National Institute of Standards and Technology
U.S. Department of Commerce

U.S. Resilience Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Northrop Grumman Corporation
Trusted, Innovative, World-Class Supply Chain

INTERVIEWS

Kevin Engfer
Director, Supplier Mission Assurance, Northrop Grumman Information Systems

Michael Ozmun
Information Security (Enterprise Shared Services)

The Next New Things in Risk Management

- Supply Chain Leadership Council coordinates best practices and information sharing across the company.
- Supplier Assessment Management System (SAMS) provides objective measurement criteria for supplier performance in eight major categories.
- Supplier cybersecurity questionnaires identify areas where mentoring and additional training is required and Northrop Grumman Corporation provides guidance to its suppliers.

Company Overview

A producer of aerospace and defense technology, Northrop Grumman Corporation (NGC) is the fifth largest defense contractor in the world, and in the top 100 of Fortune 500 companies in the United States. NGC is a federated company; each of its four sectors is run by a sector president and each sector is responsible for its own profit and loss. The four sectors include:

- **Aerospace/Aircrafts:** provides manned and unmanned aircraft systems, space systems, and advanced technologies. Customers include NASA, the Department of Defense and commercial providers.
- **Electronic Systems:** provides airborne radar, navigation systems, electronic countermeasures, precision weapons, airspace management systems, space payloads, marine and naval systems, communications systems, and government system. It includes legacy businesses from the Westinghouse acquisition.
- **Technical Services:** provides life-cycle solutions and long-term services for global customers. Key capabilities include platform sustainment and modernization, advanced training solutions, high-technology engineering services, and operationally responsive systems.
- **Information Systems:** provides advanced information solutions for defense, intelligence, civil agency, and commercial customers, including cybersecurity solutions; command and control systems; network communications solutions; and intelligence, surveillance, and reconnaissance systems. Customers range from federal and state governments to commercial providers in the aerospace industry.

Spanning all four of these sectors are two distinct supply chains:

- **Non-deliverable** products for internal use which is managed centrally, and
- **Deliverable** products for customer use which are managed by the sector.

NGC's vision is to be "the most trusted, world-class, innovative supply-chain organization that delivers value to our customers through integration of highly skilled people, suppliers, processes, tools, and communications."[1]

Figure 1. Supply Chain Leader Council (SCLC)

Deliverable Supply Chains	Non-Deliverable Supply Chain
▪ Aerospace / Aircraft Sector ▪ Technical Services Sector ▪ Electronic Systems Sector ▪ Information Services Sector	▪ Enterprise Shared Services

Organizational Approach to Supply Chain Risk Management

What is different about NGC compared to many other high tech companies is that its business is program based, rather than product based. Program requirements in each sector are defined by the customer — and sector programs typically have unique supply chain requirements and suppliers. The kinds of suppliers and supply chain requirements for a B-2 bomber program, for example, will be quite different than those required for an information system.

In addition to the four commercial sectors, NGC has a fifth corporate structure called Enterprise Shared Services (ESS). This organization drives common policies, procedures, processes and systems throughout the corporation for supply chain and other internal support services including IT infrastructure and cybersecurity, as well as human resources, legal and accounting. The ESS group directly manages the supply chain for non-deliverable purchases.

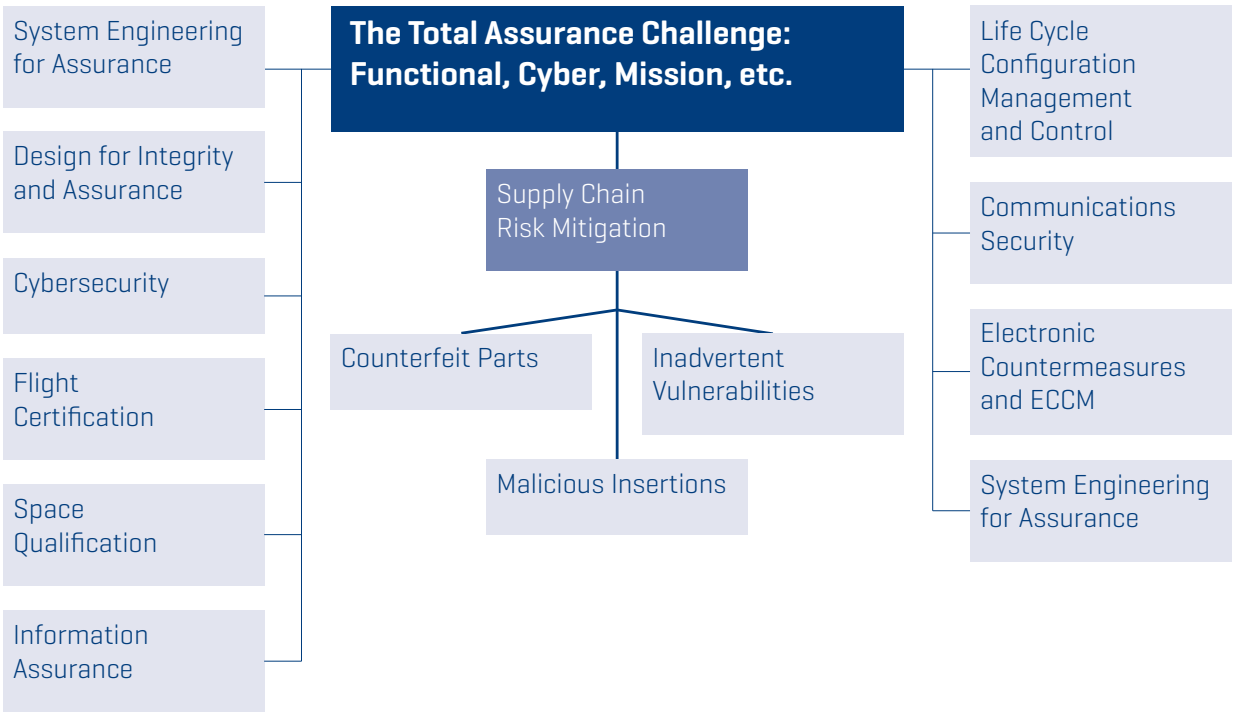
1 http://crreport.northropgrumman.com/

The President of ESS is NGC's lead executive for Supply Chain. ESS coordinates the Supply Chain Leadership Council (SCLC), which develops basic policy and process guidelines for company-wide supply chain management — from materials control and management to purchasing and transportation — to assure consistency of practice and information sharing across the sectors. The SCLC is comprised of a small ESS team responsible for strategy and policy and each sector head of supply chain, generally a vice president. This cross-company management structure has been in place for many years at NGC.

The management and oversight of supply chains — and the hands-on risk management — occurs at the sector and program level. According to Kevin Engfer, risk management tends to be a "team sport" through the product and program life cycle.

At the program level, there are cross-functional subcontractor management teams that oversee all aspects of supplier performance. These teams bring together supply chain mission assurance, quality assurance, engineering or a technical specialist. Other members may be added as needed, such as a cyber-engineering or import-export controls experts. Major subsystems typically have their own subcontractor management teams.

Figure 2. Myriad Disciplines Required for Assurance
Global Product Data Interoperability Summit, 2013



Business Case for Supply Chain Risk Management (SCRM)

NGC has a long tradition of SCRM driven primarily by the nature of its business, types of products it develops, kinds of suppliers it uses, and its unique customer contract issues. It is critical for NGC to maintain its ability to deliver in an execution-based business environment. And, of course, it goes without saying that minimizing quality and security concerns is paramount when working to secure the nation's defense.

Guiding Principles of SCRM

First, the NGC supply chains tend to be oriented around the program life cycle. There are some types of requirements that are associated with development; others with manufacturing or services and support. Second, NGC manages supply chain related risk on a risk-basis, and these risks change with time. Technical risks, given the complexity of the systems and products, have always been top of mind. But, there are emerging risks that are bubbling to the top: cyber risks or, for products with long development cycles, supply chain continuity risks. Counterfeit risks are also a top-of-mind concern.

Supplier Risk Management Systems

Given the size and scope of NGC's business, suppliers play a key role in their success. In 2013 alone, the company spent more than $8 billion dollars with approximately 9,500 suppliers.[2]

To measure supplier performance, NGC developed an internal web-based tool called Supplier Assessment Management Systems (SAMS). SAMS assessments provide an objective data relative to the supplier's technical, quality (mission assurance), cost, schedule, management, proposal, supply chain management and customer satisfaction performance. Ratings are based on a color scale of red (unsatisfactory), yellow (marginal), green (satisfactory) or blue (excellent).

2 http://crreport.northropgrumman.com/

Figure 3. Supplier Assessment Management System (SAMS): 8 Categories of Assessment

Management
- Responsiveness
- Program Management
- Risk/Opportunity Management
- Expert Staffing

Proposal
- Team Commitment
- Proposal Strategy
- Proposal Adequacy and Negotiation

Technical
- Product Performance
- Systems Engineering
- Software Engineering
- Logistics & Sustainment
- Part Materials & Processes
- Service Level Performance

Cost
- Cost
- Financial Health

Schedule

Mission Assurance & Quality
- Quality
- Process Effectiveness

Supply Chain Management

Customer Satisfaction

Criteria for Excellent Rating

The SAMS Framework defines criteria against which a score is derived for each assessment area. The criteria for an "excellent" rating include:

1. **Program Management:** Consistently proactive and cooperative leadership; appropriate resources, tools and infrastructure available to support program requirements; risks and opportunity processes and procedures well integrated, captured, tracked and communicated; and availability of expert staffing.
2. **Technical:** Key performance parameters or systems attributes exceed design requirements; timely and accurate design, analysis, coding, verification and documentation for systems and software; detailed plan to support all elements.

3. **Cost:** Strong evidence of cost management; timely, accurate and complete invoicing; and strong financial health rating.
4. **Schedule:** Clearly measurable events and criteria for successful completion and with a time buffer.
5. **Proposal:** Management commitment demonstrated at all levels; creative and innovative solutions; proposal complete, on time and RFP compliant at affordable price; and acceptance of contract T&Cs.
6. **Supply Chain Management:** Robust sub-tier selection and qualifications NGC provided full visibility to lower tiers; fully engaged supply chain organizations with supplier management tools, resources/processes, surge capability and risk mitigation/opportunity capture systems in place.
7. **Mission Assurance/Quality:** Consistent, accurate and complete submittal of deliverables; consistently meet quality requirements; effective quality management systems with capability to detect quality issues early.
8. **Customer Satisfaction:** High degree of satisfaction with subcontract performance in terms of product quality and cost.

The SAMS tool is used to assess performance and evaluate risk from the programs all the way up to the corporate level. It covers everything from purchase orders to major subcontracts. It can analyze how the supply chain is performing in key areas or to highlight a group of critical suppliers that support different sectors. It also provides the information to identify areas for improvement.

One focus of attention are risks associated with single-source, small, and foreign businesses that may be more vulnerable to program performance deficiencies.[3] Another area of concern has been financial health of the supply base, given the downsizing in procurement and stresses in the defense industrial base. To address customer concerns and potential vulnerabilities, NGC includes financial health assessments of its suppliers in order get a fuller picture of the health of its supply base.

OASIS: Many of its suppliers are local businesses situated near NGC operations. The Online Automated Supplier Information System (OASIS) creates a "One Northrop" approach across all of the sectors. This online portal provides suppliers with everything from terms and conditions to training. NGC also posts information videos on topics such as supplier chain security and identity management and supplier scorecards.

3 http://crreport.northropgrumman.com/

Quality: NGC relies on supplier quality management system certifications to understand the basic capabilities of a supplier. Suppliers are required to implement and maintain a quality management system appropriate for the type of product or service being procured. If the risk is deemed to be high for a highly-engineered product, NGC has the right to perform periodic reviews. Typically, inspection teams from mission assurance, engineering and supply chain will verify that the right systems are in place to minimize performance and quality risks.

NGC has a corporate approach to "counterfeit material prevention" which prescribes preventive measures, training, communication, counterfeit alert management, and procedures for comprehensive material assurance. The Enterprise Material Authenticity team, chartered by the Corporate Quality Council — bringing together a team from quality, engineering, supply chain, contracts, and legal — takes the lead on counterfeit parts protection efforts.

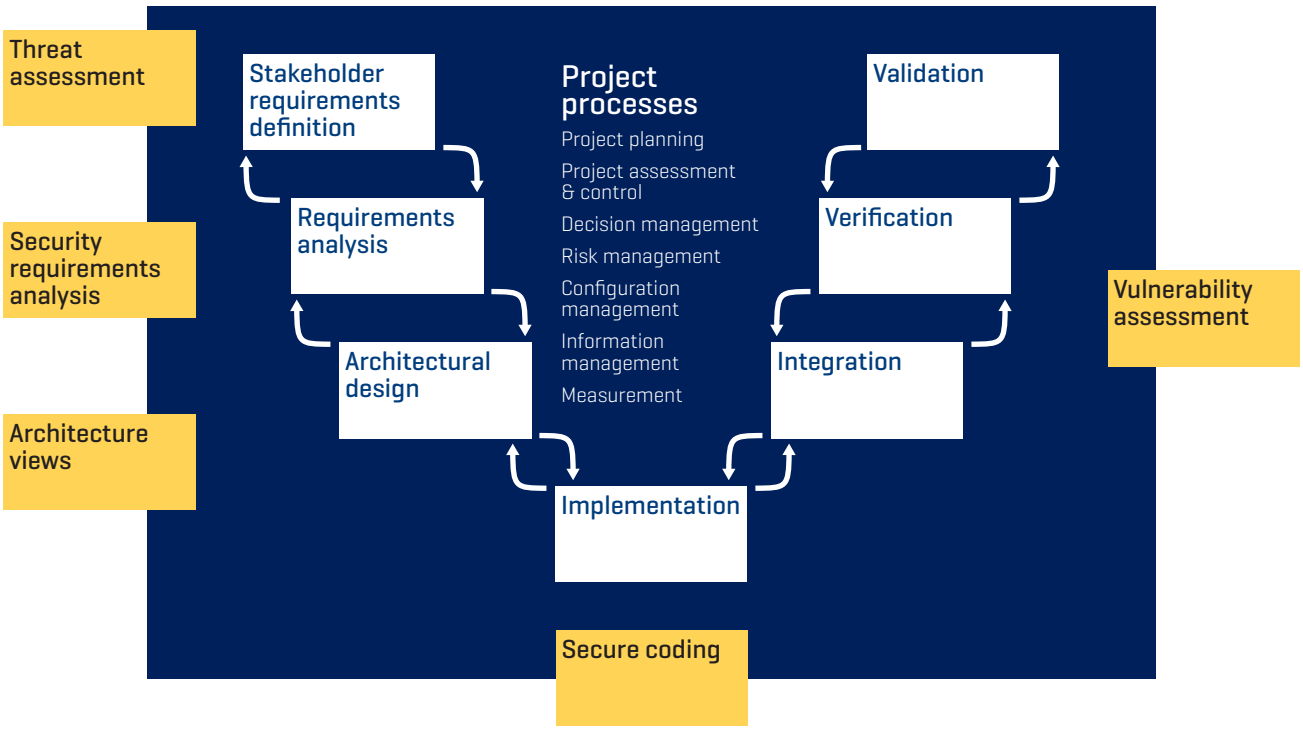
Cyber Security in the Supply Chain

Northrup Grumman has been a vocal proponent of the growing dangers of cyber risks to the supply chain risk. Given the nature of its business, NGC is acutely aware of the emerging vectors of attack through supply chain partners and components.

Because program requirements are set by its customers, NGC has begun educating its customers about the need to build security into products and systems through the program life cycle, from design to delivery. This may require a shift in the culture of some of its customers, which have long been focused on investing in performance rather than security.

The ESS cyber team develops new methodologies and standard tools to manage cyber risks. An increasing number of customers are requiring SC risk management plans, which include identification of the ways NGC manages particular risks associated with programs that include software development. NGC uses a couple of methodologies and a standard tool developed by ESS. Inspection requirements exist through the development process, and these inspections must be passed before a project can proceed.

Figure 4. Building Security into the Design Process



Standards

NGC adheres to the widely accepted standards for quality management, such as AS 9100, a quality management standard for the aerospace industry, and ISO 9000, and it looks for those capabilities in its major suppliers. NIST standards, like 7622 (Supply Chain Risk Management for Information Systems) is an area of increased attention and compliance efforts.