



34th Annual **INCOSSE**
international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024



Acquisition Security Framework (ASF): Informing Software Bill of Materials (SBOM) Use

1

Copyright 2024 Carnegie Mellon University.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT®, Carnegie Mellon® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM24-0798



The Supply Chain Challenge

Supply Chain/Acquisition Risk Is Increasing



- Heartland Payment Systems (2009)
- Silverpop (2010)
- Epsilon (2011)
- New York State Electric and Gas (2012)
- Target (2013)
- Lowes (2014)
- AT&T(2014)
- HAVEX / Dragonfly attacks on energy industry (2014)
- DOD TRANSCOM contractor breaches (2014)
- Equifax (2017)
- Marriott (2018)
- SolarWinds (2020)
- Log4j (2021)
- Medibank (2022)
- MOVEit...(2023)

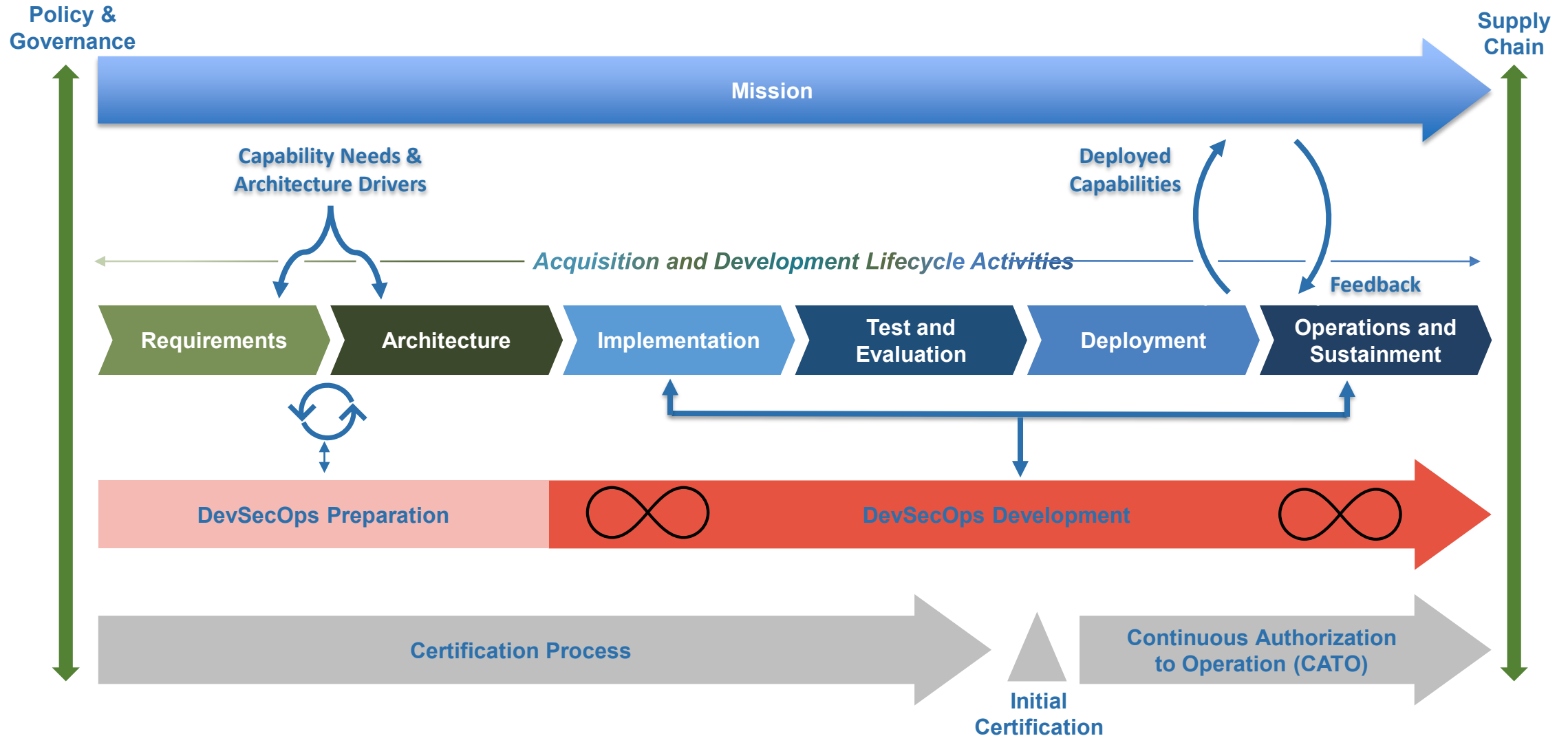
In more than 230,000 organizations, 98% have a relationship with a third party that has been breached within the last two years.

<https://www.securityweek.com/98-of-firms-have-a-supply-chain-relationship-that-has-been-breached-analysis/>

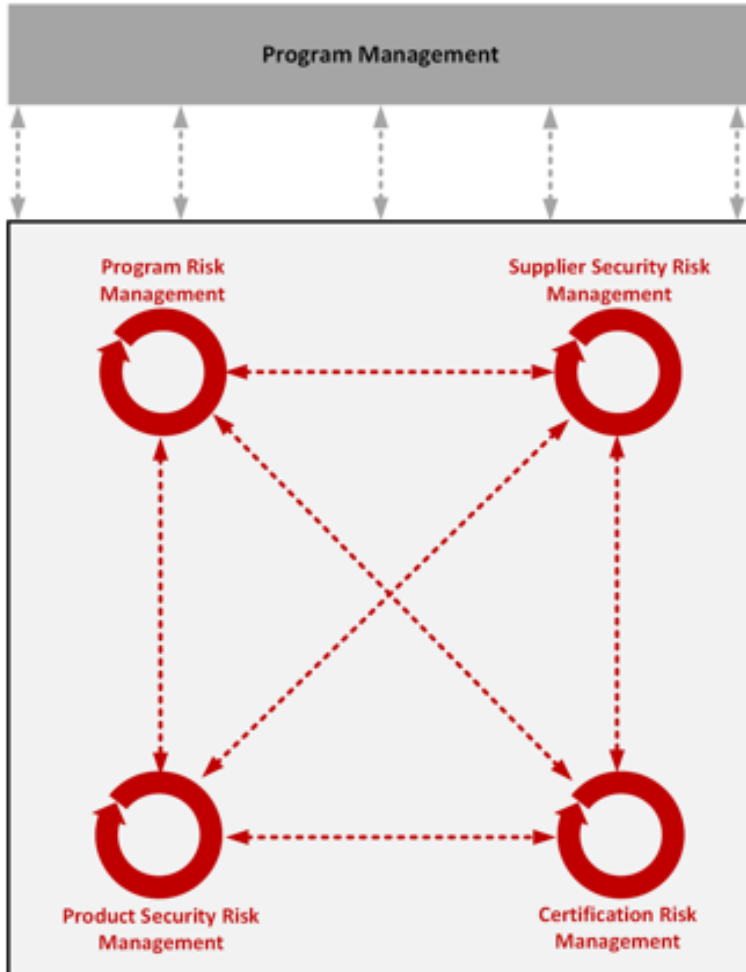
Key Software and Supply Chain Challenges

- Systems are increasingly software intensive and complex
- Third-party components are widespread throughout every system and require an integrated acquisition, engineering, development, and operational focus to ensure sufficient security and resilience.
- Managing relationships with third parties is a critical success factor.
 - A program can no longer effectively manage cyber risks alone.
 - Supply chain risk management requires collaboration.
 - Interactions with suppliers is increasingly data-driven

Acquisition Landscape



Challenge: Integrating Security and Supply Chain Risk Management across the Organization



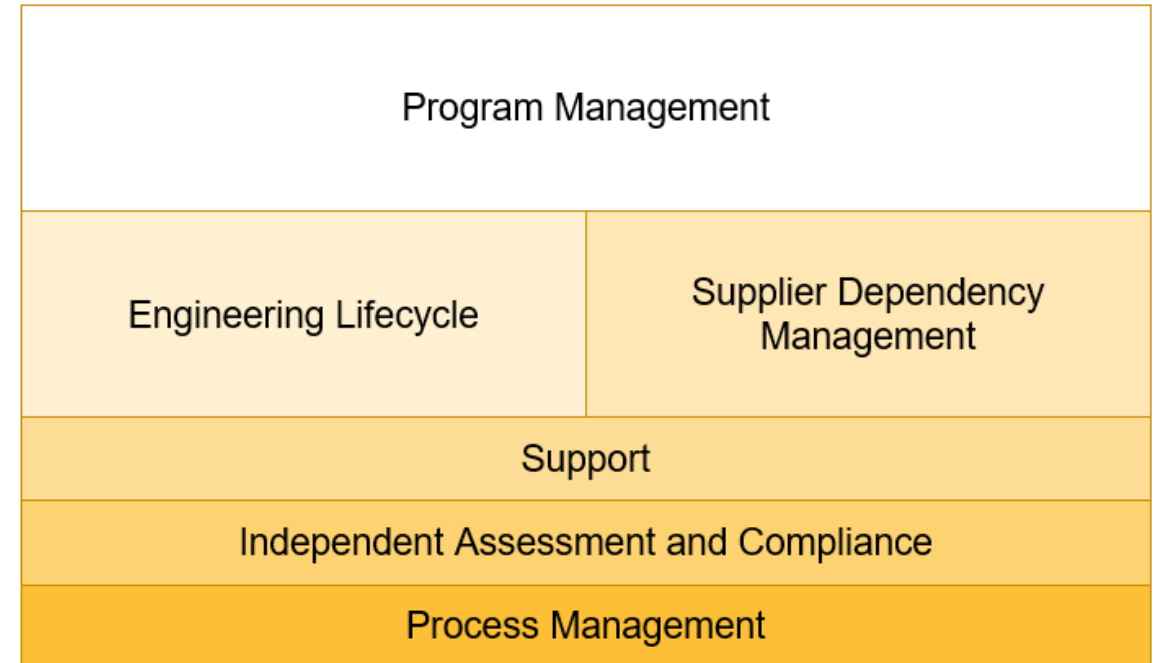
- Security and supplier risk management are typically outside of the program risk management.
- Information is scattered in many documents such as Program Protection Plan (PPP), Cybersecurity Plan, System Development Plan, Supply Chain Risk Management Plan, etc.
- Many activities across the organization are critical to managing cyber risks and must be addressed collaboratively across the lifecycle and supply chain and integrated with program risk management.



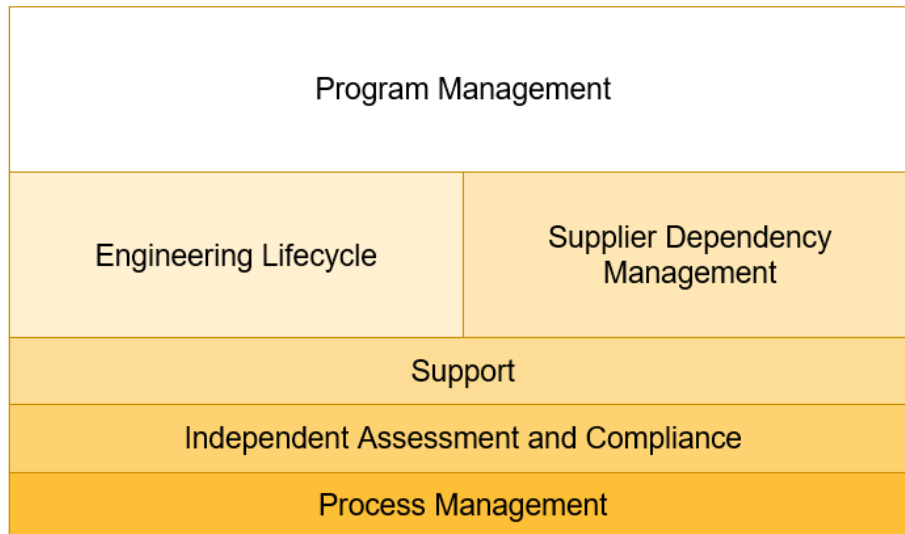
Acquisition Security Framework (ASF)

What is ASF?

- Collection of leading practices for building and managing secure and resilient software-reliant systems linking program management, engineering, and supplier management
- Proactive approach to enabling system security and resilience engineering across the lifecycle and supply chain
- Roadmap for efficiently and predictably building security and resilience into a system for manageable delivery



ASF Goals and Practices



The ASF includes 51 goals and 334 practices spread across the following six practice areas:

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

ASF Key Principles

Risk Based

- Focused on decision making to enable effective identification and management of security/resilience risks

Lifecycle Focused

- Security/resilience practices are integrated into lifecycle phases, from initial concept through system disposal

Process Oriented

- Facilitates more stable environments that produce consistent results over time

Collaboration Focused

- Promotes effective management of results through teamwork and timely communication

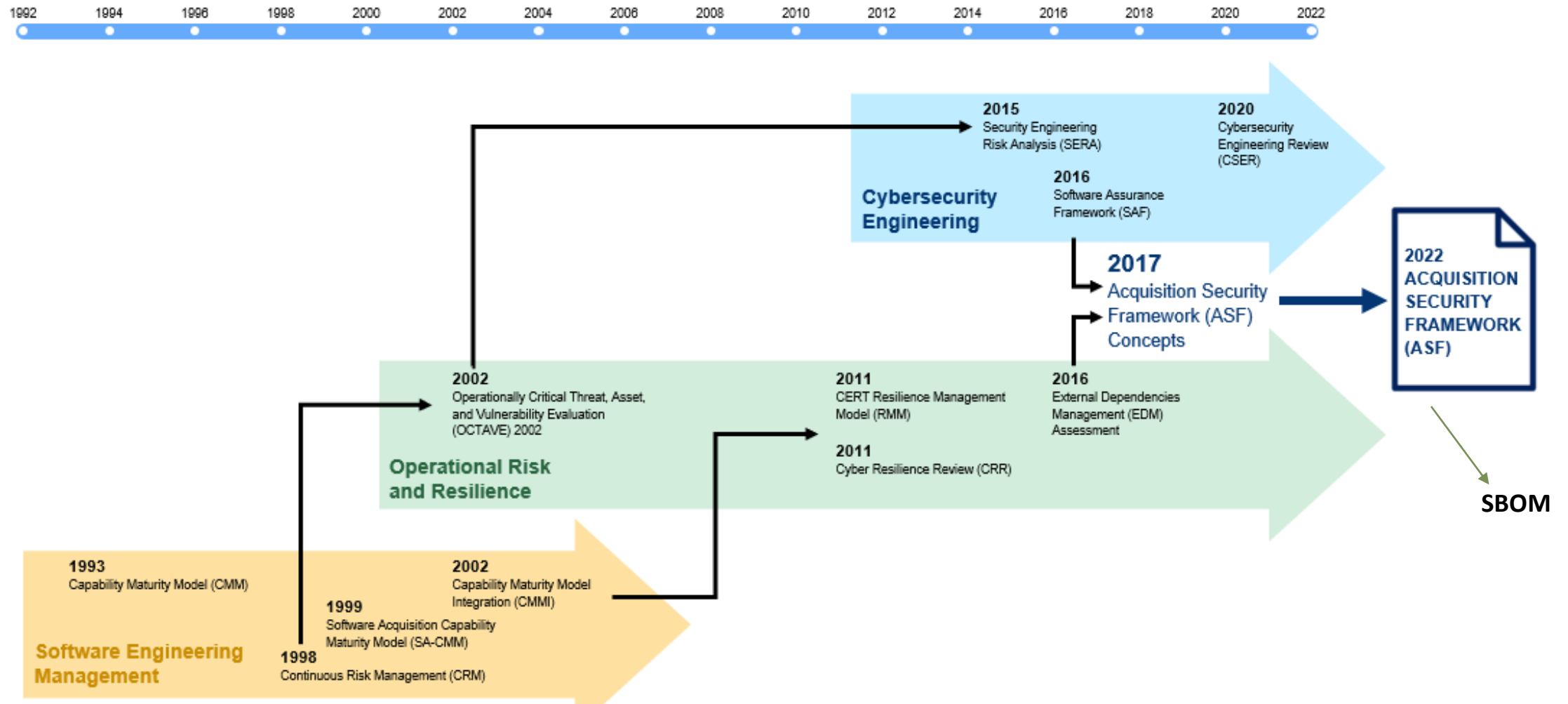
Context Sensitive

- Focused on the organizational context in which security/resilience practices are being applied

Software Focused

- Systems are increasingly software intensive and complex, requiring increased focus on management of security and resilience

ASF Research Lineage



Applied Using Tailored Risk Frameworks

- ASF principles and concepts enable effective management of security and resilience risks across a range of challenges areas.
- Frameworks consistent with ASF principles and concepts can be tailored based on problem space and scope:
 - SBOM Framework (prototype completed)
 - Security Engineering Framework (SEF) delivered to the Cyber Resiliency Office for Weapons Systems (CROWS) to be integrated into the Air Force Systems Security Engineering Cyber Guidebook (SSECG)

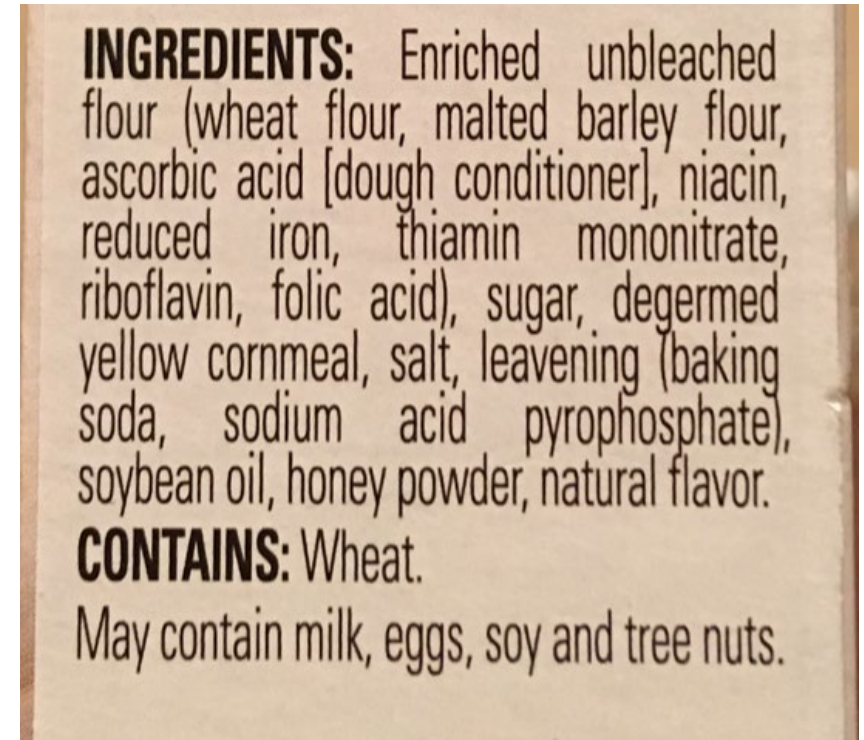


SBOM Framework

What is a Software Bill of Materials (SBOM)

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.¹

SBOMs are mandated under a federal directive EO 14028, *Executive Order on Improving the Nation's Cybersecurity*²



¹ *The Minimum Essential Elements of a Software Bill of Materials*, United States Department of Commerce, July 12, 2021, https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

² *Executive Order on Improving the Nation's Cybersecurity*, White House, 12 May 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

SBOM Framework – Our Approach

1. Surveyed SBOM perspectives and use cases - revealed a strong emphasis on defining the content and format
2. Expanded on existing practices – utilized a lifecycle approach
3. Outlined key activities – requirements, build, deploy, use
4. Determined needed practices – enable ongoing use and management
5. Codified SBOM Framework – five goal areas were identified:
 - *Requirements*
 - *Planning*
 - *Build/Construct*
 - *Deploy/Use*
 - *Manage/Support*
 - *Infrastructure*

Perspectives on SBOM and Use Cases

The Department of Commerce noted in the “Minimum Elements” document that:

“...these are the initial steps and requirements needed to support the basic use cases. There is more work to be done to expand transparency in the software supply chain and to support visibility for securing software.” [Source: Department of Commerce](#) The Minimum Elements For a Software Bill of Materials (SBOM), 2021

Common SBOM Use Cases:

- » **Build an SBOM for a system**
- » Receive and manage third-party SBOMs
- » **Manage known vulnerabilities**
- » Manage software versions
- » Manage code reuse
- » Manage software components that reach end of life
- » Manage software licenses

[Source:](#) National Telecommunications and Information Administration (NTIA) Use Cases Working Group, 2019.

Leveraging ASF to Improve SBOM Use Cases

Activity	Use Case
Requirements	
Plan	
Build / Construct	<i>Build SBOM for system Receive and manage third-party SBOMs</i>
Deploy / Use	<i>Manage known vulnerabilities</i>
Manage / Support	
Infrastructure	

44 practices were developed for activities in the lifecycle that enable and support operational use of the SBOM data

SBOM Framework Goals -- Requirements

Goal 1—SBOM requirements for the program are identified and managed.

The purpose of this goal is to ensure that SBOMs are integrated with the program's security/resilience activities.

- | |
|---|
| 1. Are program goals (e.g., reducing risk, managing system security/resilience) established for using SBOMs? |
| 2. Are program requirements (e.g., required and desired data elements) established for SBOM content? |
| 3. Are program requirements established for using SBOMs to support risk reduction and security/resilience activities? |
| 4. Are criteria/triggers in place for reviewing SBOM requirements? |
| 5. Are SBOM requirements updated periodically based on reviews and lessons learned? |
| 6. Are baseline (i.e., boilerplate) SBOM requirements that apply to all program and system suppliers identified and documented? |
| 7. Are criteria used to evaluate each supplier's ability to meet the program's SBOM requirements? |
| 8. Are SBOM requirements included in formal agreements? |

SBOM Framework Goals -- Plan

Goal 2—A plan for developing and using SBOMs is developed.

The purpose of this goal is to ensure that the programs have a plan for using SBOMs to manage software security/resilience risks.

- | |
|--|
| 1. Are standards, guidelines, and policies for implementing SBOM practices and artifacts established? |
| 2. Are requirements established for implementing SBOM practices and artifacts to support risk management across the program or system? |
| 3. Is sufficient funding allocated for implementing SBOM practices and artifacts across the program or system? |
| 4. Are staff members assigned to implement SBOM practices and artifacts across the program or system? |
| 5. Are roles and responsibilities established for SBOM practices? |
| 6. Do stakeholders understand their roles in implementing, managing, and supporting SBOM practices? |
| 7. Is SBOM training for technical and program staff members provided as needed? |
| 8. Is a plan developed to manage SBOM practices and artifacts across the program or system? |
| 9. Is the SBOM plan monitored and adjusted as needed? |

SBOM Framework Goals – Build / Construct

Goal 3—SBOM data is created for the system, subsystems, and components.

The purpose of this goal is to ensure that accurate and complete SBOM data is created and validated for the system, subsystems, and components.

- | |
|---|
| 1. Does the program's SBOM format meet specified requirements? |
| 2. Is architecture information that identifies software components for each system and subsystem available? |
| 3. Are information sources (e.g., engineering data, licensing data, results of software composition analysis) for creating an SBOM specified and used? |
| 4. Are SBOMs for the system's commercial off-the-shelf (COTS) software, government off-the-shelf (GOTS) software, and open-source software (OSS) available? |
| 5. Is an SBOM created or identified for each software component? |
| 6. Are multiple SBOMs integrated to construct dependency trees for the system? |
| 7. Is SBOM data validated for completeness and accuracy? |

SBOM Framework Goals -- Deploy / Use

Goal 4—Vulnerabilities are identified and managed in SBOM software components, leading to reduced system risk.

The purpose of this goal is to ensure that SBOMs are used to manage vulnerabilities in the system's software components.

- | |
|---|
| 1. Are known vulnerabilities and available updates monitored for software components identified in the system's SBOM? |
| 2. Are vulnerabilities in SBOM components identified? |
| 3. Is the mission risk of each SBOM component assessed? |
| 4. Are software updates prioritized based on their potential impact to mission risk? |
| 5. Are software component reviews/updates conducted based on their mission-risk priorities? |
| 6. Are vulnerability management status, risks, and priorities tracked for each software component? |

SBOM Framework Goals -- Manage / Support

Goal 5—SBOM risks are managed for system components.

The purpose of this goal is to ensure that accurate, complete, and timely SBOM data is available for system components to effectively manage risk.

- | |
|--|
| 1. Are the suppliers for system components identified? |
| 2. Is supplier data reviewed periodically and updated as needed? |
| 3. Are SBOMs for system components identified, analyzed, and tracked? |
| 4. Are SBOMs managed to ensure they are current? |
| 5. Are the risks related to incomplete or missing SBOM data identified and mitigated? |
| 6. Are risks and limitations related to managing and redistributing SBOM information identified and managed? |
| 7. Is the provenance of SBOM data established and maintained? |

SBOM Framework Goals -- Infrastructure

Goal 6—SBOM practices, software, and tools are selected, implemented, and managed.

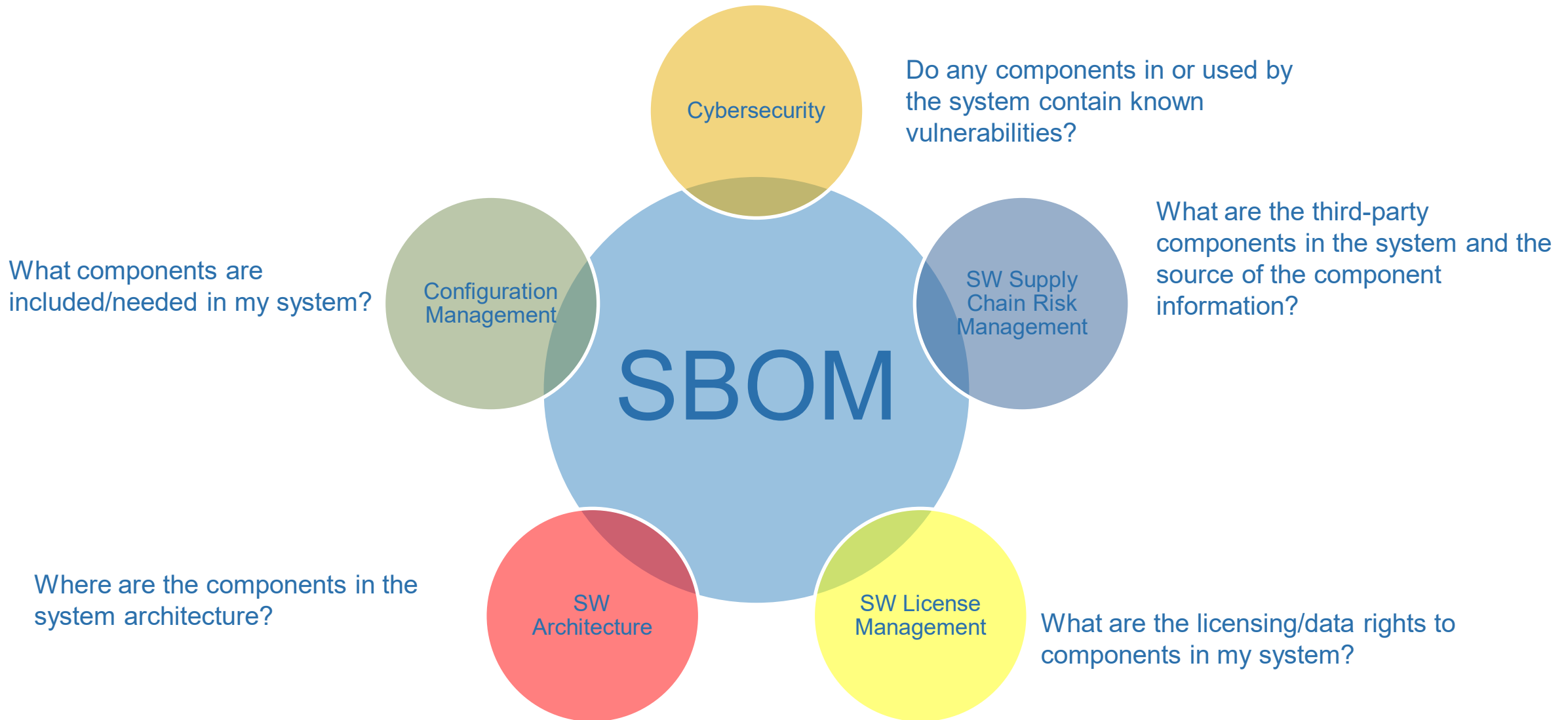
The purpose of this goal is to ensure that SBOM practices, software, and tools are integrated into the program's infrastructure.

- | |
|---|
| 1. Are technical requirements for the SBOM infrastructure developed and documented? |
| 2. Are SBOM practices, software, and tools selected and implemented? |
| 3. Are SBOM practices, software, and tools monitored and managed? |
| 4. Is the security/resilience of SBOM practices, software, and tools managed? |
| 5. Are the integrity and authenticity of SBOM data validated and managed? |
| 6. Is each SBOM and its related artifacts managed across the organization? |
| 7. Is each SBOM and its related artifacts managed for each system? |



SBOM: Visualizing Relationships

SBOM Relationships with Other Areas

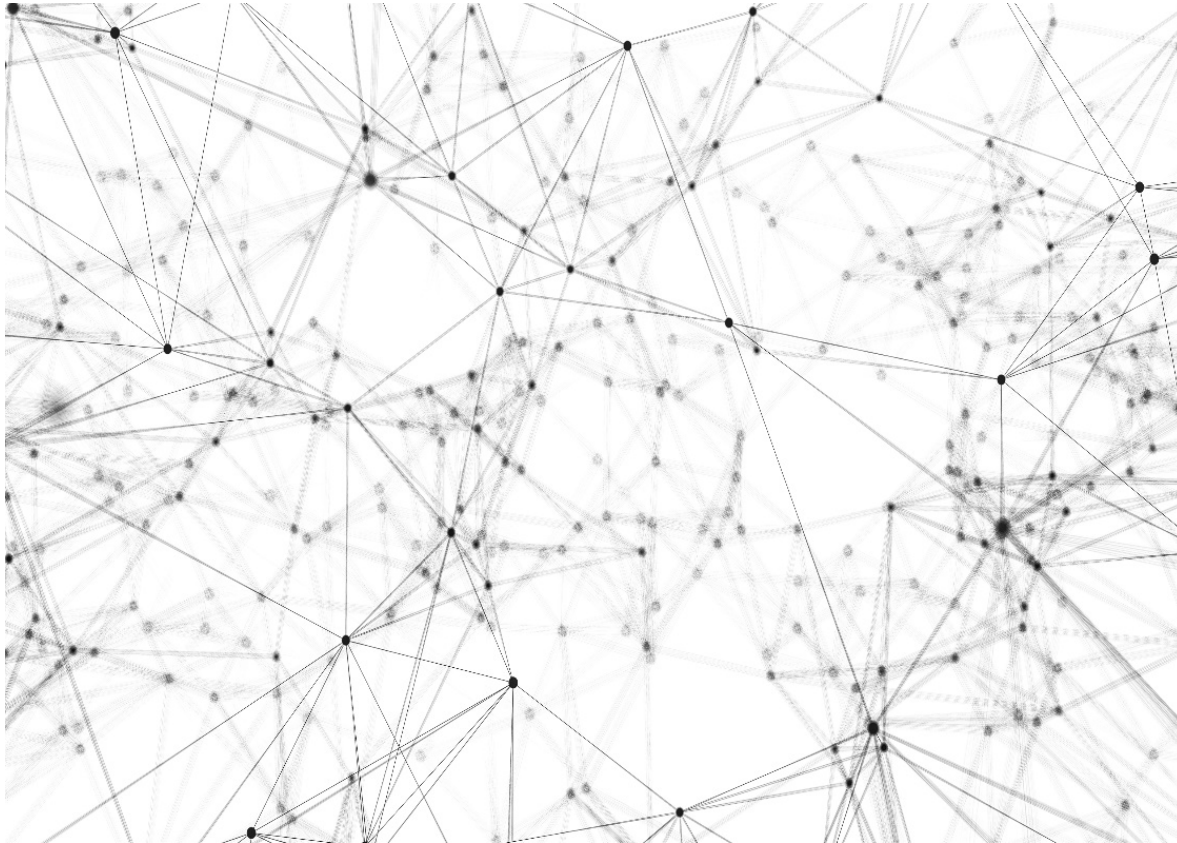


SBOMs at Many Levels



- Organizations tend to focus on the product(s) coming through their development pipeline(s)
- What about the tools in the pipeline(s)? Do you know what is there?
- What about the other software used to support the product?
- How do you get complete situational awareness across the entire program?

Using Graphs to Visualize the Unknown



“Graphs form the foundation of modern data and analytics techniques, with capabilities to enhance and improve user collaboration, Machine Learning models, and explainable Artificial Intelligence.” – Gartner, “Top 10 Tech Trends in Data and Analytics,” 16 Feb 2021¹

- A graph lets the problem be represented through **Nodes** and **Relationships** of the nodes to each other
- Using graphs encodes relationships that cut across data elements and exposes their critical aspects that would not otherwise be visible

¹ <https://www.gartner.com/smarterwithgartner/gartner-top-10-data-and-analytics-trends-for-2021>

SBOMs and Graphs: A Closer Look

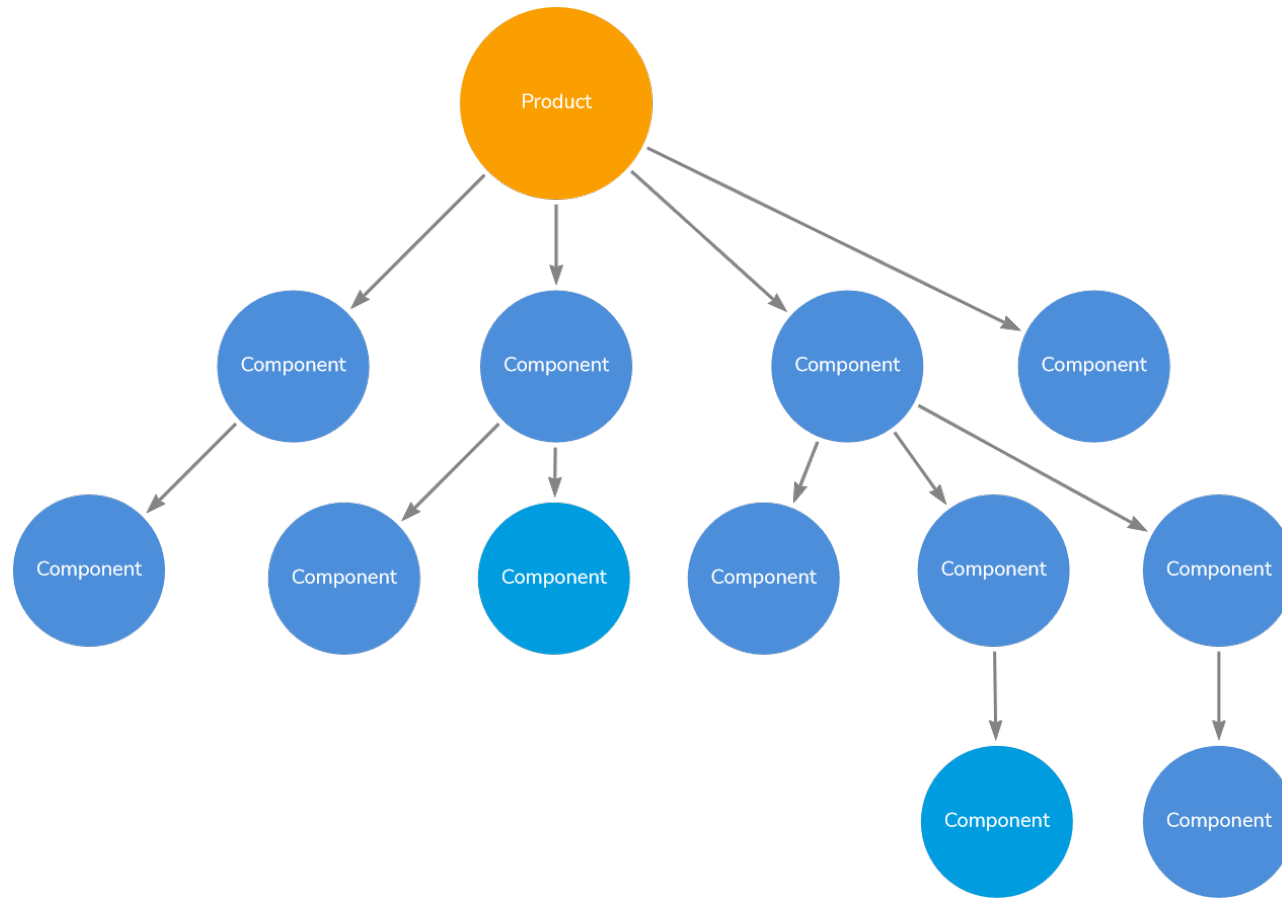
A closer review of SBOM guidance shows an expectation of graphs (highlighting added for emphasis):

Depth.** 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.

*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. **It should be noted that some use cases require complete or mostly complete graphs, such as the ability to “prove the negative” that a given component is not on an organization’s network.***¹

¹ *The Minimum Essential Elements of a Software Bill of Materials*, United States Department of Commerce, July 12, 2021,
https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

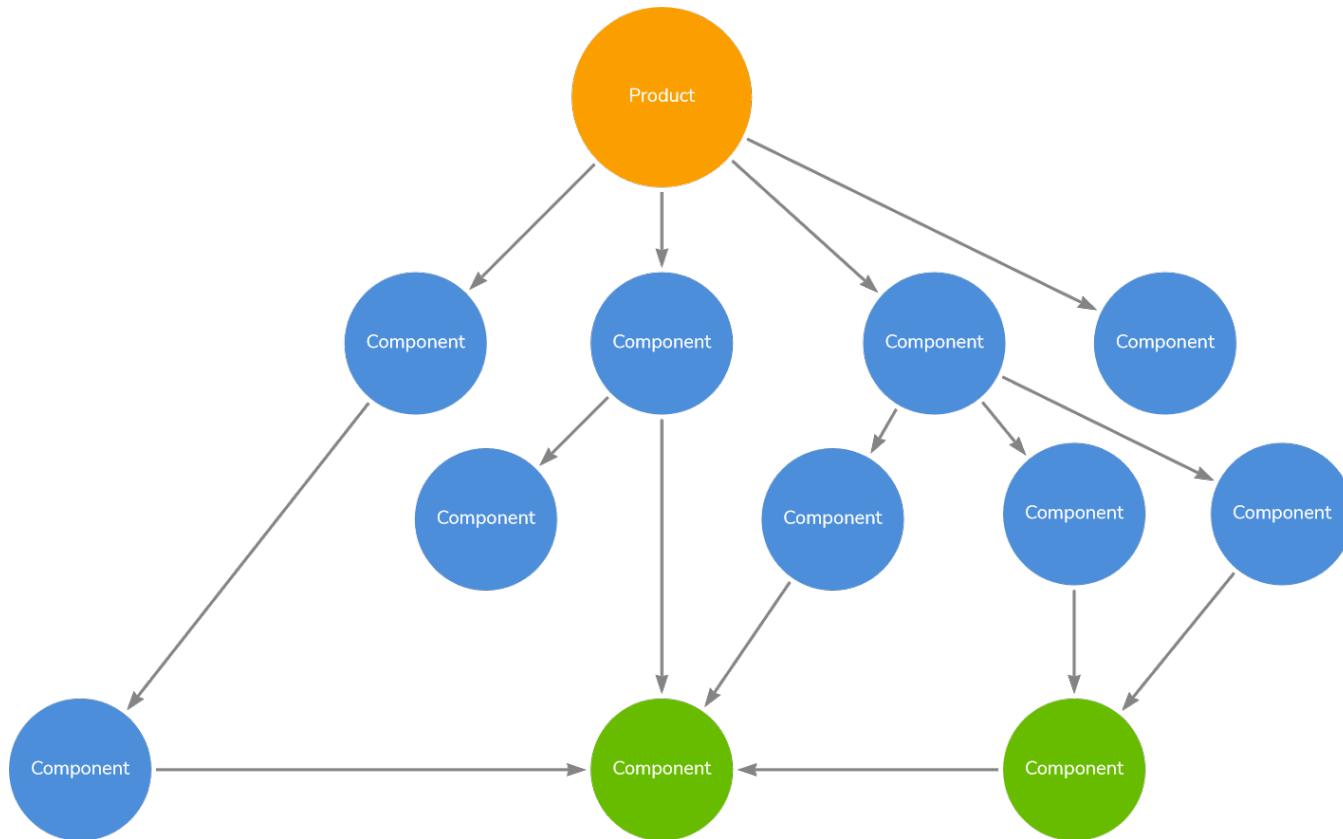
SBOM Dependencies – 1



Many organizations think their generated SBOM data looks this way

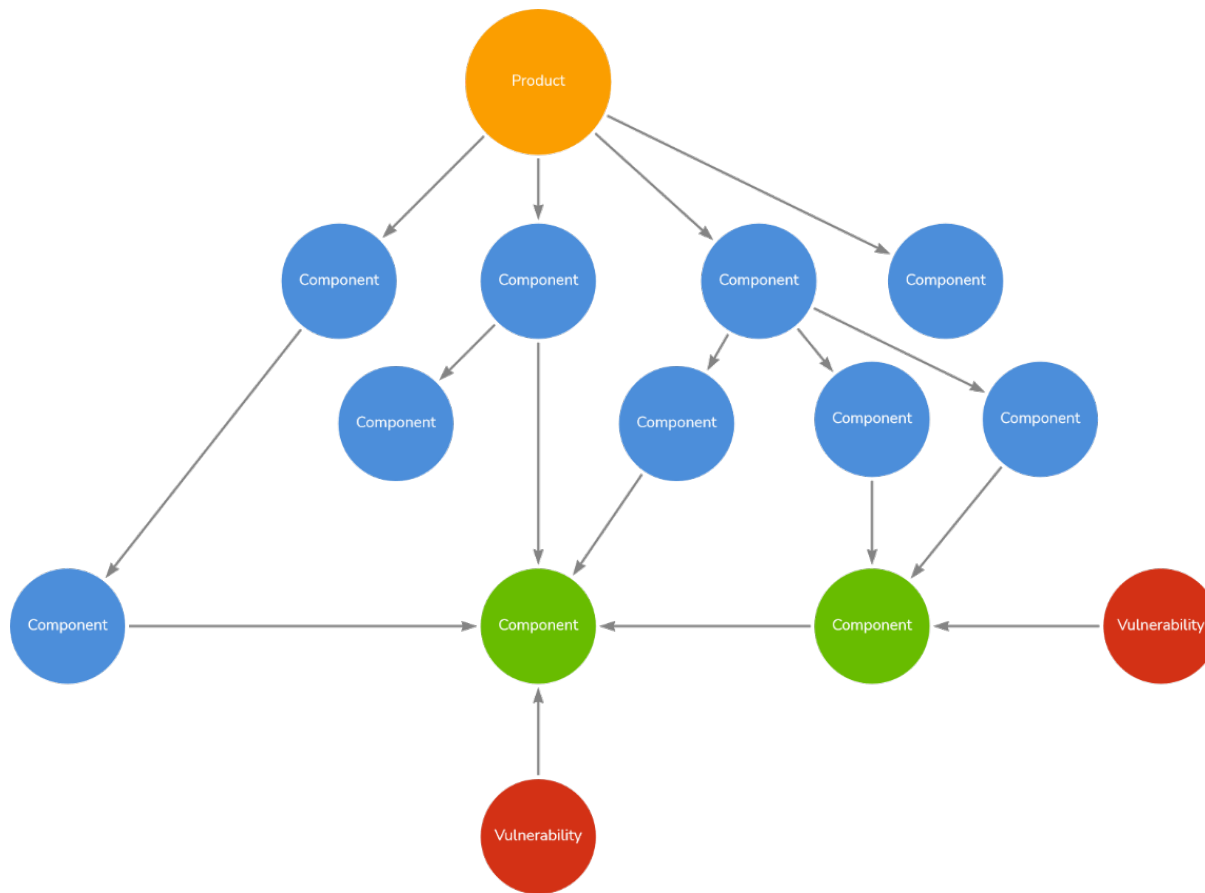
- Assuming the secondary and tertiary SBOM dependencies are ingested from their respective suppliers to augment the graph

SBOM Dependencies – 2



The reality is the component dependencies are not as clean as most organizations think

SBOM Dependencies – 3



By adding the known vulnerabilities, pulled from an authoritative source such as the National Vulnerability Database (NVD) to the graph, the potential system impacts and risks become visible through the relationships

Summary

- Systems are increasingly software intensive and complex.
- Third-party components are widespread throughout every aspect of a system (components, tools, services) and require an integrated acquisition, engineering, development, and operational focus to ensure sufficient security and resilience.
- The SBOM Framework leverages ASF to inform practices to build, deploy, and use SBOMs to better identify risk.
- SBOMs and their activities offer expanded data analytic/mining opportunities – visualizing the unseen/unknown to provide innovative new methods and insights to inform risk reduction.

Supporting ASF Reference Materials

SEI ASF related materials - <https://insights.sei.cmu.edu/library/acquisition-security-framework-asf-collection/>

White Paper – *Software Bill of Materials Framework: Leveraging SBOMs for Risk Reduction* <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=982283>

Technical Note - *Alberts, Christopher; Bandor, Michael; Wallen, Charles; & Woody, Carol. Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk (Expanded Set of Practices). CMU/SEI-2023-TN-004. Software Engineering Institute. 2023. <https://doi.org/10.1184/R1/24128475>*



34th Annual **INCOSE** international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

www.incose.org/symp2024
#INCOSEIS