Carnegie Mellon University
Software Engineering Institute

ACQUISITION SECURITY FRAMEWORK (ASF): AN ACQUISITION AND SUPPLIER PERSPECTIVE ON MANAGING SOFTWARE-INTENSIVE SYSTEMS' CYBERSECURITY RISK

Christopher Alberts (cja@cert.org)
Michael Bandor (mbandor@sei.cmu.edu)
*Charles M. Wallen (*cmwallen@sei.cmu.edu*)*
Carol Woody (cwoody@cert.org)

September 2022

Abstract: Supply chain cyber risks stem from many organizational dependencies, including 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 the organization's contracted third parties, even when the organization does not explicitly contract for technology. Virtually all products and 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 can be scattered across the organization, resulting in inconsistencies, gaps, and slow response to disruptions. The Acquisition Security Framework (ASF) contains leading practices that support programs acquiring/building a secure, resilient software-reliant system to manage these risks. It defines the organizational roles that must effectively collaborate to engineer systematic resilience processes to avoid gaps and inconsistencies. It also establishes how an organization should ensure it has effective supply chain risk management that supports its mission and objectives. The ASF contains proven and 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

Looking back, we can see a pattern of attacks targeting the supply chain. Likewise, organizations have not considered the risks and weaknesses inherent in their supply chains. Over the years, the Software Engineering Institute's (SEI's) experience in cybersecurity, risk management, and acquisition/operations enabled it to research these attacks and supply chain weaknesses and failures to develop guidance for organizations.

Examples of Cybersecurity Attacks

Concern for cyber risk has been growing due to multiple high-impact failures that can be attributed to acquisition and supplier management breakdowns. The potential impact of cybersecurity attacks became evident with the Heartland payment system breach in 2008 [1]. With Heartland, millions of dollars were lost due to a software error for a product from an organization that was fully compliant with all regulatory mandates. At the time, this incident 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 Brands, Inc. attack in December 2013 expanded the concern for supply chain risk. In this successful attack, the perpetrators used stolen credentials from a supplier to connect to Target's operational environment and 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 [2].

New impacts from the increasing 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 [3].

The Inherent Risks of Supply Chains

In a 2010 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 represented a failure to consider the responsibilities the acquirer must assume based on the lifecycle use of third-party products. As a result, organizations were exposed to an extensive range of cyber risk that increased over time [4].

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 fails to address the following:

- the increasing supplier role in providing software and services
- system designs that provide increased and frequently unexpected access to software
- the introduction of weaknesses into software-reliant systems that are reachable by an attacker

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 are critical to reducing the potential success of cyberattacks [5].

Organizations' Ineffective Cybersecurity Practices

During that 2010 research project, we found that few programs were implementing effective cybersecurity practices and supplier oversight early in the acquisition lifecycle. Figure 1 shows the wide range of practices that were available for use but that were not integrated into standard practice.

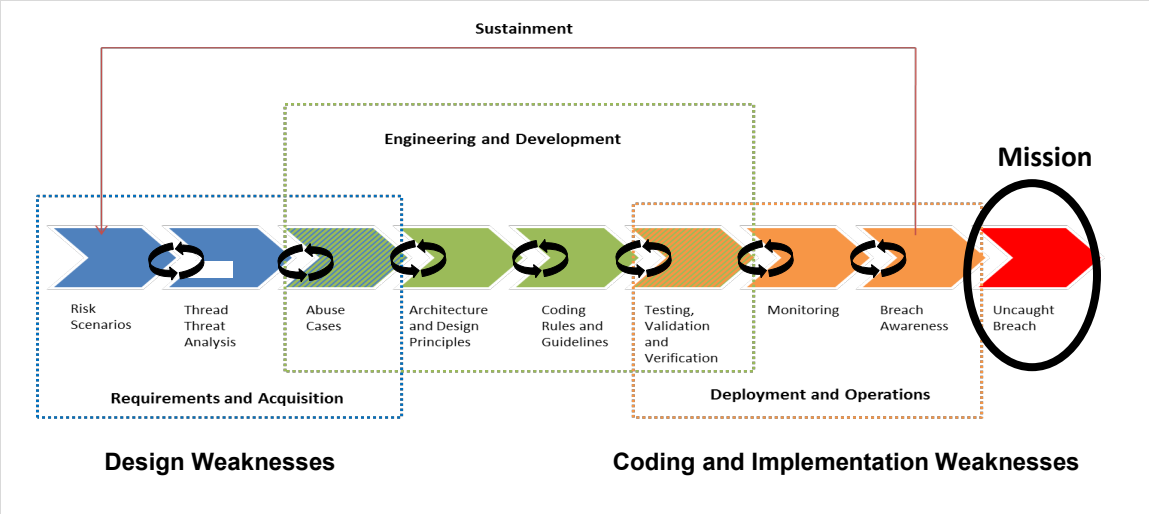

Figure 1: Cybersecurity Practices Available Across the Lifecycle to Address Security Weaknesses

SEI Research and Guidance

In the SEI's CERT Division, supplier-oriented risks were a key factor driving early research into more effective methods for managing cyber risks. We clearly recognized that the growing complexity of threats required organizations to use more structured approaches to cyber risk management. The interconnected nature of cybersecurity among internal and external stakeholders requires a more collaborative and integrated approach that systematically and proactively manages security. Not only do organizations need better security methods, but their expanding outsourcing strategies raise major concerns that their suppliers also need better security management processes and tools.

Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes [6], published in 2007, was the first release of these innovative concepts, helping to reset security management approaches and forming the basis for work that continues to evolve today.

The *CERT Resilience 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 [7].

In 2015, CERT researchers 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)* [8].

Based on the CERT-RMM, the CRR establishes a baseline of cybersecurity capabilities that helps an organization understand the following:

- its operational resilience
- its ability to manage cyber risks to critical services during normal operations as well as during times of operational stress and crisis

A Culmination of Prior SEI Research and Guidance

Based on the prior work at the CERT Division, in 2016, researchers from 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 [9], addressing the issues covered thus far. (Figure 2 provides a summary of the ASF's lineage over the last thirty years.)

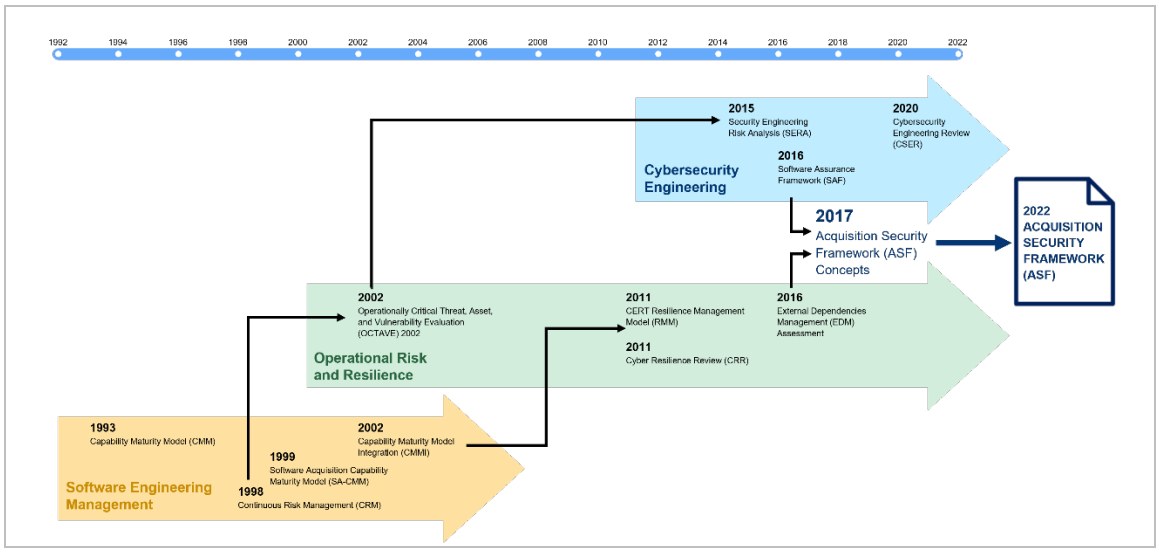

Figure 2: Historical Research Lineage of the Acquisition Security Framework

The Acquisition Security Framework (ASF)

Managing supply chain cyber risk is especially challenging because it is broad and pervasive, and responsibility is spread widely across multiple organizations. Today's complex threats and organizational structures increasingly call for a more systematic approach to managing multiple internal and external stakeholders.

The CERT Division's *Acquisition Security Framework (ASF)* is an integrated, systems-oriented perspective that considers the full supply chain risk management lifecycle [9]. It applies not only to daily operations but also to efforts to build ever more complex systems of systems supported using a mix of internal and supplier-based resources.

Acquisition and development must consider the operational context and plan for sufficient risk management, and operations must establish processes that effectively integrate each added supplier into ongoing processes and practices.

The 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. The framework provides a mechanism for the following:

- increasing an organization's confidence about the level of its vendors' performance
- improving its understanding of potential gaps
- making improvements based on a suggested roadmap

The ASF outlines a process management approach that provides an infrastructure for efficiently engineering technology and collaborating with suppliers to deliver and operate complex systems.

Development of the ASF

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 continues today and 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 process-based techniques that are designed to manage cyber risk from early requirements definition through operations. These new techniques have brought improved methods and outcomes, including a lifecycle orientation shared by DevSecOps and the ASF. Facilitating integrated cybersecurity in environments with complex supplier-dependent systems demands these innovative solutions.

How the ASF Works for Supply Chains

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 nearly every aspect of the organization. The need for organizations to access a wide range of technical skills to create, integrate, and support the multi-faceted capabilities that have become operational necessities drives their greater reliance on suppliers. Therefore, managing potential supply chain risk requires processes that foster effective collaboration across the many participants interacting with each of the organization's suppliers over time.

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

- Program Management
- Engineering Lifecycle
- Supplier Dependency Management
- Support
- Independent Assessment and Compliance
- Process Management

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 expansive management requires processes that enable those who are performing practices in the six practice areas to effectively connect and continuously collaborate since all aspects of 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.

The ASF Structure

As mentioned in the previous section, the framework contains six practice areas: Program Management, Engineering Lifecycle, Supplier Dependency Management, Support, Independent Assessment and Compliance, and Process Management. As shown in Figure 3, each practice area has two or three domains. Within each domain, there are at least six goals. Each goal has a group of practices that support that goal. The practices are phrased as questions that an organization can use to determine and evaluate current and planned organizational capabilities.

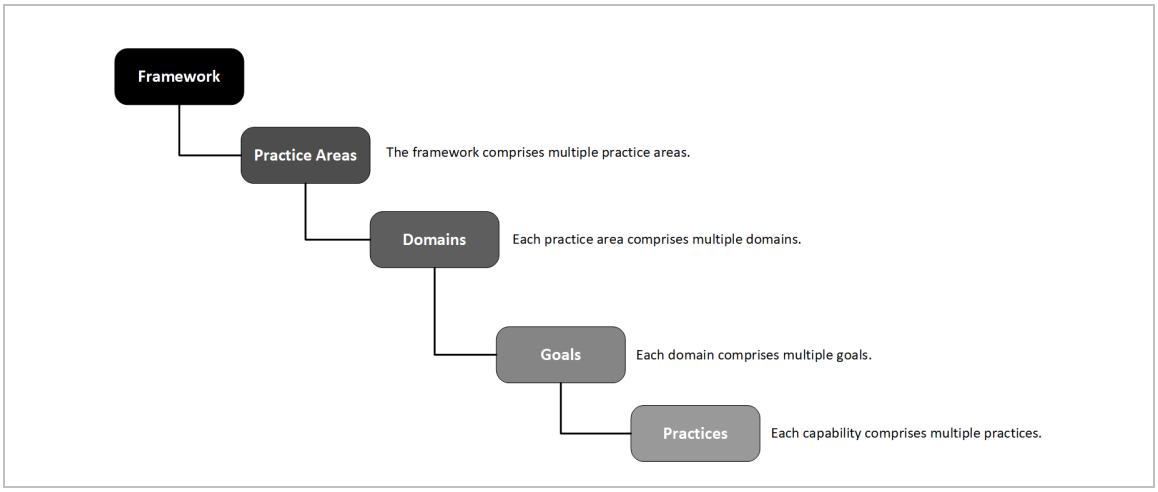

Figure 3: ASF Organizational Structure

Many ASF practices interrelate to support the communication that must continually occur among those implementing the practice area goals and practices. Currently, limited collaboration and communication among system teams about tasks that require supplier management creates potential risks.

An example of poor collaboration is when program leaders are not aware of risky choices made by acquisition and engineering teams or that the organization's relationships with its suppliers are not being managed effectively.

An example of effective collaboration is when practices in the Engineering Lifecycle domain 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 the previous work we described earlier in the Background section. Working with subject matter experts, we also have assembled practices for two of the remaining four areas.

In the remainder of this section, we share a summary of the information we assembled about the domains and goals from the practice areas we have developed so far.

For **Program Management**, we identified the following domains:

- *Domain 1: Program Planning and Management* covers goals related to integrating security/resilience into a program's planning and management activities.
- *Domain 2: Requirements and Risk* covers goals for managing security/resilience requirements and risks at the program level.

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

- *Domain 1: Engineering Infrastructure* covers goals related to infrastructure development, operation, and sustainment.
- *Domain 2: Engineering Management* covers goals related to technical activities and product risk management.
- *Domain 3: Engineering Activities* covers goals related to 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:

- *Domain 1: Relationship Formation* covers goals related to planning, formal agreements, supplier evaluation, and supplier risk.
- *Domain 2: Relationship Management* 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: Supplier Protection and Sustainment* covers goals for supplier disruption, maintenance, and situational awareness.

For **Support**, we identified the following domains:

- *Domain 1: Program Support* covers goals to ensure that security/resilience training, resources, and assistance are available to the program or system as needed.
- *Domain 2: Security Support* covers goals to provide oversight and management of the program's security-related activities.

Next Steps for the ASF

We are actively developing the remaining two practice areas: Independent Assessment and Compliance and Process Management.

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

Building the ASF is clearly a challenge, but the larger concern is making sure that the approach is usable by those who need it. Our supply chain risk focus must shift from selecting guidelines that suppliers should follow to improving collaboration among the parts of the acquiring organization that interact with suppliers to establish clear and effective actions and measures for effective management. To that end, we have taken this multi-pronged 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

[1] M. Gordover, "Lessons Learned from the 2008 Heartland Breach," 19 March 2015. [Online]. Available: https://www.proofpoint.com/us/blog/insider-threat-management/throwback-thursday-lessons-learned-2008-heartland-breach. [Accessed 27 September 2022].

[2] Aorato Labs, "The Untold Story of the Target Attack Step by Step," August 2014. [Online]. Available: http://aorato.webstick.co.il/labs/report/untold-story-target-attack-step-step/#. [Accessed 27 September 2022].

[3] D. Temple-Raston, "A Worst Nightmare" Cyberattack: The Untold Story of the SolarWinds Hack," 16 April 2021. [Online]. Available: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack. [Accessed 27 September 2022].

[4] R. Ellison, J. Goodenough, C. Weinstock and C. Woody, "Evaluating and Mitigating Software Supply Chain Security Risks," 2010. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9337. [Accessed 27 September 2022].

[5] C. Alberts and C. Woody, "Prototype Software Assurance Framework (SAF): Introduction and Overview," 2017. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=496134. [Accessed 27 September 2022].

[6] R. A. Caralli, J. F. Stevens, C. M. Wallen, D. W. White, W. R. Wilson and L. R. Young, "Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes," 2007. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8389. [Accessed 27 September 2022].

[7] R. A. Caralli, J. H. Allen and D. W. White, CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience, Addison-Wesley, 2011.

[8] DHS, "Assessments: Cyber Resilience Review (CRR)," 2014. [Online]. Available: https://www.us-cert.gov/ccubedvp/self-service-crr. [Accessed 27 September 2022].

[9] C. Alberts, C. Woody, C. Wallen and J. Haller, "Assessing DoD System Acquisition Supply Chain Risk Management," *CrossTalk,* May/June 2017.

Legal Markings

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.

DM22-0886

Contact Us

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

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu