SYM-AM-24-031

# Excerpt from the Proceedings of the Twenty-First Annual Acquisition Research Symposium

## Acquisition Research: Creating Synergy for Informed Change

May 8–9, 2024

Published: April 30, 2024



Prepared for the Naval Postgraduate School, Monterey, CA 93943.

The research presented in this report was supported by the Acquisition Research Program at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).


ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

# Improve Acquisition Cybersecurity Risk Using the Acquisition Security Framework and Software Bills of Materials Risk Framework

**Dr. Carol Woody—**is principal researcher for the CERT Division of the Software Engineering Institute (SEI). She focuses on cybersecurity engineering for building capabilities and competencies to measure, manage, and sustain cybersecurity and software assurance for highly complex software-reliant systems and systems of systems. She has been a member of the CERT technical staff for over 20 years. Dr. Woody coauthored the book Cyber Security Engineering: A Practical Approach for Systems and Software Assurance, published as part of the SEI Series in Software Engineering. The CERT Cybersecurity Engineering and Software Assurance Professional Certificate, a self-paced online training program, is based on research she led. [cwoody@cert.org]

**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. Today, Wallen works closely with the CERT Division of the Software Engineering Institute on initiatives to strengthen the resilience of critical infrastructure, to improve software assurance, and to enhance and/or refine techniques for managing supply chain risk. [cmwallen@sei.cmu.edu]

**Christopher Alberts—**is a principal cybersecurity analyst in the CERT Division of the Software Engineering Institute 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 coauthored two books and published over 50 technical reports and articles. Alberts has BS and ME degrees in engineering from Carnegie Mellon University. [cja@cert.org]

**Michael S. Bandor—**is a senior software engineer in the Software Solutions Division of the Software Engineering Institute. He has 34 years of experience with Department of Defense systems, including business, command and control, satellite, aircraft, and ground-based radar systems. Bandor has been with the SEI for 19 years. Prior to the SEI, Bandor served in the United States Air Force from which, after a career spanning more than 22 years, he retired in 2005 as a Senior Noncommissioned Officer. [mbandor@sei.cmu.edu]

## Abstract

Increasingly, complex, software-intensive systems rely on software from third parties. However, recent events, such as MoveIT, SolarWinds®, and Log4j™ (Liu, 2021), demonstrate the profound cybersecurity consequences of lax third-party component management. Too often, these components are unknown, and suppliers are only beginning to be incentivized to consider the risk their products pose. For their part, acquirers remain primarily focused on cost and schedule. To help manage these challenges, and to deliver a secure-by-design outcome, the Carnegie Mellon University Software Engineering Institute (SEI) developed the Acquisition Security Framework (ASF). The ASF describes practices needed across the supply chain to reduce risk gaps.

In a derivative effort, the SEI also developed the Software Bills of Materials (SBOM) Framework, a set of SBOM practices and process for managing risk. Building and using SBOM requires heightened collaboration between suppliers and acquirers. Achieving effective SBOM results requires planning, tooling, trained staff, measurement, and monitoring, because technology and its use is always changing. Information available from an SBOM can offer insights into the

challenges faced by the groups engaged in managing a system. This paper describes both frameworks and the opportunities for improving acquisition cybersecurity risk provided by each.

## Introduction

Software supply chain risk has increased exponentially since 2009 when the Heartland Payments System breach (King, 2009) made the issue newsworthy. The perpetrators reaped 100 million debit and credit card numbers. At the time, this was the largest data breach in recorded history, but it would not remain so. Recent events in 2020 and 2021, such as SolarWinds and Log4j, a popular logging package for Java (Liu, 2021), show that the scale of disruption from a third-party software supplier can be massive as organizations grow their dependence on software-reliant technology.

The reuse of software has enabled faster fielding of systems because common components can be sourced externally, but all software comes with vulnerabilities, and attackers have expanded their capabilities to exploit them in products that have broad use. Virtually all products or services that an organization acquires are supported by, or integrated with, information technology that includes third-party software and hardware components and services. Each component represents a potential source of cybersecurity risk. For many organizations, information about the acquisition of products or services, practices, and decision points critical to monitoring and managing their supply chain risks and operational implementation is scattered. Security and supplier risk management typically lie outside of the engineering efforts that manage system and program risk management. However, dependency on systems, networks, and the multitude of suppliers necessary to support that environment is unprecedented. Managing the risk of those dependencies and environments has become a primary personal, business, and governmental imperative. Unfortunately, many organizations have resisted changing their approach to managing risk to systems, suppliers, and software. Instead, they have continued to rely on checklists, adding more regulation, and using software development and operational methods that do not effectively address the risk challenges.

Short-term budget and schedule demands become key drivers that can distract from more efficient, effective, secure, and resilient approaches to managing technology and systems. However, resilience and security are elusive goals that require new methods, risk-driven organizational cultures, and strong leadership to achieve. But what do we mean by terms like resilience and security? The terms security and resilience, while sometimes used interchangeably, offer different emphases and perspectives on managing cyber risk. Both perspectives are important, and rather than attempting to parse the differences, this paper uses both terms and recognizes their interdependence. The National Institute of Standards and Technology (NIST), has established the following definitions (National Institute of Standards and Technology, 2021):

> **Cybersecurity**—Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
>
> **Cyber Resilience**—The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency responds to any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning.

Many Software Engineering Institute (SEI) solutions share a common theme: using technology to enable mission success. This theme has driven the development of several innovative SEI solutions, such as the Capability Maturity Model Integration (CMMI); the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE); and the CERT Resiliency Management Model (CERT-RMM). These solutions resulted in highly influential bodies of knowledge that have informed the subsequent development of many methods, tools, and techniques, including the Acquisition Security Framework (ASF). However, the ASF's research influences are not limited to CMMI, OCTAVE, and CERT-RMM. As illustrated in Figure 1, the ASF has been influenced by a rich SEI research lineage that includes software engineering management, operational risk and resilience, and cybersecurity engineering.

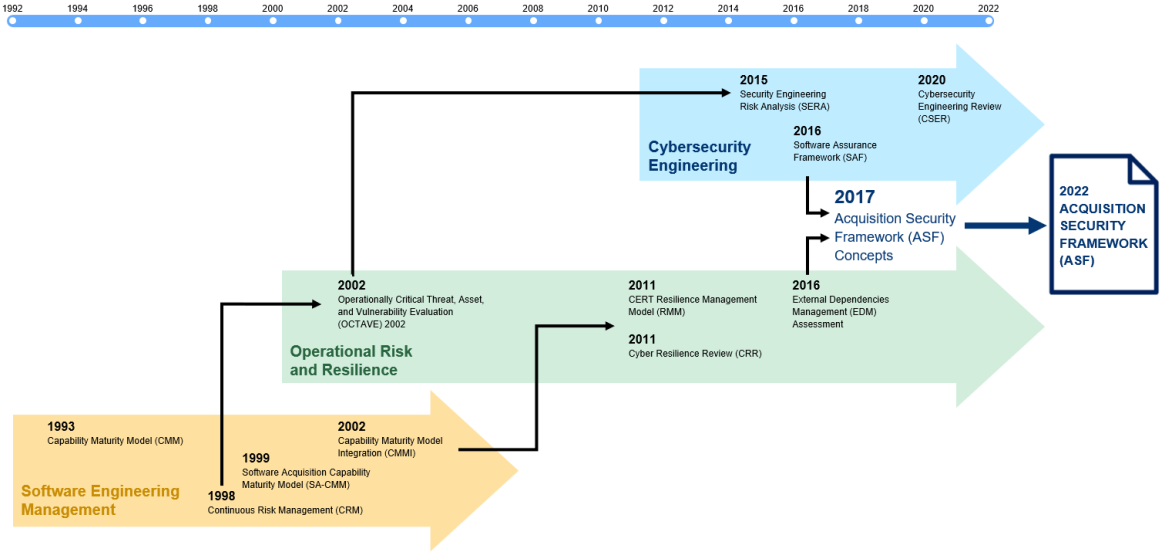


**Figure 1: Research Lineage of the ASF**

To facilitate the management of software and third-party challenges, and to deliver a Secure by Design outcome, the SEI has developed an ASF that describes the practices needed across the supply chain to reduce risk gaps. To help address software risk, the ASF and the methods it leverages were utilized to build a Software Bills of Materials (SBOMs) framework. SBOMs have come to the forefront of efforts to strengthen software risk management and transparency that can help manage suppliers and software components that are a common aspect of today's application development process.

Based on our broad experience helping organizations address engineering, security, and supplier risks, the SEI team assembled the following six key principles for use in developing and applying a framework to remedy the gaps described above:

- **Risk Based**—A risk-based management approach improves decision-making, enables effective identification and management of security/resilience risks, and facilitates prioritization of security/resilience activities and resources based on mission impact.
- **Lifecycle Focused**—Security/resilience practices must be integrated consistently into each lifecycle phase, from initial concept through system disposal.
- **Process Oriented**—Higher degrees of process management translate to more stable environments that produce consistent results over time.

- **Collaboration Focused**—Teamwork and timely communication across teams and organizations facilitate effective security/resilience management.
- **Context Sensitive**—Implementation of security/resilience practices must consider the organizational context in which these practices are being applied, including program and organizational requirements, operational mission, supplier network, and lifecycle phase.
- **Software Focused**—Systems are increasingly software intensive and complex, requiring an integrated acquisition, engineering, development, and operational focus to manage security/resilience risks.

The ASF supports improved decision-making to effectively address threats and vulnerabilities in a timely manner using risk considerations to prioritize security/resilience activities and resources based on mission impact. This approach recognizes the importance of proactively managing risks by investing in security/resilience activities that target risk levels acceptable to the program or system.

The ASF establishes a systematic, integrated process of engineering, developing, implementing, operating, and retiring information systems and programs. This approach emphasizes the importance of a collaborative approach to managing programs, teams, and systems that recognizes the importance of building software-reliant systems that consistently address security/resilience risks in the face of change and evolving threat environments.

The ASF emphasizes management of activities and practices that target the achievement of programmatic goals. Process improvement is a key aspect of the ASF. It promotes ongoing refinements to existing activities and practices. Process management treats change as continuous and expected, requiring ongoing effort to ensure that processes remain effective at adapting to evolving program and system objectives.

The ASF establishes active linkages among teams, systems, and processes across participating organizations. Integration facilitates collaboration and communication directed toward a common set of goals. This integrated approach leads to increased efficiency, improved productivity, and more effective risk management.

ASF goals and practices provide an actionable, context-sensitive roadmap for managing security/resilience across the systems lifecycle and supply chain. These goals provide a conceptual foundation that can be tailored to an organization's specific context and mission. In addition, the ASF's principles and underlying philosophy can be applied to other types of security/resilience problems, such as integrating an SBOM into an acquisition program's security/resilience risk management practices.

Software is a growing component of modern business and mission-critical systems. As a result, software assurance is becoming increasingly important to programs across all sectors. A key aspect of software assurance is keeping security and resilience risks within acceptable tolerances across the systems lifecycle. The ASF leverages acquisition, engineering, and assurance disciplines to build security/resilience into software and systems across the lifecycle.

## Acquisition Security Framework

The SEI team applied the principles and concepts described above to create the ASF. ASF is a framework of leading practices and processes for managing the security/resilience of applications and systems of systems. The ASF facilitates an integrated approach to cyber risk management across a system's lifecycle and supply chains. The motivation for developing the ASF came from a need for innovative methods to manage third-party/acquisition risk, the growing role of software in systems, the lack of integration among support teams, and the

complexity of systems. Key to meeting these challenges is taking a multidisciplinary approach to managing cyber risk over a system's lifecycle, and the ASF incorporates this necessity.

Many security/resilience solutions focus on a few aspects of engineering, such as security/resilience requirements specification, secure coding practices, or supply chain risk management. In contrast, the ASF leverages a proven set of integrated program management, engineering, and supplier management practices and processes that span the systems lifecycle. ASF practices promote proactive dialogue across all program and supplier teams, helping integrate communication channels and facilitate information sharing. As a result, the ASF enables programs to acquire, develop, and operate complex systems that function at a lower level of risk in an increasingly contested, challenging, and interconnected cyber environment.

The ASF is designed to help a program coordinate the management of engineering and supply chain risks across system components, including hardware, network interfaces, software interfaces, and mission capabilities. The ASF includes 51 goals and 334 practices spread across the following six practice areas:

1. Program Management
2. Engineering Lifecycle
3. Supplier Dependency Management
4. Support
5. Assessment and Compliance
6. Process Management

Within each practice area, critical domains are identified, and questions relevant to the analysis of goals for each domain are provided. ASF goals and practices provide a roadmap for managing security and resilience across a system's lifecycle and supply chain. The response to each question gives an organization or program insight into how well each practice is addressed and where there may be potential concerns. The ASF defines engineering-driven, risk-based practices and processes for building, deploying, and operating secure and resilient systems. The following sections describe each of the six practice areas. Details about the domains, goals, and practices for each practice area are available in the SEI technical note *Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk* (Alberts et al., 2022).

**Program Management**

From a traditional perspective, program management is focused on controlling cost, schedule, and performance. In the ASF, the Program Management practice area defines a set of practices for ensuring that security/resilience are addressed from the earliest stages of an acquisition and throughout the systems lifecycle. Including security/resilience considerations during a program's early planning and management activities provides a foundation for coordinated and integrated management of security/resilience across all program teams. The Program Management practice area also identifies security/resilience practices for requirements and risk management that are coordinated across the program and lifecycle.

**Engineering Lifecycle**

The term *engineering lifecycle* describes the range of management and technical activities needed to build and operate a system, from initial concept though development, production, deployment, and support. In the ASF, the Engineering Lifecycle practice area defines a set of practices for integrating security/resilience into a program's systems engineering and software engineering activities. In addition to addressing the technical aspects of security/resilience engineering, the Engineering Lifecycle practice area also ensures that the program's engineering activities are planned and managed, including those performed by third-

party contractors. Finally, Engineering Lifecycle practices ensure that engineering processes, software, and tools (i.e., the engineering infrastructure) are secure and resilient, reducing the risk of attackers being able to disrupt program and system information and assets.

**Supplier Dependency Management**

A broad network of contracted and non-contracted suppliers enables a program access to specialized skills, components, and infrastructure in a cost-effective manner. At the same time, these supplier relationships create dependency risks that must be managed in the context of the program's overall risk management strategy. Suppliers of products and services that are governed by contractual agreements require careful management and monitoring. Some suppliers, such as infrastructure providers and government service providers, do not typically rely on contracts to codify relationships, leading to dependency risks that are frequently overlooked. While non-contracted suppliers are often less of a concern, programs must manage security/resilience risks resulting from these dependencies as well. In the ASF, the Supplier Dependency Management practice area provides leading practices for managing dependencies that should be considered when building secure/resilient systems.

**Support**

As it works toward its acquisition and development mission, a program requires support from a variety of organizational departments, groups, and teams. Organizational support activities provide a broad range of services, including security management, facility management, access management, measurement and analytics, and training. The Support practice area outlines leading practices that facilitate integrated support for acquiring, developing, and managing secure/resilient systems across their lifecycle.

**Independent Assessment and Compliance**

An independent assessment is an activity in which individuals who are not directly connected with a program or system evaluate some or all aspects of that environment and report the results to designated stakeholders. Compliance is the act of conforming to the requirements outlined in the set of laws, regulations, policies, and standards that a program or system must meet. In the ASF, the Independent Assessment and Compliance practice area defines activities for reviewing a program or system to determine whether it meets security/resilience requirements, including customer, product, and product component requirements, and whether it fulfills its intended use when placed in its target environment.

**Process Management**

Process management comprises practices that facilitate the predictable and efficient delivery of program activities, putting the program in a position to achieve its security and resilience objectives. Process management practices help clarify and align an organization's strategies, policies, procedures, standards, and approach. A key premise of process management is that organizational outcomes are highly influenced by the quality of its processes. Increased use of consistent process management translates to more stable environments that produce predictable results over time and help enable mission success at lower risk. In addition, process management is based on the principle that change is continuous. Managing change in a program or system environment requires continual management and improvement of processes, helping to ensure that those processes continue to meet their objectives. A key challenge to every acquisition program is implementing an appropriate level of process management that reflects its environment, mission, and objectives. The ASF leverages process management to help ensure that cyber investments are implemented and managed effectively across the program and its suppliers. In the ASF, the Process Management practice area defines activities for managing and improving the processes used to acquire, develop, and operate software-reliant systems.

## Leveraging ASF to Address SBOM Challenges

Teams of business and technology experts must collaborate and develop new techniques for identifying potential risks and proactively managing (i.e., tracking, analyzing, and mitigating) risks. SBOMs can help facilitate the building of those new techniques and foster the necessary collaboration. The U.S. Department of Commerce (DOC) defines an SBOM as follows (Department of Commerce [DOC], 2021):

> **An SBOM** is a formal record containing the details and supply chain relationships of various components used in building software. In addition to establishing these minimum elements, this report defines the scope of how to think about minimum elements, describes SBOM use cases for greater transparency in the software supply chain, and lays out options for future evolution.

SBOMs have come to the forefront of efforts to strengthen cybersecurity risk management tools, which was a highlight of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, issued on May 12, 2021 (The White House, 2021). EO 14028 requires U.S. government agencies to enhance software supply chain security and integrity, with a priority on addressing critical software.[1] A key aspect of enhancing software supply chain security and integrity is transparency. Implementing SBOMs for critical software will help establish transparency in the software supply chain. Therefore, EO 14028 calls for standards, procedures, and criteria for providing SBOMs for products directly or publishing them on a public website.

Our survey of SBOM publications and guidance revealed a strong emphasis on defining the content and format of SBOMs. Establishing a standard for SBOM content is an important aspect of the problem; however, organizations also need guidance on how to plan for, develop, deploy, and use SBOMs. As a result, our team at the SEI focused its research activities on the SBOM lifecycle.[2] SBOMs must support more, including (1) proactively considering how to best manage risks posed by third parties, and (2) developing effective mitigations as new or emerging threats and vulnerabilities emerge. There are too many moving parts and risks in today's software-driven technology environments to simply rely on ad hoc or poorly organized SBOM practices and processes.

Developing more comprehensive and collaborative SBOM practice frameworks will offer techniques for effectively establishing and managing proactive software information and risk management programs. Using SBOMs can also provide software developers, integrators, and risk managers with a unique opportunity to collect information that they can analyze, monitor, and act on to manage software components, suppliers/dependencies, provenance, vulnerabilities, and more—the possibilities are extensive.

### Building the SBOM Framework

We started developing the SBOM Framework by reviewing published use cases. Based on this review, we developed core SBOM practices, which primarily focused on developing SBOMs (i.e., building and construction practices) and using them to manage known security

---

1 *Critical software* is defined as software that performs functions critical to achieving trust, such as affording or requiring elevated system privileges or direct access to networking and computing resources.

2 ASF was developed using multiple influential bodies of knowledge that have informed the subsequent development of tools and techniques that have been further refined through extensive use across a range of sectors and industries. The organizational outcomes that result from the ASF approach are characterized by efficient and predictable environments and more manageable delivery and risk outcomes. The SBOM lifecycle refers to the set of activities required to plan for, develop, and use an SBOM.

vulnerabilities and associated risks (i.e., operational use practices).3 We then expanded on this initial set of practices by considering a lifecycle perspective. Here, we identified practices for specifying requirements, developing plans, and allocating resources needed to build and use SBOMs. Finally, we identified practices for activities that enable and support operational use of SBOM data. These practices include management and support practices, third-party practices, and infrastructure practices. The result is an SBOM Framework comprising the following six goals:[4]

1. Requirements
2. Planning
3. Build/Construct
4. Deploy/Use
5. Manage/Support
6. Infrastructure

The framework currently includes 44 practices distributed across the six goals. It provides a starting point for integrating SBOMs with a program's security risk management practices. As we collect lessons learned from piloting the framework and gathering feedback from the community, we will update the framework's goals and practices as appropriate.

**Leveraging SBOM practices**

SBOMs have been primarily designed to help organizations build more structure into the management of software risks. That management must include not only identifying, but effectively mitigating, security and resilience risks in systems. Clearly, much more can be done to facilitate a broader benefit of using SBOMs. Data from SBOMs, while a key factor in managing risk, have many other possible uses and innovations.

Achieving effective SBOM results requires planning, tooling (because the scale is too great), training staff to do the job, measuring, and monitoring. Information that can be gathered from an SBOM can offer insights into the challenges faced by the groups engaged in managing a system. Figure 2 depicts some of the support teams that could use and benefit from SBOM information and processes to improve software and systems. The SBOM Framework largely focuses on the risks posed by software components and the suppliers who develop and/or manage that software. There are many other potential uses of, and innovation opportunities for, SBOM use, particularly given the vast data that SBOMs can provide.

---

3 An SBOM has multiple operational uses, including managing known security vulnerabilities, software versions and licenses, code reuse, and software end-of-life issues. The SBOM Framework focuses on managing security vulnerabilities and risks.

4 There is not a separate goal for third-party practices in the SBOM Framework. Third-party practices are included in Goal 1 (Requirements) and Goal 5 (Manage/Support).

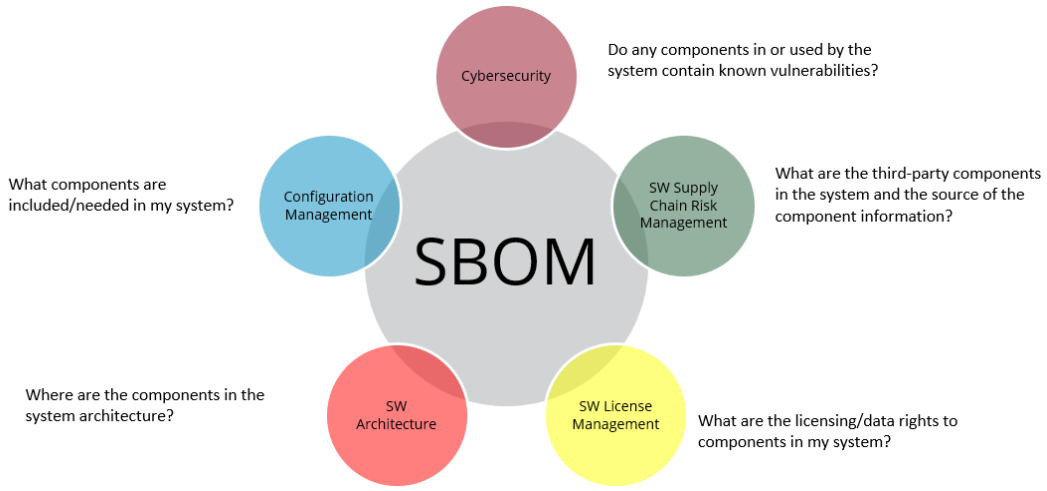


**Figure 2: SBOM Relationships With Other Areas**

The SBOM Framework addresses the establishment of processes to manage multiple SBOMs and the vast data that they can provide; however, those processes will likely require further tuning as pilot-related activities provide input about improvements and tooling. Data about software risks and vulnerabilities are rich and extensive. Unfortunately, the risk information that SBOMs contain only adds to what is already an overwhelming conglomeration of content and potential information. Organizing and prioritizing that information is a challenge, and we expect that the SBOM Framework can help direct its users' efforts to establish the most effective approach for them. Key to that approach will be the collaborative use of methods and tools by multiple teams involved in software and systems management.

SBOM data analysis can be leveraged to visualize difficult or, in some cases, unseen relationships and dependencies. These relationships and dependencies can be invaluable to teams who manage software in ever more complex technical environments. That benefit was described in *The Minimum Elements for a Software Bill of Materials (SBOM)* (DOC, 2021):

> An SBOM should contain all primary (top level) components, with all their transitive dependencies listed. At a minimum, all top-level dependencies must be listed with enough detail to seek out the transitive dependencies recursively.
>
> Going further into the graph will provide more information. As organizations begin SBOM, depth beyond the primary components may not be easily available due to existing requirements with subcomponent suppliers. Eventual adoption of SBOM processes will enable access to additional depth through deeper levels of transparency at the subcomponent level.

## Conclusion and Next Steps

There is a saying attributed to Benjamin Franklin: "Change is the only constant in life. One's ability to adapt to those changes will determine your success in life." As technology and risks continue to evolve, we must adapt our approaches to meet these new challenges across their lifecycles. The ASF was built using research and leading practice methods developed by the SEI over the last 30-plus years. The ASF concepts, principles, and leading practices provide a roadmap for managing the highly dynamic technology and threat environments we must address today. ASF accomplishes that objective by recognizing that acquisition and suppliers are the lifeblood that supports businesses getting things done. Collaborating with suppliers and

other partners is essential to efficiency and the effective management of operational risk and resilience.

We have applied ASF concepts and principles to build a software-oriented framework for considering security/resilience. That ASF derivation is an SBOM Framework that can be used to build processes and leading practice environments that can address acquisition and software supply chain risk. The SBOM Framework provides a lifecycle programmatic approach to building and managing SBOMs and software risk. The framework was designed to support continuous process and practice improvement, along with measurement and monitoring of the threat environment, to drive effective security/resilience results. An SBOM program can also be leveraged to manage software for multiple cybersecurity data needs and related collaboration among technology support areas.

It is imperative that we move beyond the current compliance-driven mindset and institute a culture of risk management, with responsible information sharing and collaboration among all participants in acquisition and development, across the lifecycle. The ASF and SBOM initiatives explicitly recognize the value of leading practices, process management, and optimization of cyber risk investments, as well as the importance of establishing cyber capabilities that can adapt to change. We have successfully piloted ASF and the SBOM Framework derivative in selected environments and would welcome the opportunity to assist with further pilots to confirm accuracy and completeness. Use the frameworks to improve practices in your organization, and let us know if you see opportunities for enhancing them.

## Acknowledgments



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.



DM24-0377

## References

Alberts, C., Bandor, M., Wallen, C., & Woody, C. (2022, November 11). *Acquisition Security Framework (ASF): Managing systems cybersecurity risk*. Software Engineering Institute.

https://insights.sei.cmu.edu/library/acquisition-security-framework-asf-managing-systems-cybersecurity-risk/

Department of Commerce. (2021, July 12). *The minimum elements for a Software Bill of Materials (SBOM).* https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

King, R. (2009, July 6). *Lessons from the data breach at Heartland*. Bloomberg. https://web.archive.org/web/20140608030215/http:/www.businessweek.com/stories/2009-07-06/lessons-from-the-data-breach-at-heartlandbusinessweek-business-news-stock-market-and-financial-advice

Liu, N. (2021, December 21). *SolarWinds to Log4j: More risk management wake-up calls*. SDxCentral. https://www.sdxcentral.com/articles/news/solarwinds-to-log4j-more-risk-management-wake-up-calls/2021/12/

National Institute of Standards and Technology. (2021, December). *Developing cyber-resilient systems: A systems security engineering approach* (NIST SP 800-160 Vol. 2 Rev. 1). Computer Security Resource Center. https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

The White House. (2021, May 12). *Executive order on improving the nation's cybersecurity* (Exec. Order No. 10428). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/


Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net