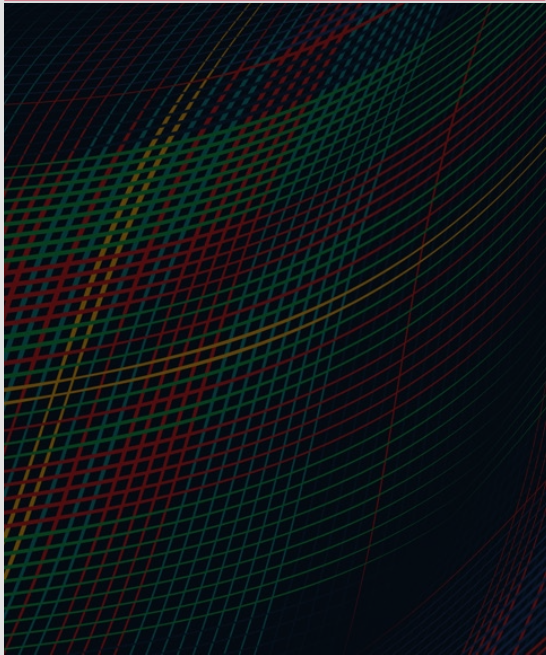
Carnegie Mellon University
Software Engineering Institute

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

JUNE 2023

Carol Woody



Document 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.

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.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

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.

DM23-0571

Agenda

- Brief ASF Overview
- Tailoring ASF for SBOM Use Cases

ASF: Informing SBOM Use Cases and Risk Reduction

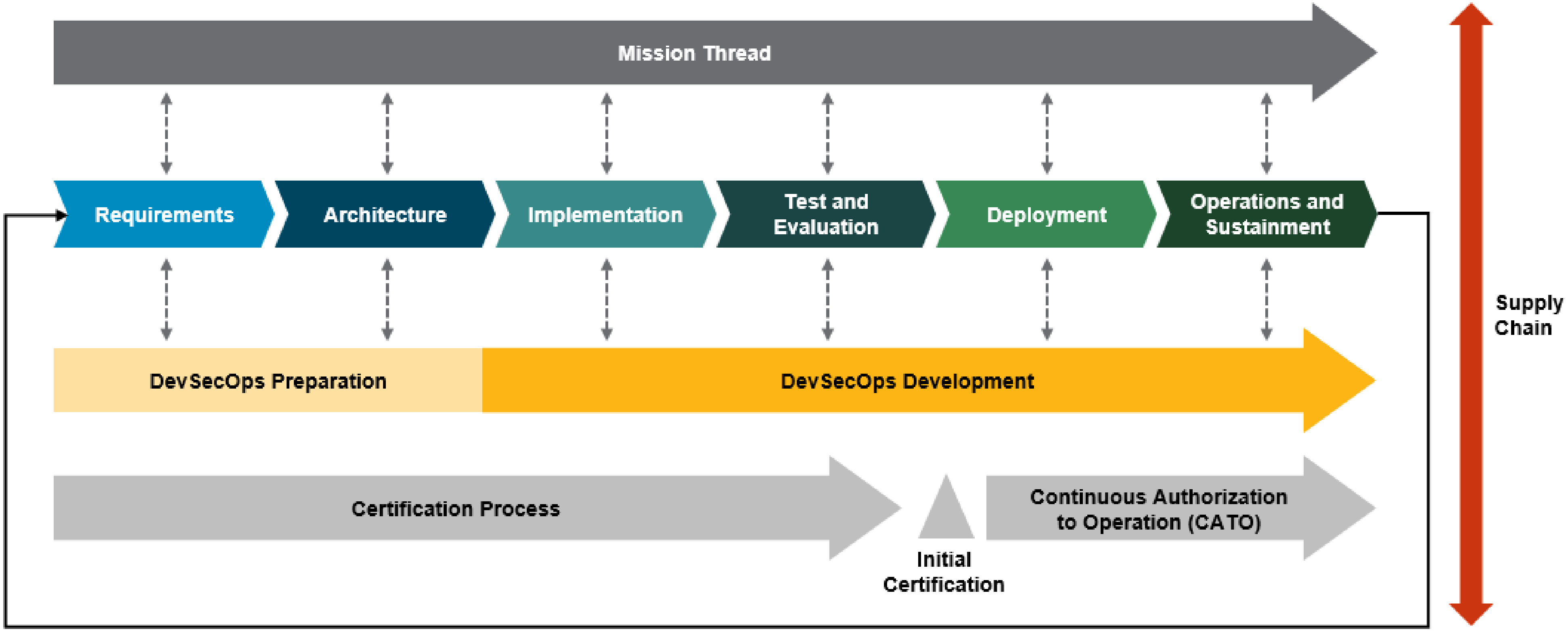
ASF Overview

Supply Chain/Acquisition Risk Is Increasing

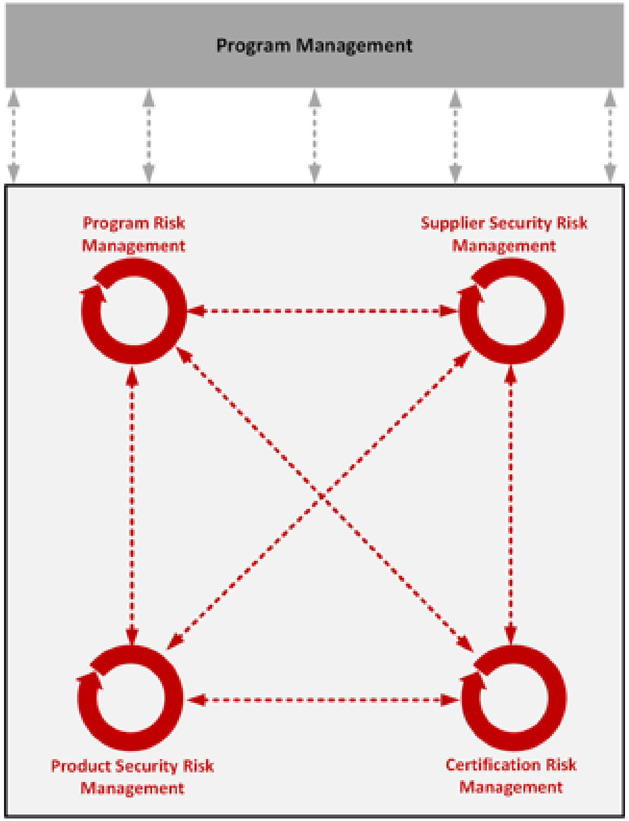
More than 230,000 organizations were examined to discover their relationships with third parties. 98% of organizations have a relationship with a third party that has been breached within the last two years.
https://www.securityweek.com/98-of-firms-have-a-supply-chain-relationship-that-has-been-breached-analysis/

- 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



Lack of Integrated Security and Supplier Risk Management across the Organization


Program Management
Program Risk Management
Supplier Security Risk Management
Product Security Risk Management
Certification Risk Management

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 should 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.

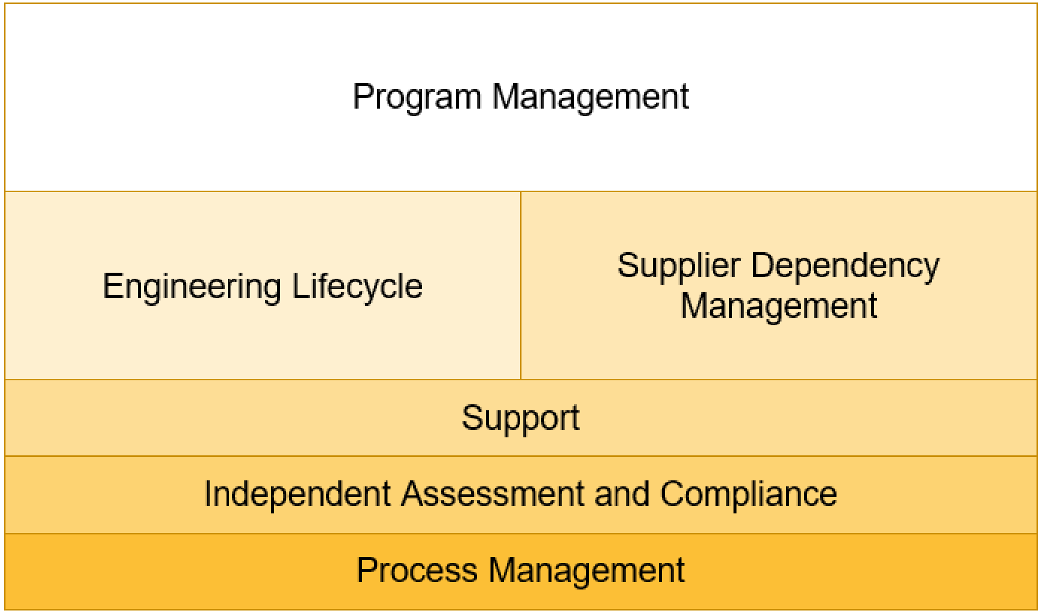
- A program cannot effectively manage cyber risks alone.
- Supply chain risk management requires collaboration.

What is the Acquisition Security Framework (ASF)?

The ASF is a collection of leading practices and processes for building and operating secure and resilient software-reliant systems, which are:

- designed to proactively enable system security and resilience engineering across the lifecycle and supply chain.
- provides a roadmap for building security and resilience into a system rather than "bolting it on" after deployment.

ASF contains questions to assess the practices in use to support efficient and predictable system and supply chain environments and reduced risk outcomes.



Program Management

Engineering Lifecycle

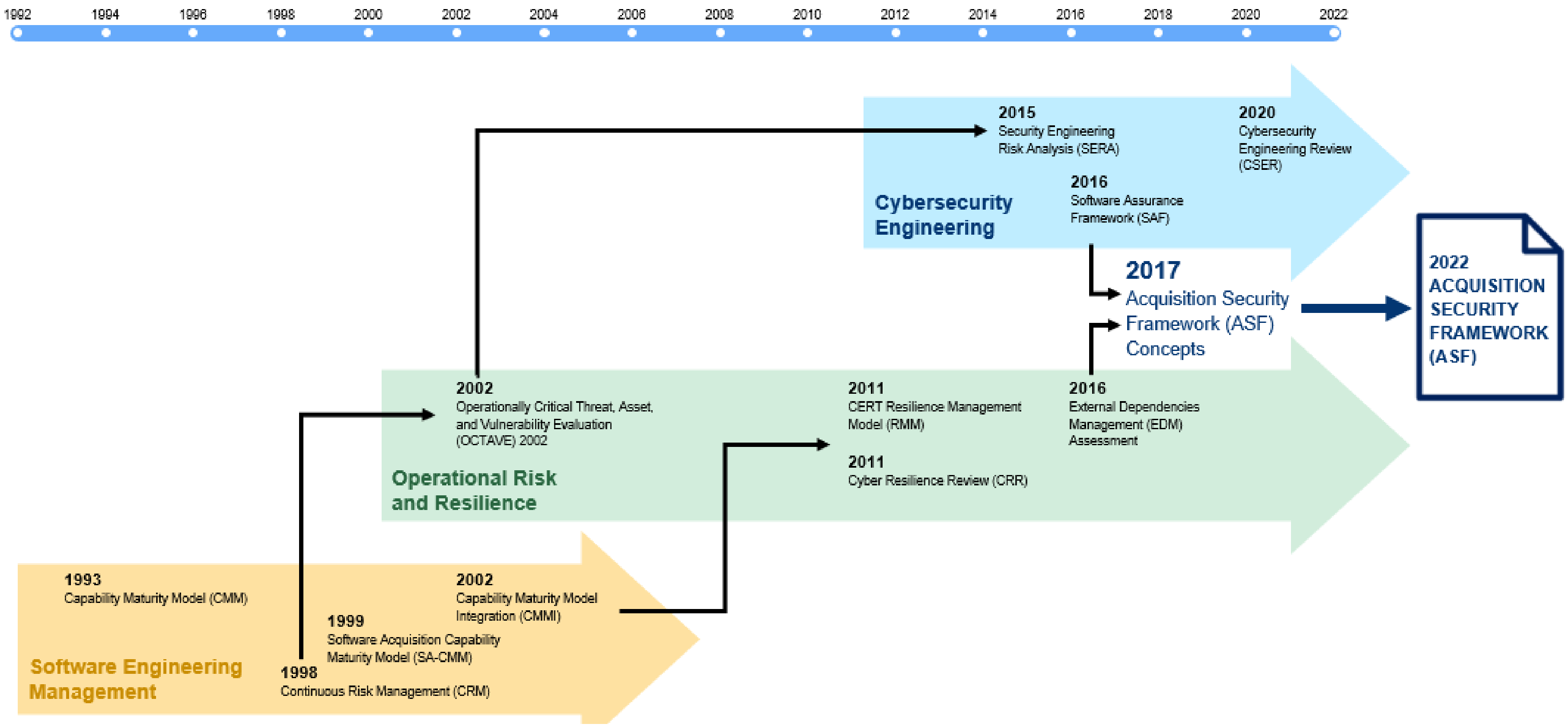
Supplier Dependency Management

Support

Independent Assessment and Compliance

Process Management

ASF Research Lineage



Cybersecurity Engineering

2015
Security Engineering Risk Analysis (SERA)

2016
Software Assurance Framework (SAF)

2020
Cybersecurity Engineering Review (CSER)

2017
Acquisition Security Framework (ASF) Concepts

2022
ACQUISITION SECURITY FRAMEWORK (ASF)

Operational Risk and Resilience

2002
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) 2002

2011
CERT Resilience Management Model (RMM)

2011
Cyber Resilience Review (CRR)

2016
External Dependencies Management (EDM) Assessment

Software Engineering Management

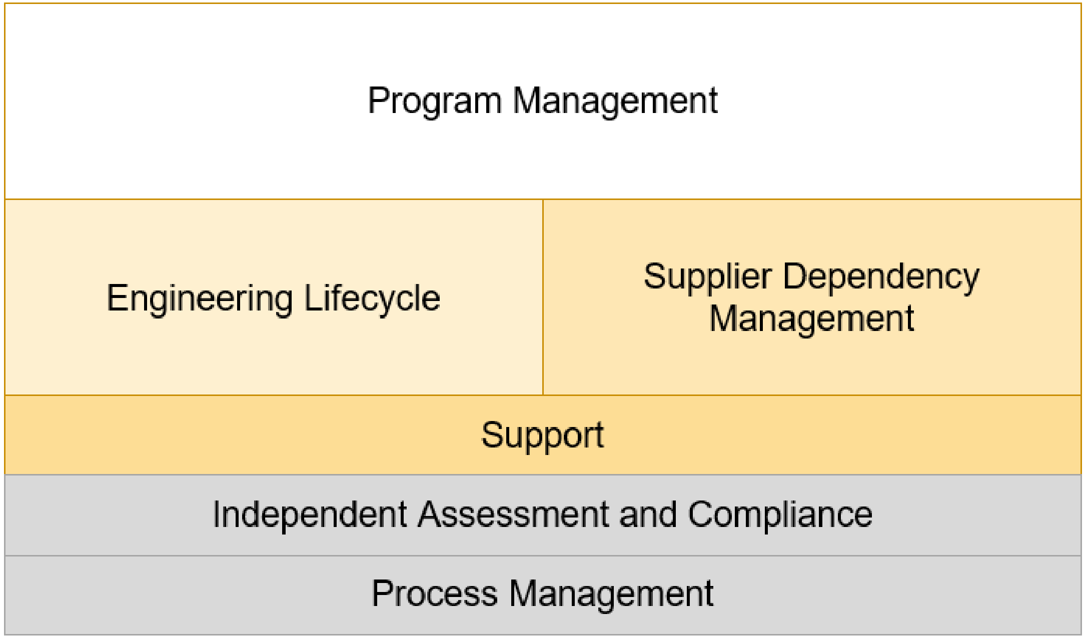
1993
Capability Maturity Model (CMM)

1998
Continuous Risk Management (CRM)

1999
Software Acquisition Capability Maturity Model (SA-CMM)

2002
Capability Maturity Model Integration (CMMI)

ASF: Current Development Status



Program Management

Engineering Lifecycle

Supplier Dependency Management

Support

Independent Assessment and Compliance

Process Management

Four of the six areas are ready for use:

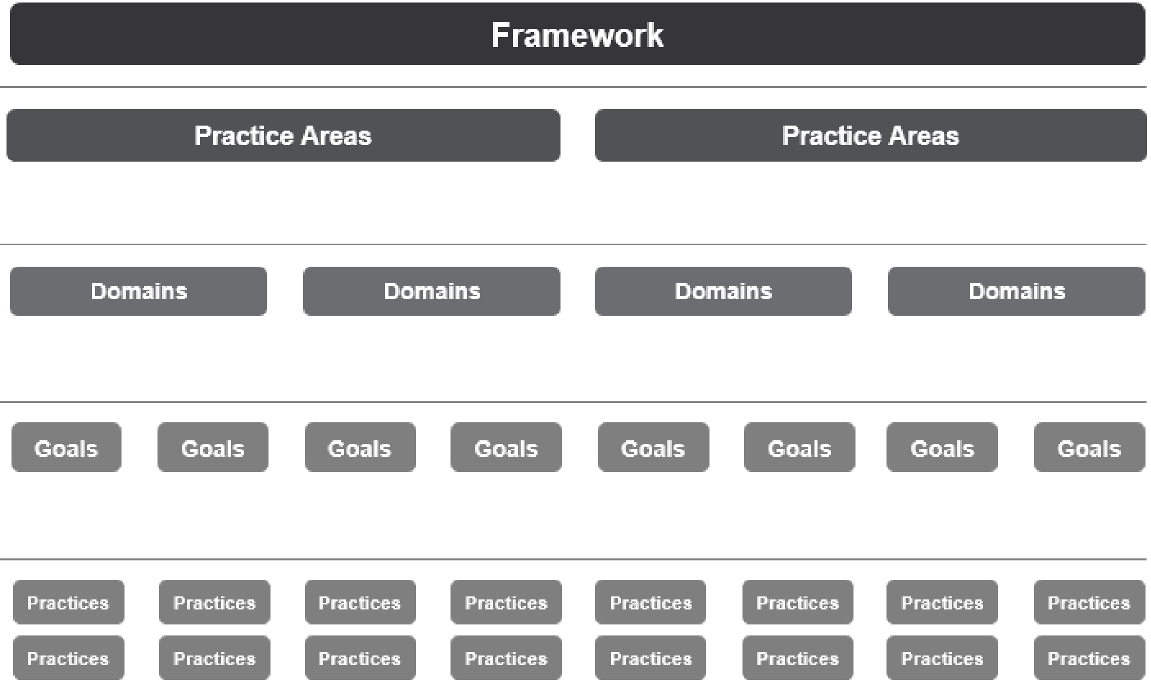
- Program Management
- Engineering Lifecycle
- Supplier Dependency Management
- Support

The remaining areas are near completion and will be published this summer:

- Independent Assessment and Compliance
- Process Management

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

ASF: Elements and Structure



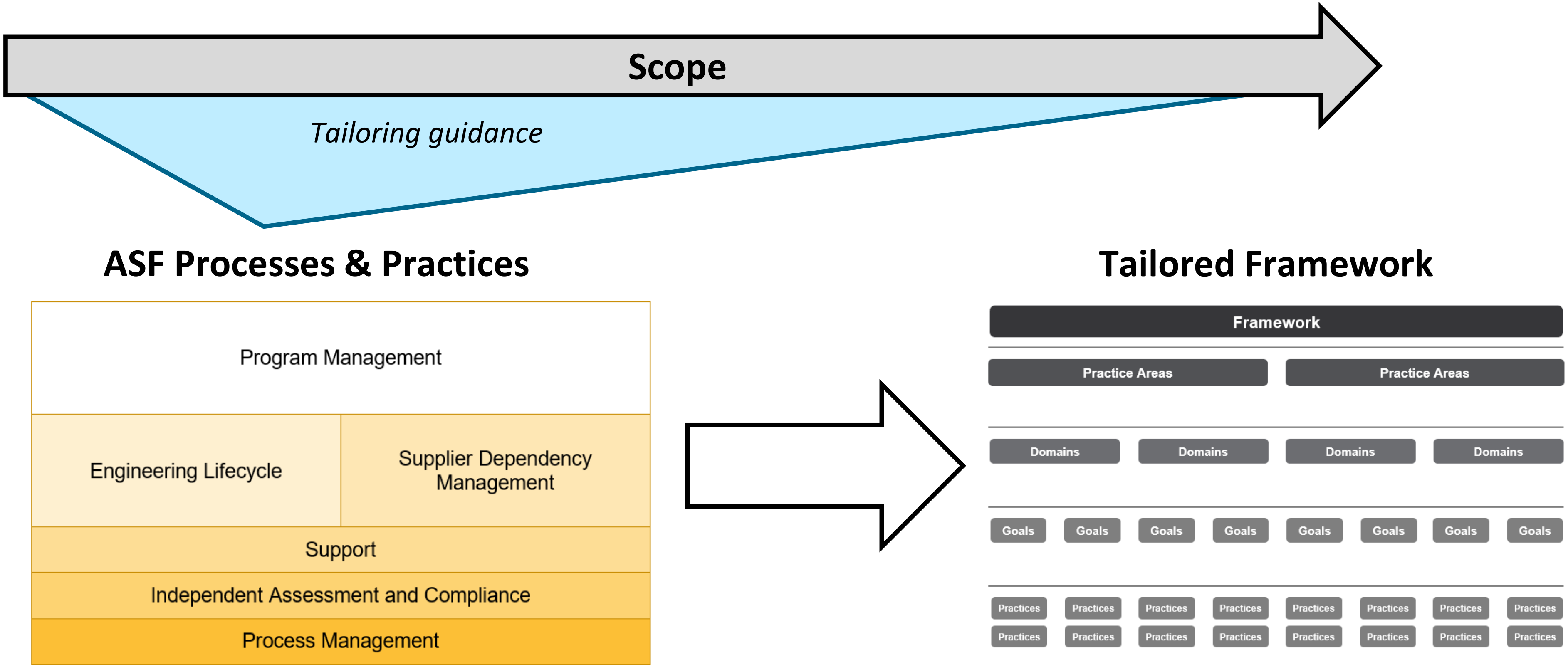
The framework comprises multiple practice areas.

Each practice area comprises multiple domains

Each domain comprises multiple goals.

Each capability comprises multiple practices

Creating Tailored Risk Frameworks



[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]

Tailored Risk Frameworks

ASF practices and processes enable effective management of security and resilience risks across a range of important acquisition and supply chain practice areas.

Frameworks consistent with ASF can be tailored based on problem space and scope:

- Software Bill of Materials (SBOM) Framework (prototype completed)
- Cybersecurity Engineering Framework (in progress)
- Zero Trust Framework (planned)

Leveraging ASF to Inform SBOM Use Cases and Risk Reduction

Carnegie Mellon University Software Engineering Institute

Perspectives on SBOM and Use Cases

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, a Dept of Commerce 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

Source: Department of Commerce The Minimum Elements For a Software Bill of Materials (SBOM), 2021
https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

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 Practice Areas for Implementing an SBOM

Requirements

Planning

Construction

Operational Use

Management & 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?

Construction

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?

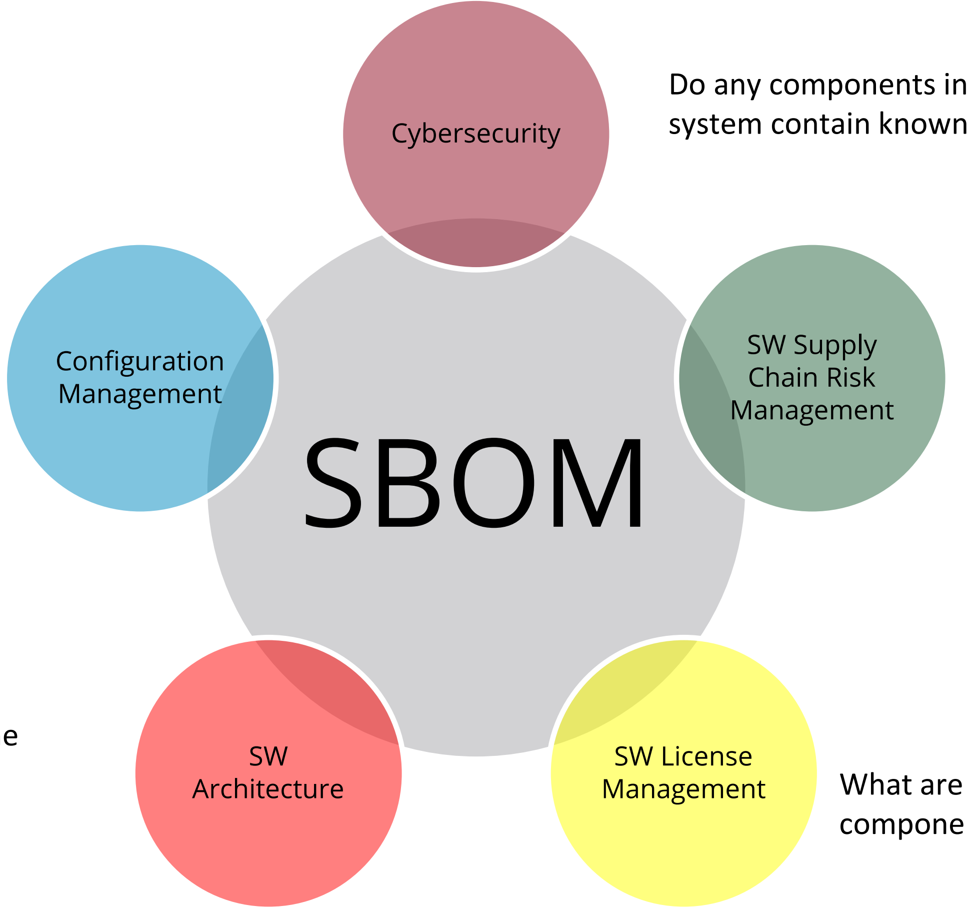
Infrastructure

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?

Next Steps: SBOM Relationships with Other Areas



Cybersecurity: Do any components in or used by the system contain known vulnerabilities?

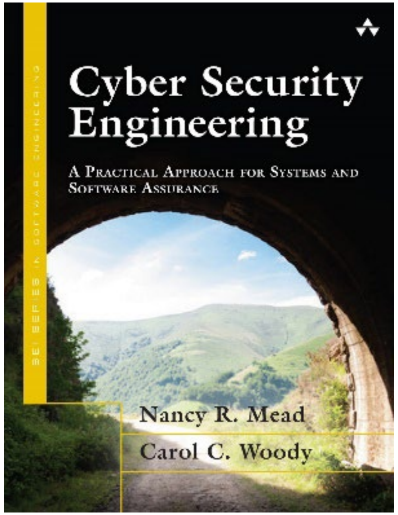
Configuration Management: What components are included/needed in my system?

SW Supply Chain Risk Management: What are the third-party components in the system and the source of the component information?

SW Architecture: Where are the components in the system architecture?

SW License Management: What are the licensing/data rights to components in my system?

Additional Resources


Cyber Security Engineering
A Practical Approach for Systems and Software Assurance
Nancy R. Mead
Carol C. Woody
SEI Series in Software Engineering

Cyber Security Engineering

A Practical Approach for Systems and Software Assurance

Nancy Mead

Carol Woody

ASF Resources

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

SEI Web Resources

sei.cmu.edu

CERT Cybersecurity Engineering and Software Assurance Professional Certificate

sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=33881