enough or changing fast enough to indicate an acute risk, the integrator might go straight to a root-cause investigation in order to return to Six Sigma efficiency.

Through true collaboration, supported by rigorous processes such as training, contracts, and monitoring and investigating leading indicators, the old, transaction-based relationship between contractors and suppliers can evolve into a strategic one. This is a long-term strategy that companies should start implementing today.

Small steps yield big results

Despite all best efforts to identify risks in advance, unanticipated risks will arise, and known risks will evolve. What separates winners from losers is the ability to monitor these changes and then mitigate risks before a delivery deadline is missed or a component fails testing. This ability is within reach.

What separates winners from losers is the ability to monitor changes in the operating environment and mitigate risks before they become major problems.

Effective supply chain risk management starts with incremental steps that lead to large changes over time. Adjustments to existing business processes, technology, and employee training have a multiplier effect: They start changing the culture of supply chain risk management.

Still, executives may wonder how their supply chains will have time for operations if they have to identify, assess, and monitor so much information. It is important to keep in mind that suppliers up and down the chain are already gathering and analyzing risk information. Employees and suppliers have a huge amount of useful data. They just need a risk management framework and incentives to understand and communicate the information.

The potential benefits of more effective supply chain risk management justify the costs. Planning for and monitoring risk can be significantly less expensive and time-consuming than resolving supply chain disruptions. Supply chains that collaborate closely to manage risk will significantly improve their ability to keep programs within budget, schedule, and technical specifications. This not only yields immediate cost savings, but also increases long-term value. Effective program execution is critical to establishing a durable competitive advantage.

Endnotes

- ¹ Thomson Reuters (2008).
- ² US Government Accountability Office, Testimony Before the Committee on Armed Services, US Senate (June 3, 2008).
- ³ Quoted in Joseph C. Anselmo and Michael A. Taverna, "Market Focus," *Aviation Week & Space Technology* (October 13, 2008), page 12.
- ⁴ Peggy Hollinger, "Supplier Is Given Boost by Airbus," *Financial Times* (October 3, 2008).
- ⁵ Department of Defense Office of Inspector General, *Logistics: H-60 SeaHawk Performance-Based Logistics Program (D-2006-103)* (August 1, 2006).
- ⁶ Lockheed Martin press release, "Lockheed Martin F-35 Takes Shape, Readies for First Flight" (February 22, 2006).
- ⁷ Brian Grow, Chi-Chu Tschang, Cliff Edwards, and Brian Burnsed, "Dangerous Fakes—How Counterfeit, Defective Computer Components from China Are Getting into U.S. Warplanes and Ships," *BusinessWeek* (October 2, 2008).
- ⁸ David Gow, "Siemens Prepares to Pay \$2bn Fine to Clear up Slush Fund Scandal," *The Guardian* (January 25, 2008).
- ⁹ Carter Dougherty, "The Sheriff at Siemens Sees an Endless Battle," *International Herald Tribune* (October 6, 2008).
- ¹⁰ "German Prosecutors Fine Siemens €201 Million," *International Herald Tribune* (October 4, 2007).
- ¹¹ The act outlaws "corrupt payments to foreign officials for the purpose of obtaining or keeping business." US Department of Justice, "Lay-Person's Guide to the FCPA Statute" (June 2001). Available at www.usdoj.gov/criminal/fraud/fcpa.
- ¹² Department of Justice press release, "Fact Sheet: The Department of Justice Public Corruption Efforts" (March 27, 2008).
- ¹³ During the period of January 1 to September 30, 2008, there were nine FCPA enforcement actions with SEC penalties and eight FCPA enforcement actions with DOJ penalties.
- ¹⁴ As of September 2008, the year had seen 16 separate enforcement actions brought against individuals, one more than in all of 2007.
- ¹⁵ Proposed Rules, Federal Register, Vol. 72, No. 219 (November 14, 2007), www.usdoj.gov/criminal/nptff/far/docs/2007/nov/11-14-07FedReg.pdf.
- ¹⁶ Dave Michaels, "Justice Department Joins Case Against Lockheed Martin," *The Dallas Morning News* (November 19, 2007).
- ¹⁷ Philip Taubman, "Efforts to Slow Defense Industry's Brain Drain," *The New York Times* (June 25, 2008).
- ¹⁸ Daniel Michaels and J. Lynn Lunsford, "Lack of Seats, Galleys Delays Boeing, Airbus," *The Wall Street Journal* (August 8, 2008).
- ¹⁹ Q3 2008 Boeing Company Earnings Conference Call (October 22, 2008).
- ²⁰ US GAO, Decision, Matter of: Lockheed Martin MS2 Tactical Systems (B-400135; B-400135.2) (August 8, 2008), www.gao.gov/decisions/bidpro/400135.htm.
- ²¹ For more analysis of this issue across multiple industries, see PricewaterhouseCoopers' *From Vulnerable to Valuable: How Integrity Can Transform a Supply Chain* (December 2008).
- ²² Quoted in "The Next 100 Years," *Aerospace International* (July 9, 2008).
- ²³ US GAO, *Department of Defense: A Departmentwide Framework to Identify and Report Gaps in the Defense Supplier Base Is Needed* (October 2008), www.gao.gov/highlights/d095high.pdf.
- ²⁴ The executive summary can be found online at www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf.
- ²⁵ "Likelihood" is the probability that any potential issue, severe or otherwise, will actually occur and disrupt a program. A highly probable, non-critical risk may be a cost of doing business that is simply paid for when it occurs. On the other hand, if the potential severity is high but the probability is remote, the best response may be to monitor for changes in probability and make sure a plan is in place if the probability increases. The impact of a risk when it is realized is often called "severity." More severe risks interfere with more important program objectives. Sometimes this means multiple smaller objectives that add up to one big problem. The basic question is this: If a risk is realized, will it be a major catastrophe, a manageable problem, or something in between?
- ²⁶ Quoted in Deborah Hawkins, "Shifting the Make/Buy Ratio Sharpens Our Competitive Edge," *The Integrator*, Northrop Grumman Integrated Systems newsletter (September 22, 2008).
- ²⁷ PricewaterhouseCoopers, *Confronting Corruption: The Business Case for an Effective Anti-Corruption Programme* (2008).
- ²⁸ www.nhc.noaa.gov/index.shtml.

Methodology

This PricewaterhouseCoopers white paper represents new analysis on how aerospace and defense companies can work with their global partners to effectively and collaboratively manage supply chain risks. Insight was gained through various interviews with senior management in the aerospace and defense industry, as well as with cross-industry thought leaders. Findings were also based on in-house research on multi-tiered contractors' financial performance, inventory turnover, and employee growth.

PricewaterhouseCoopers conducted this research as part of continuing investigations into how to create competitive advantage in the aerospace and defense industry. The following white paper, which was previously published by PricewaterhouseCoopers, discusses other aspects of this issue:

Creating Competitive Advantage: How to Transform Program Management (2007).

For more PricewaterhouseCoopers' research on supply chain risk management across multiple industries, please see:

From Vulnerable to Valuable: How Integrity Can Transform a Supply Chain (December 2008).

To have a deeper conversation
about how this subject may affect
your business, please contact:

Glenn Brady
Partner
314.206.8118
glenn.brady@us.pwc.com

Brian Kinman
Partner
973.236.5537
brian.j.kinman@us.pwc.com

Matthew Lekstutis
Director
703.762.7239
matthew.lekstutis@us.pwc.com

Neil Hampson
Partner
+ 44 20 7804 9405
neil.r.hampson@uk.pwc.com

Or visit:

www.pwc.com/supplychainriskmanagement

This publication is printed on Finch Fine Recycled.
It is a Sustainable Forestry Initiative® (SFI) certified
stock using 10% post-consumer waste (PCW) fiber
and manufactured in a way that supports the long-
term health and sustainability of our forests.



10% total recycled fiber

The information contained in this document is provided 'as is', for general guidance on matters of interest only. Although we believe that the information contained in this document has been obtained from reliable sources, PricewaterhouseCoopers is not responsible for any errors or omissions contained herein or for the results obtained from the use of this information. PricewaterhouseCoopers is not herein engaged in rendering legal, accounting, tax, or other professional advice and services. Before making any decision or taking any action, you should consult a competent professional.