# Better Manage Your Supply Chain

## Acquisition Security Framework (ASF): Achieving a Secure, Resilient, and Survivable Supply Chain

CERT | Software Engineering Institute | Carnegie Mellon University


When you outsource your software development, you are still accountable for the cybersecurity risks. How do you avoid becoming a victim of suppliers who don't have the skills or motivation to manage cybersecurity?

Collaborate with our expert researchers to gain more insight and control over the software supply chain and better evaluate and manage the risks and gaps in the acquisition process.

## Supply Chain Risk

Supply chain risk springs from different aspects of the acquisition ecosystem, such as software development. For example, risk increases when outside suppliers develop software with little oversight from program or project managers.

In today's highly competitive and technology-driven environments, outsourcing is more than a trend—it is the way business is done effectively and efficiently. In addition, with the increased use of outsourced software and development resources, it has become more difficult to manage acquisition risk.

Relying on formal legal contracts to mitigate acquisition risk is proving to be ineffective because it fails to provide the mechanisms, flexibility, and repeatability needed to manage cybersecurity risks across the software supply chain.

Although a contract-based approach is a key supply-chain practice, it does little to help you monitor your software suppliers and ensure that software-reliant systems meet high-quality and security requirements. As risks increase, confidence in your software-reliant systems decreases.

## Longer Supply Chains

Many years ago, supply chains were more straightforward and manageable. In the current software-driven world, you now have a relationship with a prime contractor, who then has relationships with subcontractors, who also have subcontractors, and so on.

You're challenged to effectively manage a long chain of suppliers, software, requirements, systems, and contracts. How do you enforce contracts on those long chains of suppliers with limited information and control over their operations?

You may have limited power to confirm the integrity of delivered systems because you rely on an intermediary—a prime contractor or integrator. This reliance may mean that you must trust the prime contractor to manage supply chain risks for you. On top of all that, do you know if your suppliers are complying with applicable government regulations?

What can you do? How can you ensure that your suppliers' processes and controls are keeping pace with the acquisition ecosystem?

## A New Approach

Today's cybersecurity landscape requires that you implement a risk-based approach to managing the supply chain. You must also comply with new and evolving regulatory oversight, such as DFARS amendments, DoD Instruction 5000.02, and DoD Instruction 8510.01.

Keeping these challenges in mind and leveraging our knowledge of the critical regulations that affect acquisition and the supply-chain landscape, we are developing a new approach to help those like you who acquire complex software-intensive systems.

Our research focuses on a new approach to risk management and acquisition regulations to help you cut through the bureaucracy of government supply chain management.

## What Is the ASF?

Our proposed approach, the Acquisition Security Framework (ASF), is designed to not only give you more insight and control over your software supply chain, but also help you evaluate risks and gaps in how you acquire, engineer, and deploy secure software-reliant systems.

## Do these worries keep you up at night?

Do your suppliers use sound security development and management practices throughout their software acquisition and development lifecycle? Do you adequately assess and mitigate supplier risks in your final software-reliant systems? Are your systems protected against malware inserted in the supply chain? Do you monitor your systems as they change and use controls to manage the emerging risk?

We in the CERT Division understand the challenges you face daily as a government acquisition professional. We are currently researching ways to help you improve how you manage software supply chain risk by assessing the capabilities and processes of your suppliers.

Building on CERT cyber-risk management expertise and leveraging data gathered over the last ten years, we've begun developing a framework that will enable you to measure and improve your ability to manage cyber risks throughout the software supply chain.

## The Foundations of the ASF

The ASF is collection of cybersecurity practices that an acquisition program should perform when acquiring a software-intensive system. The ASF documents cybersecurity practices in the following five areas:

1. **Relationship Formation** is about evaluating and controlling supplier-related risks before you enter into relationships with your suppliers.
2. **Relationship Management and Governance** is about managing the relationships you've already formed with your suppliers.
3. **Engineering** is about building appropriate cybersecurity controls to minimize the risk of inserting vulnerabilities.
4. **Secure Product Operation and Sustainment** is about managing cybersecurity risk as you operate and maintain your software-reliant systems over time.
5. **Supply Chain Technology Infrastructure** is about securing the technologies you need to support your supply chain activities.

## The Prototype

The ASF is currently a conceptual prototype based on our in-depth study of software supply chains. Its framework must still be expanded and transformed into a usable product by our work with collaborators from the acquisition community. Once created, the framework can be piloted by early-adopter organizations.

## Get In on the Ground Floor

The ASF promises to be an innovative supplier risk management mechanism that

- increases your confidence in your suppliers' performance
- helps you understand the gaps in how you manage your supply chains
- provides a roadmap for improving how you manage supply chain risks
- supports achieving compliance with increasingly stringent supply-chain regulations and standards

## Join Us

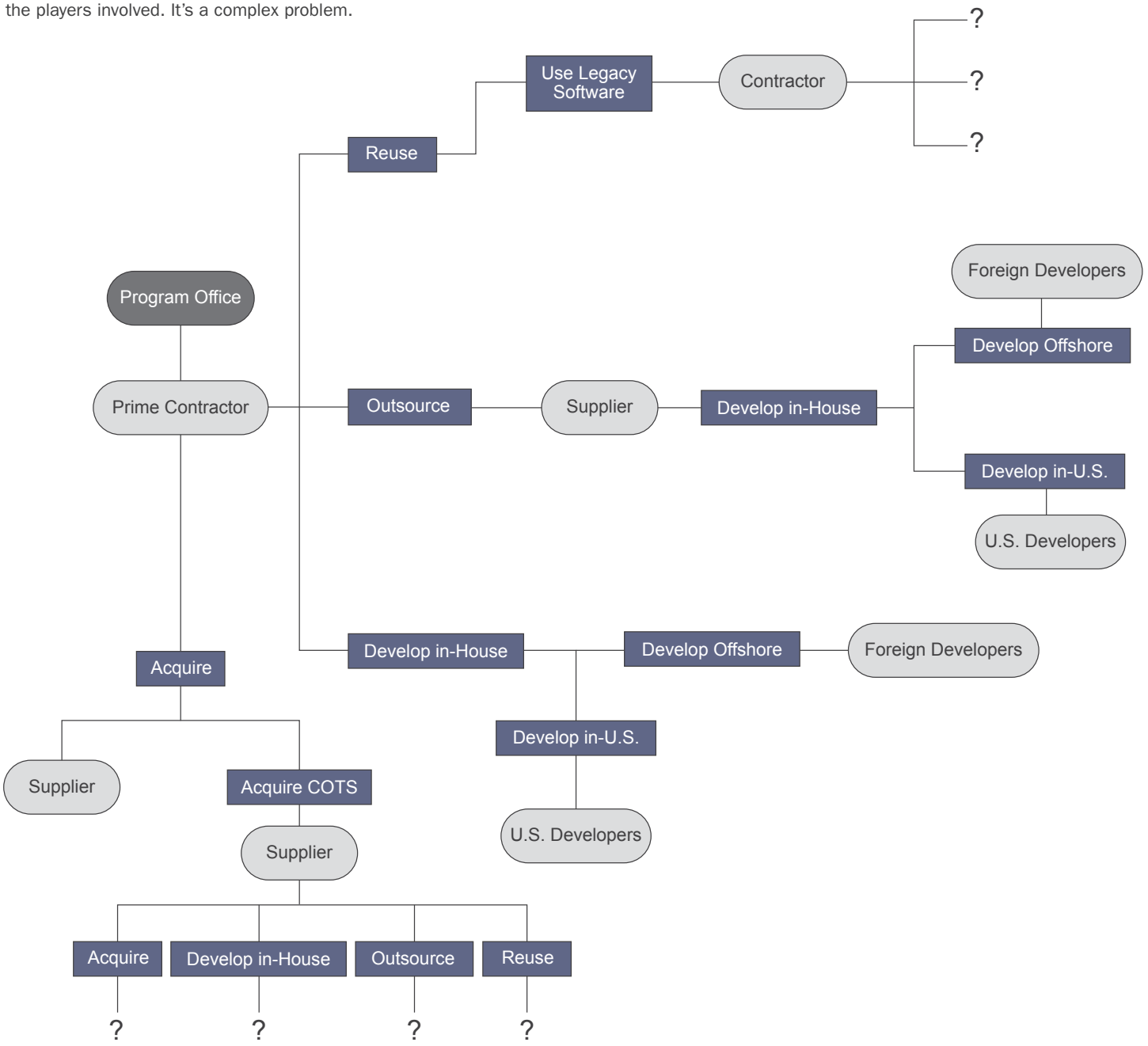
We need smart collaborators to help us shape this innovative approach. Working with us, you will have opportunities to help us develop, refine, and test the ASF, and then pilot the results.

We're looking for collaborators who are candid with their comments and will suggest improvements. As an acquirer, you're familiar with acquisition's key drivers and the requirements that the ASF must meet.

We're looking to work with you and your rich network of like-minded innovators. Help us engineer a successful approach that improves government acquisition and makes your job easier.

## The Acquisition Process

There's risk associated with today's longer supply chains and more regulated environment. You no longer have direct control over all of the players involved. It's a complex problem.




## About Us

For nearly 30 years, the CERT Division of the SEI at Carnegie Mellon University has been a leader in cybersecurity. Originally focused on incident response, we have expanded into cybersecurity areas such as network situational awareness, malicious code analysis, secure coding, resilience management, insider threats, digital investigations and intelligence, workforce development, DevOps, forensics, software assurance, vulnerability discovery and analysis, and risk management.

## Contact Us


Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

**Phone:** 412.268.5800 | 888.201.4479
**Web:** www.sei.cmu.edu | www.cert.org
**Email:** info@sei.cmu.edu