Carnegie Mellon University
Software Engineering Institute

ACQUISITION SECURITY FRAMEWORK (ASF): INTEGRATION OF SUPPLY CHAIN RISK MANAGEMENT ACROSS THE DEVSECOPS LIFECYCLE

Carol Woody, Ph.D., Presenter (cwoody@cert.org)
Charles Wallen (cmwallen@sei.cmu.edu)
Christopher Alberts (cja@cert.org)
Michael Bandor (mbandor@sei.cmu.edu)

April 2022

Abstract: Supply chain cyber risks stem from many organizational dependencies—in particular, processing, transmitting, and storing data; information technology; and communications technology. These risks are broad, significant, and growing as outsourcing options expand. Important mission capabilities can be undermined by an adversary's cyber-attack on third parties, even when the organization does not explicitly contract for technology. Virtually all products or services an organization acquires are supported by or integrate with information technology that includes third-party components/services. Practices critical to monitoring and managing these risks are scattered across the organization, resulting in inconsistencies, gaps, and slow response to disruptions. The Acquisition Security Framework (ASF) contains leading practices to support programs acquiring/building a secure, resilient software-reliant system to manage these risks. It defines the organizational roles that must effectively collaborate to avoid gaps and inconsistencies. It also establishes how an organization should ensure effective supply chain risk management that supports its mission and objectives. The framework contains proven, effective goals and leading practices, and it is consistent with supply chain risk management guidelines from the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), and Department of Homeland Security (DHS).

Background

Concern for supply chain risk has been growing. The potential impact of cybersecurity attacks became evident with the Heartland payment system breach in 2008 (Gordover, 2015). Millions of dollars were lost because of a software error for a product from an organization that was fully compliant with all regulatory mandates. This incident, at the time, brought attention to the limitations of compliance alone in addressing cybersecurity issues. What really mattered was the existence of a weakness in the software.

The Target attack in December of 2013 expanded the concern for supply chain risk. In this successful attack, the perpetrators connected to the operational environment using stolen credentials from a supplier to take advantage of the broad internal information-sharing capabilities available among third-party systems. These capabilities enabled the perpetrators to insert malware and siphon off credit card information from the point-of-sale system acquired from another supplier (Aorato Labs, August). New impacts from increasing the use of third-party software continue today. Most recently, a breach at SolarWinds leveraged a routine process for the automated distribution of software updates to send malicious code to 18,000 customers, potentially impacting government and industry through trusted network capabilities across the globe (Temple-Raston, 2021).

In a 2010 Software Engineering Institute (SEI) research project, we found that few organizations considered supply chain risk within the acquisition and development lifecycle beyond a narrowly defined vetting of the supplier's capabilities at the time of an acquisition. This failure to consider the responsibilities the acquirer had to assume based on the lifecycle use of the third-party product left the organization open to an extensive range of cyber risk that increased over time (Ellison, Goodenough, Weinstock, & Woody, 2010). In later research, we investigated the lifecycle issues of supply chain risk and identified that the operational and mission impact of cyber risk increases as organizations become more dependent on suppliers and software.

The traditional focus on operational controls for security compliance does not address the (1) increasing supplier role in providing services, (2) design, and (3) introduction of code weaknesses into software-reliant systems. As reliance on third-party components and products increases, the supply chain becomes a growing source of cyber risk. In this research concerning lifecycle issues, we identified practices throughout the acquisition and development lifecycle that were critical to reducing the potential success of cyberattacks (Alberts & Woody, 2017). However, at the time, few programs were implementing effective cybersecurity practices and supplier oversight early in the acquisition lifecycle. Figure 1 shows the wide range of practices available for use, but these were not integrated into standard practice.

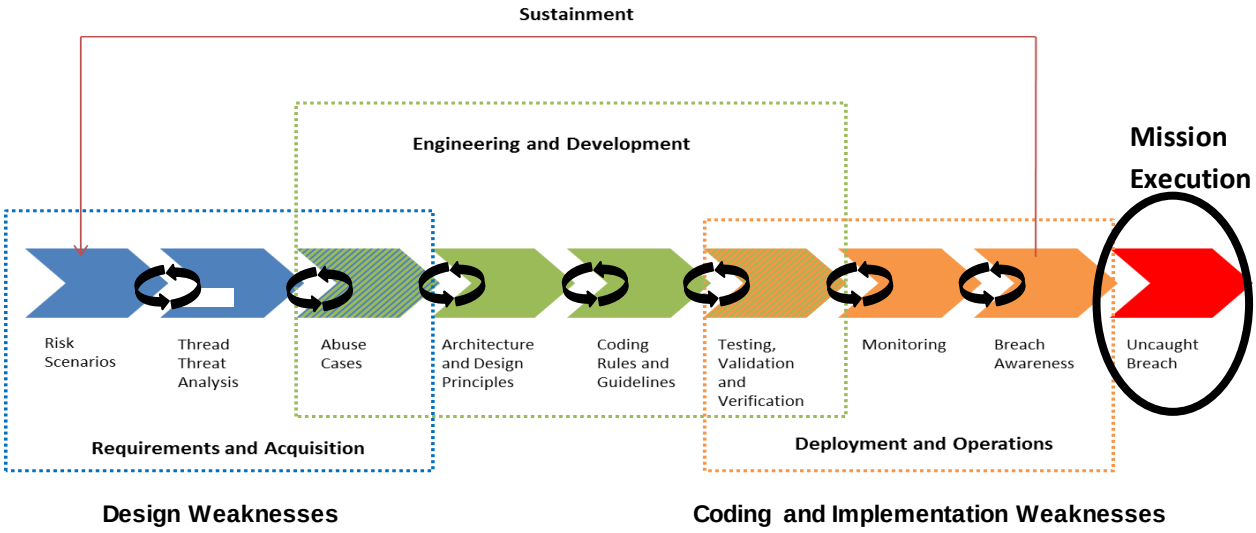

Figure 1: Cybersecurity Practices Available Across the Lifecycle to Address Security Weaknesses

Supplier-oriented risks were a key factor driving early CERT research into the development of more effective methods for managing cyber risks. We clearly recognized that the growing complexity of threats required that organizations use more systematic approaches to cyber risk management. Not only did organizations need better security methods, but their expanding outsourcing strategies led to major concerns that their suppliers also needed better security management tools. *Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes* (Caralli, et al., 2007), published in 2007, was the first release of these innovative concepts that helped reset security management approaches and formed the basis for work that continues to evolve today.

The *CERT Resiliency Management Model (CERT-RMM)*, a process improvement model first published in 2011, assembles leading practices from industry and government for managing operational resilience, which requires integration across the key organizational areas of security management,

business continuity management, and aspects of information technology (IT) and operations management (Caralli, Allen, & White, 2011). In 2015, the CERT Division of the Software Engineering Institute developed the *External Dependencies Management (EDM) Assessment* to enable critical infrastructure organizations in the United States to manage external dependency and supply chain risks. This assessment is an extension of the *DHS Cyber Resilience Review (CRR)* (DHS, 2014). Based on the CERT-RMM, the CRR establishes a baseline of cybersecurity capabilities that helps an organization understand (1) its operational resilience and (2) its ability to manage cyber risks to critical services during normal operations as well as during times of operational stress and crisis.

In 2016, researchers from both CERT acquisition and operational teams collaborated to create an integrated, systems-oriented perspective, called the *Acquisition Security Framework (ASF)*, that considers the full supply chain risk management lifecycle (Alberts C. , Woody, Wallen, & Haller, 2017). Managing supply chain cyber risk is especially challenging because it is broad and pervasive, and responsibility is spread widely across an organization. Acquisition and development must consider the operational context and plan for sufficient risk management, and operations must effectively integrate each added supplier into sustainment processes and practices.

ASF organizes leading supply chain risk management practices to measure and improve an organization's ability to manage third-party cyber risks across a system's lifecycle. It provides a mechanism for increasing an organization's confidence about the level of its vendors' performance, improving its understanding of potential gaps, and making improvements based on a suggested roadmap.

Active development of the ASF was initiated in 2020 for use in applying integrated software security engineering practices into the systems lifecycle. This development effort includes defining a risk-based framework that enables a program to do the following:

- Manage program security risks collaboratively across the lifecycle and supply chain.
- Incorporate security practices that scale to selected acquisition pathways and development approaches.
- Implement an appropriate level of process management and improvement (i.e., maturity) for security practices.

Acquisition and engineering practices continue to evolve. Emerging threats and increased system complexity have given rise to new techniques that are designed to manage cyber risk from early requirements definition through operations. These new techniques have brought improved methods and outcomes, including the lifecycle orientation shared by DevSecOps and ASF. Facilitating integrated cybersecurity in environments with complex supplier-dependent systems demands these new solutions.

Acquisition Security Framework (ASF)

Supply chain issues impact every aspect of acquisition, development, and sustainment. The expanded use of third-party code, components, products, and services has further stretched the involvement of the supply chain into almost every aspect of the organization. Organizations' need to access a wide range of technical skills to create, integrate, and maintain the multi-faceted capabilities that have become operational necessities drives them further towards greater reliance on suppliers. Managing potential supply chain risk requires effective collaboration across the many participants interacting with each supplier over time.

The ASF is a collection of cybersecurity leading practices that each acquisition program should consider when building/acquiring a secure and resilient software-reliant system. These practices can be categorized into these practice areas:

- Program Management
- Engineering Lifecycle
- Supplier Dependency Management
- Certification
- Support
- Process Management and Improvement

The framework enables programs to evaluate and manage risks and gaps when acquiring, engineering, and operating secure and resilient software-reliant systems. The challenge is to manage the supply-chain-related security risks collaboratively across the lifecycle and supply chain. This management requires processes that effectively connect those performing practices in the practice areas listed above to continuously integrate as all aspects of the acquisition, development, and operational needs change over time.

The growing challenges of supply chain risk coupled with the expanded use of automation in software development and implementation driven by moves to Agile at scale and DevSecOps require organizations to ensure the integration of effective and timely supply chain considerations through all acquisition, development, and operational practices.

ASF Structure

The framework contains layers of goals and supporting practices organized as shown in Figure 2. There are six primary practice areas: Program Management, Engineering Lifecycle, Supplier Dependency Management, Certification, Support, and Process Management and Improvement. Within each of these practice areas are two to three domains. Within each domain, there are six or more goals, each with a group of practices that support an organization in meeting each goal. The practices are phrased as questions that can be used in determining current and planned organizational capabilities.

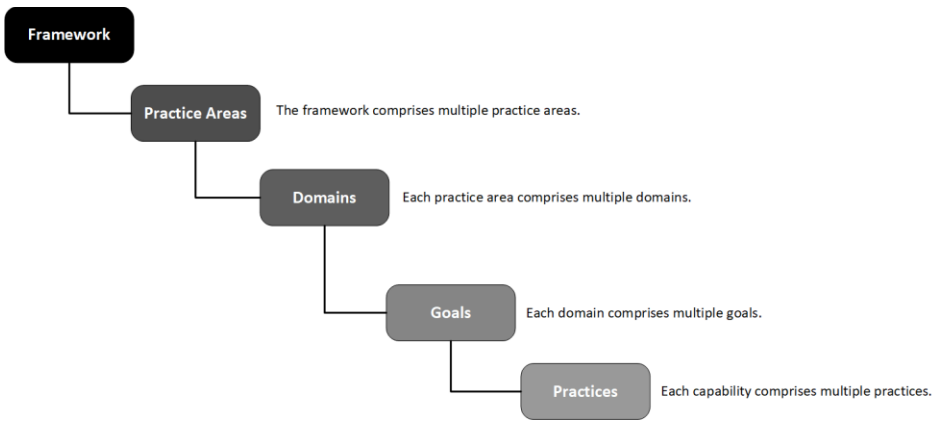

Figure 2: ASF Organizational Structure

Many of the practices are interrelated to support the communication that must occur among the practice areas on an ongoing basis. Limited collaboration and communication among systems teams on

tasks that require supplier management creates potential risks. Program leaders may not be aware of risky choices made by acquisition and engineering teams or that the organization's relationships with suppliers are not being managed effectively. For example, practices in Engineering Lifecycle domains connect to practices in the Program Management and Supplier Dependency Management domains to confirm that information sharing/reporting is occurring as needed for effective cybersecurity and supplier risk management.

Development of ASF Practice Areas and Domains

In current ASF development, we have completed practices for Engineering Lifecycle and Supplier Dependency Management, leveraging our previous work we described earlier in the Background section. In the remainder of this section, we share the information we assembled about the domains and goals in these two practice areas.

For the **Engineering Lifecycle** practice area, we identified the following domains:

- Domain 1: Engineering Infrastructure
- Domain 2: Engineering Management
- Domain 3: Engineering Activities

Domain 1 covers goals related to infrastructure development, operation, and sustainment. Domain 2 covers goals related to technical activity and product risk management. Domain 3 covers goals for engineering lifecycle activities, including requirements, architecture, third-party components, implementation, test and evaluation, transition artifacts, deployment, and secure product operation and sustainment.

For **Supplier Dependency Management** we identified the following domains:[1]

- Domain 1: Relationship Formation
- Domain 2: Relationship Management
- Domain 3: Supplier Protection and Sustainment

Domain 1 covers goals related to planning, formal agreements, supplier evaluation, and supplier risk. Domain 2 covers goals related to supplier identification and prioritization, performance and management, continuous risk management, change and capacity management, supplier access to program and system assets, dependency management, and supplier transaction management. Domain 3 covers goals for supplier disruption, maintenance, and situational awareness.

Next Steps

We are actively developing the Program Management practice area and have identified the following three domains: (1) Program Definition, (2) Program Planning and Management, and (3) Requirements and Risk. Once our work on Program Management is complete, we plan to address the remaining three ASF practice areas: Certification, Support, and Process Management and Improvement.

---

[1] Detail questions relevant to each goal in the Supply Dependency Management practice area are provided in an appendix at the end of this paper as an example of the depth of material currently available in the framework.

To help bring value quickly, we have been building methods to deploy ASF in organizations that support software-intensive systems environments. These deployment methods include exploring the use of ASF as a baseline roadmap of practices for engineering and supplier management to improve current program considerations of cybersecurity and supply chain risk. We do this by comparing program and vendor deliverables, such as the statement of work, software assurance and cybersecurity checklists, and control plans to ASF. By mapping these program items to ASF practices areas and goals, we can identify practice areas that are well addressed as well as gaps in practice areas that should be addressed.

Building ASF is clearly a challenge, but the larger concern is making sure that the approach is usable by those who need it. The focus must shift from selecting guidelines that suppliers should follow to improved collaboration among the parts of the acquiring organization that interact with suppliers to establish clear and effective actions and measures for supply chain risk management. To that end, we have taken this multi-prong approach that concurrently focuses on ASF development and deployment strategies. While this approach requires more effort, we believe it will result in a more accessible and useful tool that will support the systems and cybersecurity risk management needs of acquiring organizations.

References

Alberts, C., & Woody, C. (2017). *Prototype Software Assurance Framework (SAF): Introduction and Overview.* Retrieved March 31, 2022, from the Software Engineering Institute: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=496134

Alberts, C., Woody, C., Wallen, C., & Haller, J. (2017, May/June). Assessing DoD System Acquisition Supply Chain Risk Management. *CrossTalk*. Retrieved March 31, 2022, from https://resources.sei.cmu.edu/asset_files/Article/2017_101_001_502299.pdf

Aorato Labs. (August, 2014). *The Untold Story of the Target Attack Step by Step.* Retrieved March 31, 2022, from Aorato Labs: http://aorato.webstick.co.il/labs/report/untold-story-target-attack-step-step/#

Caralli, R. A., Allen, J. H., & White, D. W. (2011). *CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience.* Addison-Wesley. Retrieved March 31, 2022, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30375

Caralli, R. A., Stevens, J. F., Wallen, C. M., White, D. W., Wilson, W. R., & Young, L. R. (2007). *Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes.* doi:10.1184/R1/6574805.v1

DHS. (2014). *Assessments: Cyber Resilience Review (CRR).* Retrieved March 31, 2022, from Department of Homeland Security, United States Computer Emergency Readiness Team (US-CERT): https://www.us-cert.gov/ccubedvp/self-service-crr

Ellison, R., Goodenough, J., Weinstock, C., & Woody, C. (2010). *Evaluating and Mitigating Software Supply Chain Security Risks.* doi:https://doi.org/10.1184/R1/6573497.v1

Gordover, M. (2015, March 19). *Lessons Learned from the 2008 Heartland Breach*. Retrieved March 31, 2022, from Proofpoint: https://www.proofpoint.com/us/blog/insider-threat-management/throwback-thursday-lessons-learned-2008-heartland-breach

Temple-Raston, D. (2021, April 16). *A Worst Nightmare" Cyberattack: The Untold Story of the SolarWinds Hack*. Retrieved March 31, 2022, from NPR: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Appendix: ASF Goals for the Supplier Dependency Management Practice Area

Domain 1: Relationship Formation has the following goals:

- **Goal 1—Establishing supplier relationships is planned.** The purpose of this goal is to assess whether entering into relationships with suppliers is planned.
- **Goal 2—Security/resilience requirements are included in formal agreements with suppliers.** The purpose of this goal is to assess whether supplier agreements include security/resilience requirements.
- **Goal 3—Suppliers are evaluated before entering into formal relationships with them.** The purpose of this goal is to assess whether suppliers are evaluated to determine if they can meet the security/resilience requirements for the program or system before entering into relationships.
- **Goal 4—Supplier risk is managed.** The purpose of this goal is to assess whether risk management is included in supplier risk considerations.

Domain 2: Relationship Management has the following goals:

- **Goal 1—Suppliers are identified and prioritized.** The purpose of this goal is to assess whether suppliers that the program or system depends on are identified and prioritized.
- **Goal 2—Supplier performance is governed and managed.** The purpose of this goal is to assess whether performance is considered when evaluating suppliers that support the security/resilience of the program or system.
- **Goal 3—Supplier risk management is continuous.** The purpose of this goal is to assess whether the risks of relying on suppliers to support the program or system are continuously managed.
- **Goal 4—Change and capacity management include suppliers.** The purpose of this goal is to assess whether change and capacity management are coordinated with suppliers that support the program or system.
- **Goal 5—Supplier access to program or system assets is managed.** The purpose of this goal is to assess whether the risks associated with supplier access to assets is managed. (These questions involve access granted to any supplier, not only those that support the program or system.)

- **Goal 6—Infrastructure and governmental dependencies are managed.** The purpose of this goal is to assess whether the risks of depending on infrastructure providers and/or government service providers are identified and managed.
- **Goal 7—Supplier transitions are managed.** The purpose of this goal is to assess whether managing the transition of supplier relationships is based on business considerations (e.g., insolvency, nonperformance, new technology).

Domain 3: Supplier Protection and Sustainment has the following goals:

- **Goal 1—Suppliers are included in disruption planning.** The purpose of this goal is to assess whether suppliers are included in incident management and service continuity for the program or system.
- **Goal 2—Planning and controls are maintained.** The purpose of this goal is to assess whether program or system controls and plans related to suppliers are regularly tested and updated.
- **Goal 3—Suppliers are included in situational awareness reviews and analysis.** The purpose of this goal is to assess whether situational awareness activities for the program or system include suppliers. (Satisfying this goal means that information sources about threats to key suppliers are monitored for the sake of the program or system.)

Biographies

Carol Woody
Dr. Carol Woody, a principal researcher for the CERT division of the SEI at Carnegie Mellon University, is building capabilities and competencies for measuring, managing, and sustaining cybersecurity for highly complex software intensive systems and supply chains. She has successfully implemented solutions in many domains, including banking, mining, manufacturing, government, and finance. She co-authored a book, *Cyber Security Engineering: A Practical Approach for Systems and Software Assurance*, published by Pearson Education as part of the SEI Series in Software Engineering. The CERT Cybersecurity Engineering and Software Assurance Professional Certificate, released in March 2018, is based on the research she led.

Charles M. Wallen
Charles M. Wallen has been a thought leader in operations and risk management for over 25 years. He has provided consulting to public and private organizations, led industry-wide risk initiatives, and managed global operations risk management and governance programs for financial services organizations. Charles works closely with Carnegie Mellon University's Software Engineering Institute CERT Division on initiatives to strengthen the resilience of critical infrastructure, improve software assurance, and enhance/refine techniques for managing supply chain risk.

Christopher Alberts
Christopher Alberts is a Principal Cybersecurity Analyst in the SEI's CERT Division, where he leads applied research and development projects in software assurance and cybersecurity. His research interests include risk analysis, measurement and analysis, modeling and simulation, and assessment. His research has been adopted by a variety of government and industry organizations, both nationally and internationally. He has co-authored two books and published over 50 technical reports and articles. Alberts has BS and ME degrees in engineering from Carnegie Mellon University.

Michael Bandor
Michael Bandor is a Senior Software Engineer in the SEI's Software Solutions Division (SSD). He is responsible for leading teams that enable the organizations within the Department of Defense (DoD) and other customer organizations to enhance the predictable performance and mission assurance in the acquisition, evolution, and operations of software-reliant systems. He has more than 32 years of experience with DoD systems, including business systems, command and control systems, satellite systems, and ground-based radar systems. He has more than 22 years of military (USAF) experience. He earned a BS in Computer Science/Software Engineering from Weber State University.

Document Marking

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.