

Acquisition Security Framework (ASF): Informing Software Bill of Materials (SBOM) Use Cases and Risk Reduction

FEBRUARY 22, 2023

Christopher Alberts
Mike Bandor
Charles Wallen
Carol Woody (Team Lead)

Document Markings

Copyright 2023 Carnegie Mellon University.

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.

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.

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

DM23-0161

Agenda

- ASF Overview
- Leveraging ASF to Inform SBOM Use Cases and Risk Reduction

ASF: Informing SBOM Use Cases and Risk Reduction

ASF Overview

Supply Chain/Acquisition Risk Is Increasing

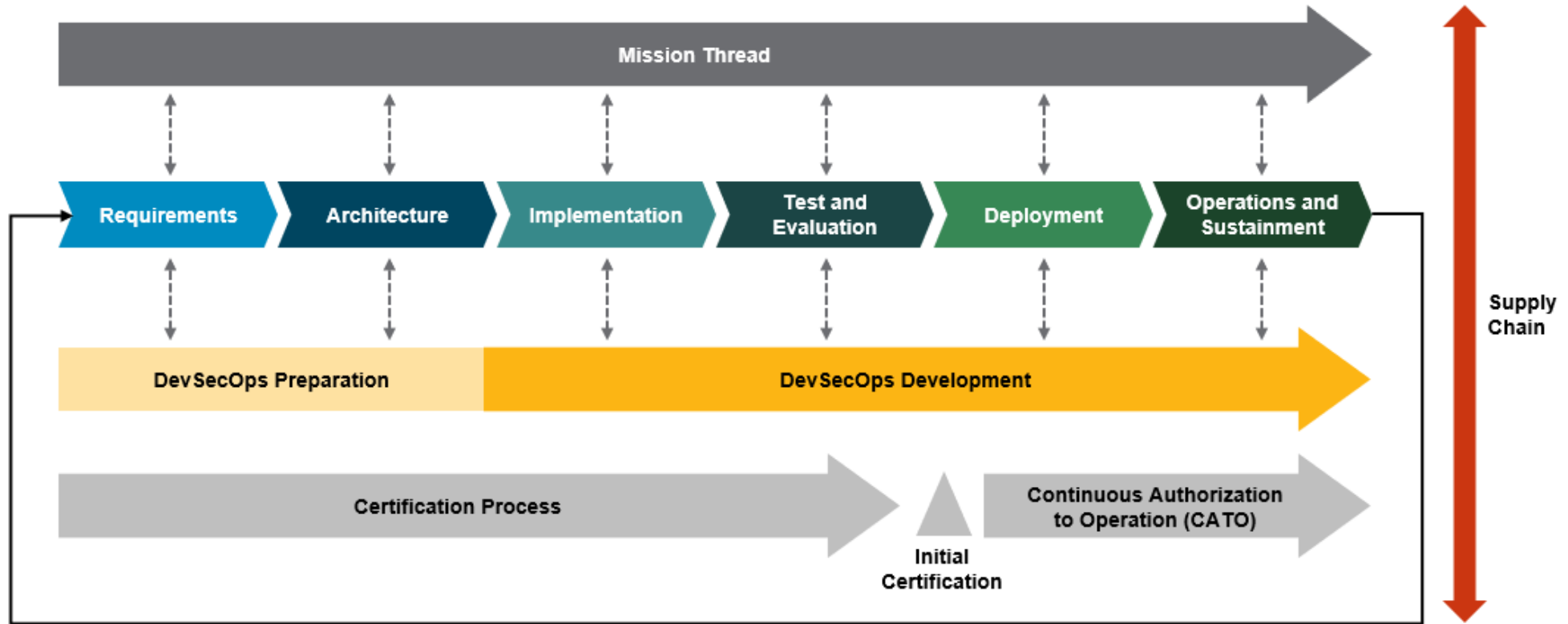


More than 230,000 organizations were examined to discover their relationships with third parties. 98% of organizations have a relationship with a third party that has been breached within the last two years.

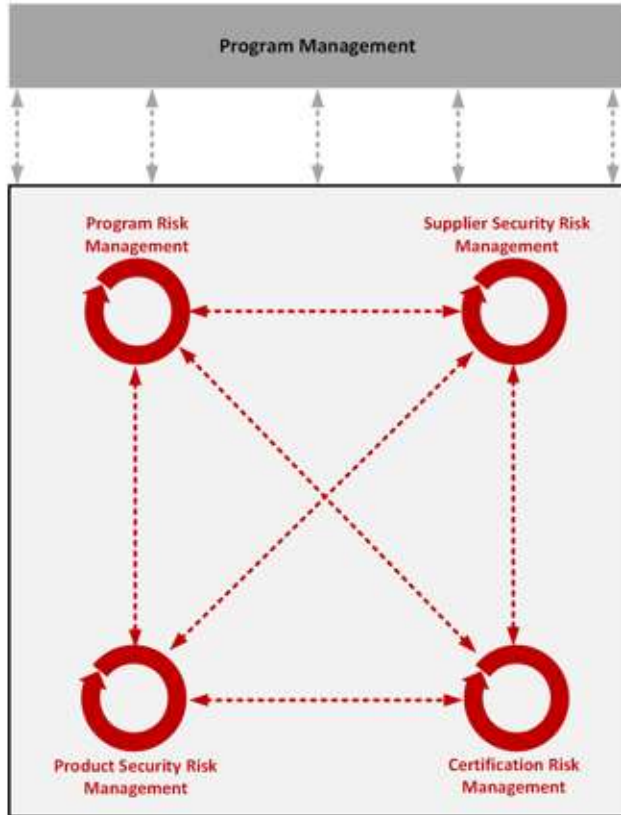
<https://www.securityweek.com/98-of-firms-have-a-supply-chain-relationship-that-has-been-breached-analysis/>

- 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)
- ?...(2023)

Acquisition Cybersecurity Problem Space



Challenge: Integrated Security and Supplier 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.

Key Supply Chain Cybersecurity Challenges for Acquisitions

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 cannot effectively manage cyber risks alone.
- Supply chain risk management requires collaboration.

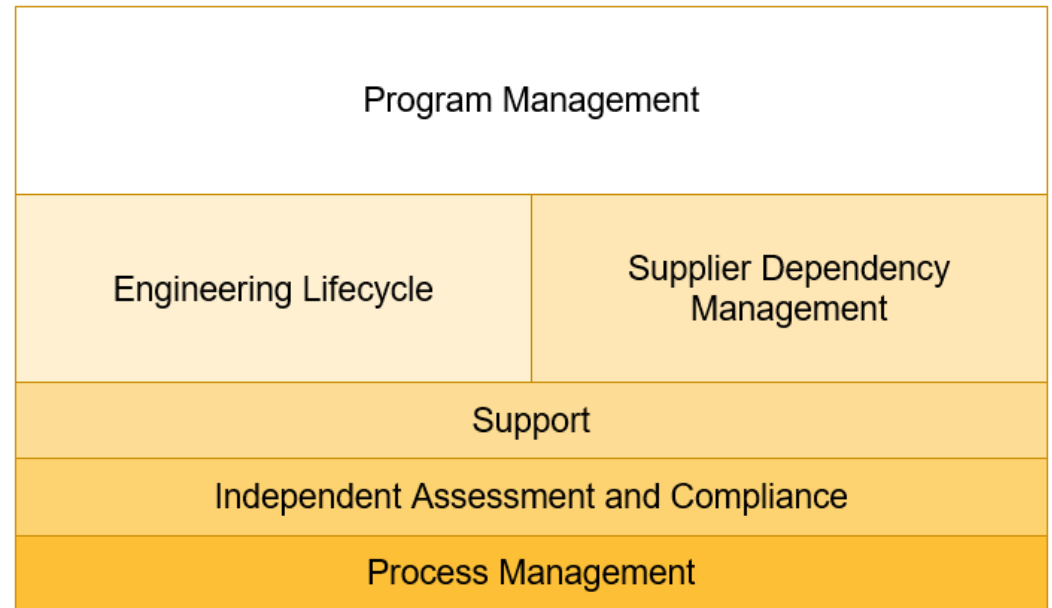
What is the Acquisition Security Framework (ASF)?

The ASF is a collection of leading practices for building and operating secure and resilient software-reliant systems.

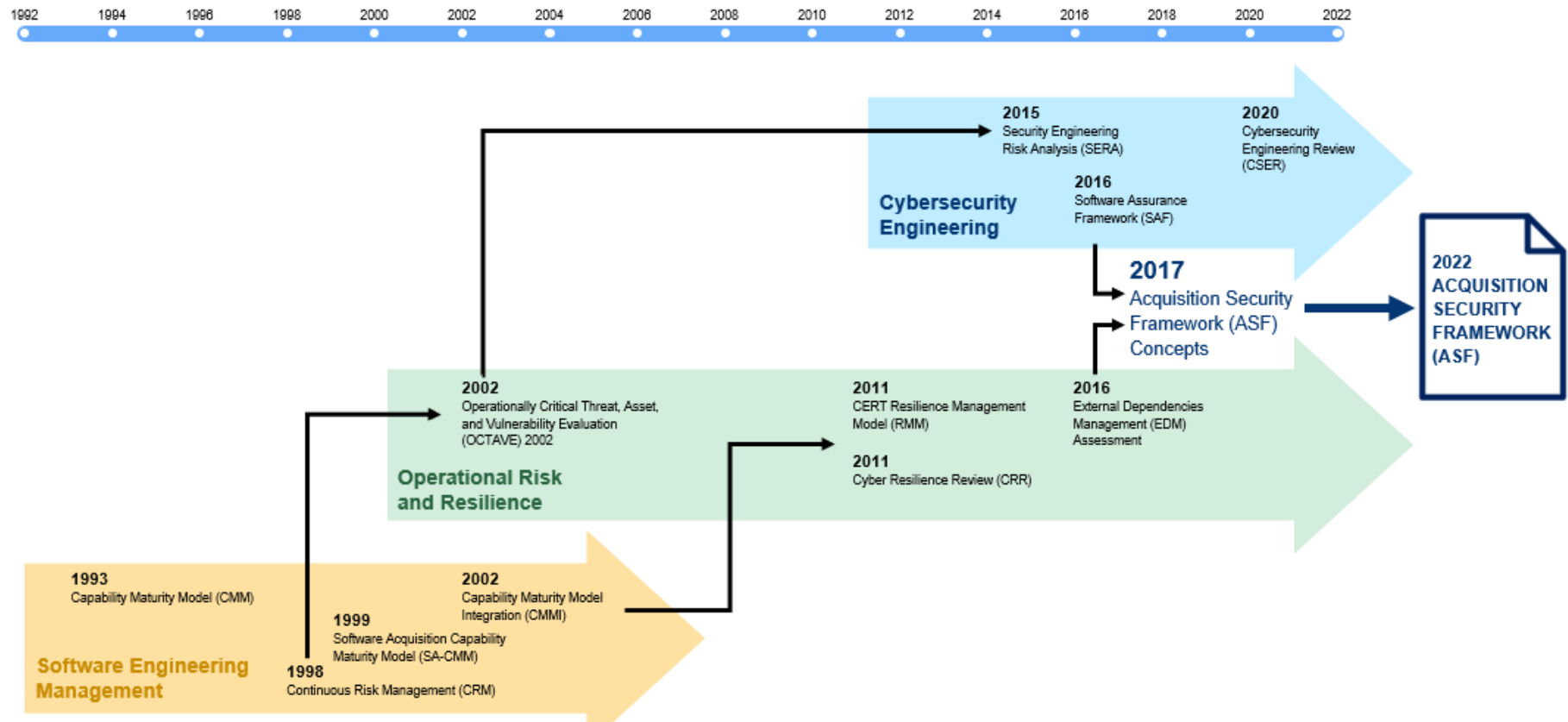
The ASF is designed to proactively enable system security and resilience engineering across the lifecycle and supply chain.

It provides a roadmap for building security and resilience into a system rather than “bolting it on” after deployment.

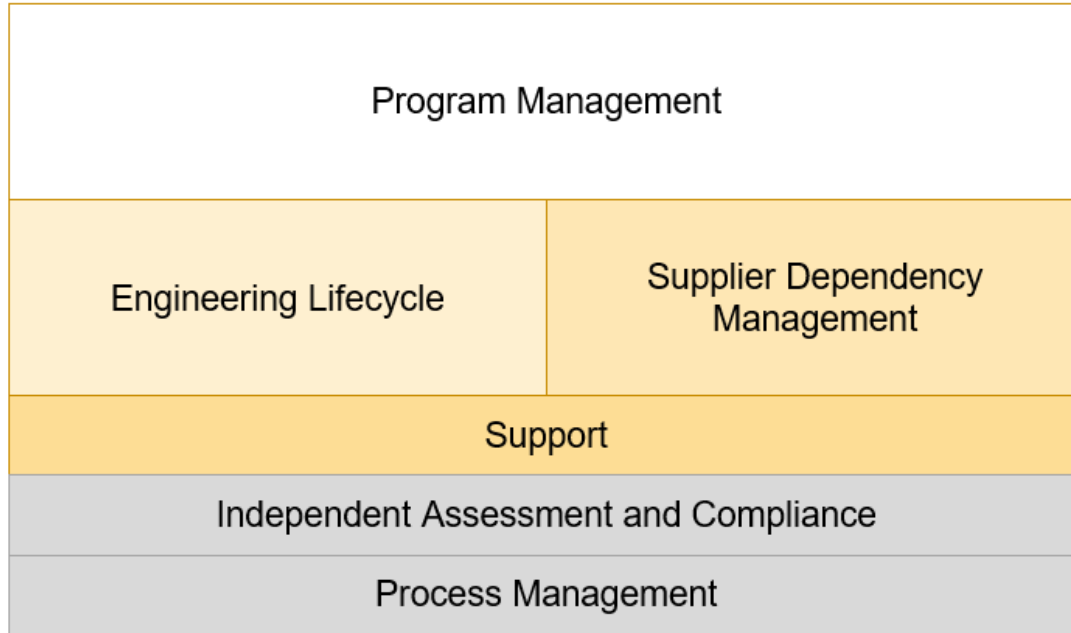
ASF principles and concepts facilitate efficient and predictable systems environments and more manageable delivery and risk outcomes.



ASF Research Lineage



ASF: Current Development Status



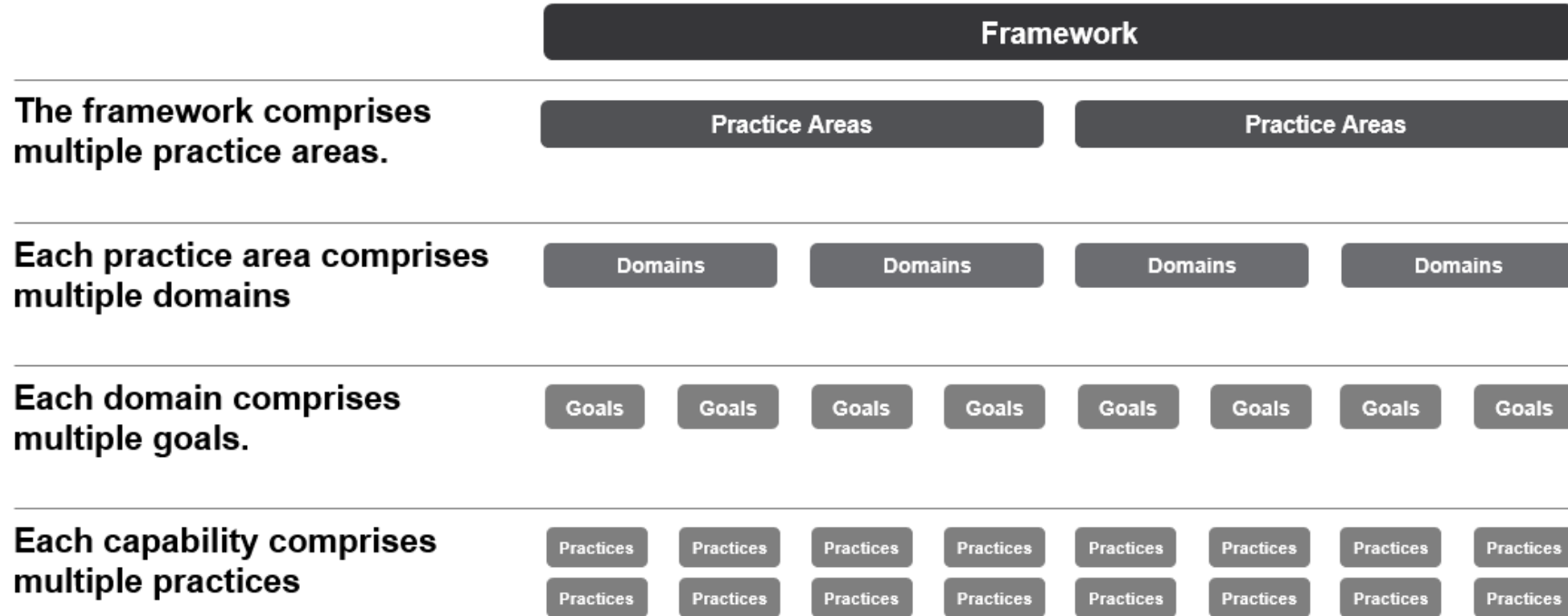
Four of the six areas are ready for use:

- Program Management
- Engineering Lifecycle
- Supplier Dependency Management
- Support

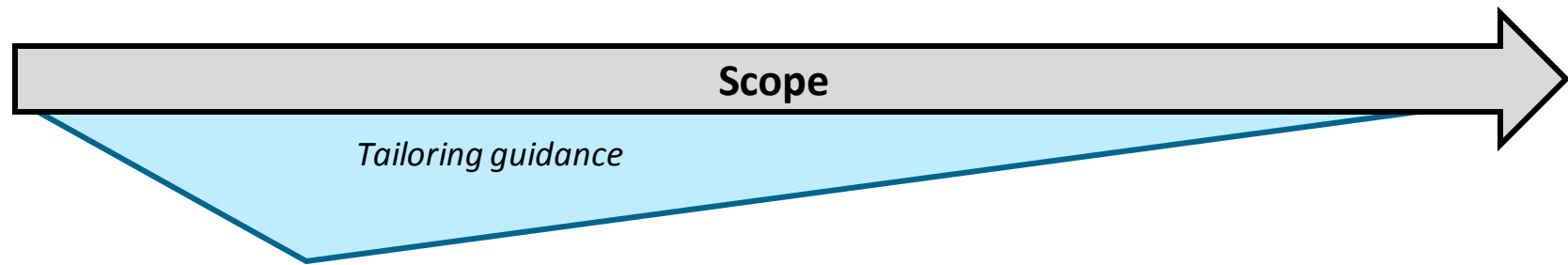
The remaining areas will be completed this calendar year:

- Independent Assessment and Compliance
- Process Management

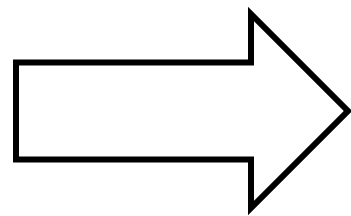
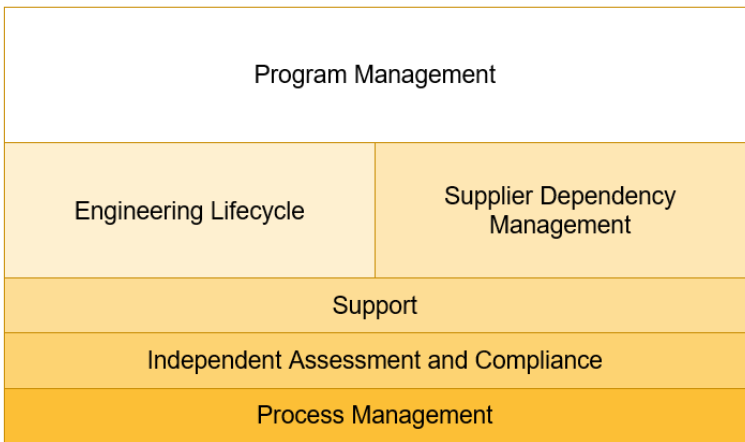
ASF: Elements and Structure



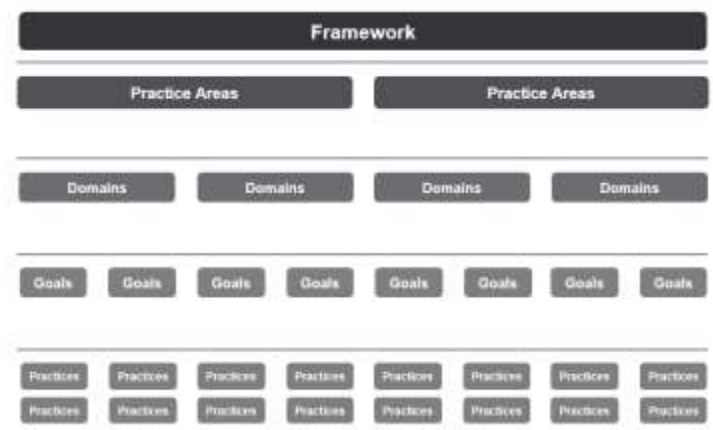
Creating Tailored Risk Frameworks



ASF Principles and Concepts



Tailored Framework



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)
- Cybersecurity Engineering Framework (in progress)
- Zero Trust Framework (proposed)

ASF: Informing SBOM Use Cases and Risk Reduction

Leveraging ASF to Inform SBOM Use Cases and Risk Reduction

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.

ASF Concepts Applied to SBOM: Setting the Scope

We considered the common use cases when setting the scope.

To set the scope, we developed a scenario for implementing an SBOM that includes the following:

- *Develop / construct* an SBOM.
- *Use the SBOM* to support identification of known vulnerabilities and risk reduction.

SBOM practices were established based on this scenario.

Key Activities for Implementing an SBOM

Requirements

Planning

Build / Construct

Deploy / Use

Manage / Support

Infrastructure

Leveraging ASF to Inform Common SBOM Use Cases

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

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? |

Planning

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? |

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?

Operational Use: Vulnerability Management

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? |

Management and 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? |

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? |

The Team



Carol Woody
Principal Researcher
CERT Division

Email: cwoody@cert.org



Christopher Alberts
Principal Cyber Security
Analyst
CERT Division



Charles M. Wallen
Information and Infrastructure
Security Analyst
CERT Division



Mike Bandor
Senior Software Engineer
Software Solutions Division

ASF References

White Paper - Acquisition Security Framework (ASF): An Acquisition and Supplier Perspective on Managing Software-Intensive Systems' Cybersecurity Risk
<https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=887698>

Technical Note - Alberts, Christopher; Bandor, Michael; Wallen, Charles; & Woody, Carol. Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk. CMU/SEI-2022-TN-003. Software Engineering Institute, Carnegie Mellon University. 2022. <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=889215>