



# ATO Cybersecurity Awareness Symposium

NAS Cybersecurity  
Enabling the Art of the Possible

Acquisition Security Framework (ASF): Integration of Supply Chain Risk  
Management Across the System Lifecycle  
Carol Woody, Ph.D.

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](mailto:permission@sei.cmu.edu).

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

DM23-0093

# Software is Everywhere

You think you're building (or buying, or using) a product such as:

car or truck

satellite

mobile phone

development tools

home security system

aircraft

pacemaker

security tools

home appliance

financial system

bullets for a gun

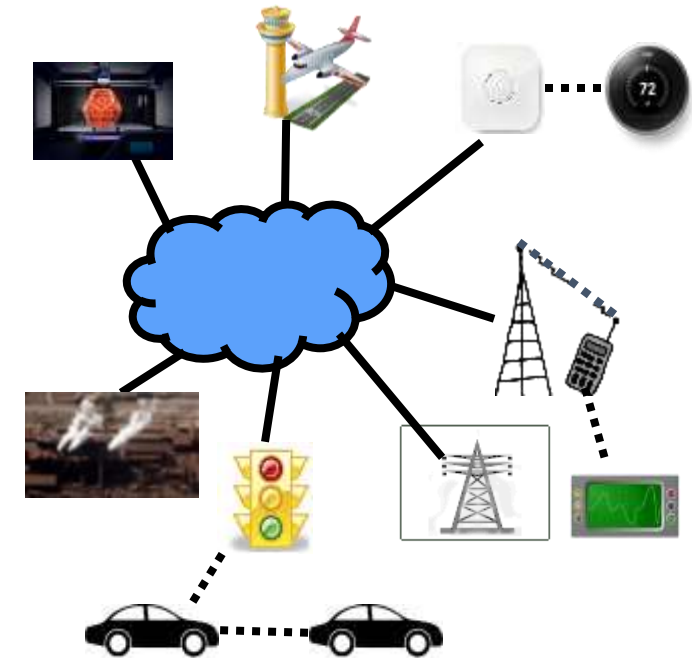
Actually, you're getting **a software platform:**

- Software is a part of almost everything we use.
- Software defines and delivers component and system communication.
- Software is used to build, analyze and secure software.

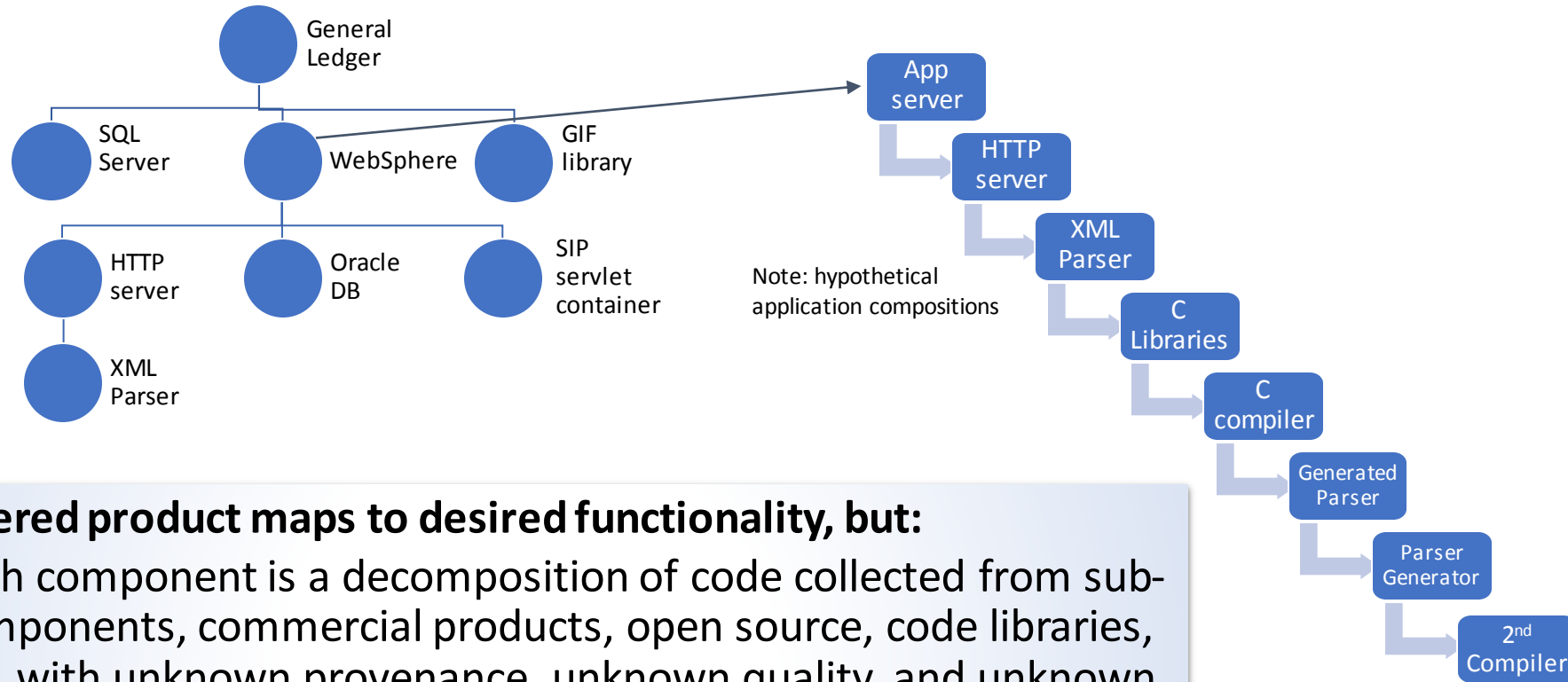
**All software has defects:**

- Best-in-class code has <600 defects per million lines of code (MLOC).
- Good code has around 1000 defects per MLOC.
- Average code has around 6000 defects per MLOC.

(based on Capers Jones research <http://www.namcook.com/Working-srm-Examples.html>)



# Software Development is Now Assembly



## Delivered product maps to desired functionality, but:

- Each component is a decomposition of code collected from sub-components, commercial products, open source, code libraries, etc. with unknown provenance, unknown quality, and unknown security
- No one person, team, or organization knows how all the pieces work

Reuse is rampant!

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

# Supply Chain/Acquisition Risk is Increasing

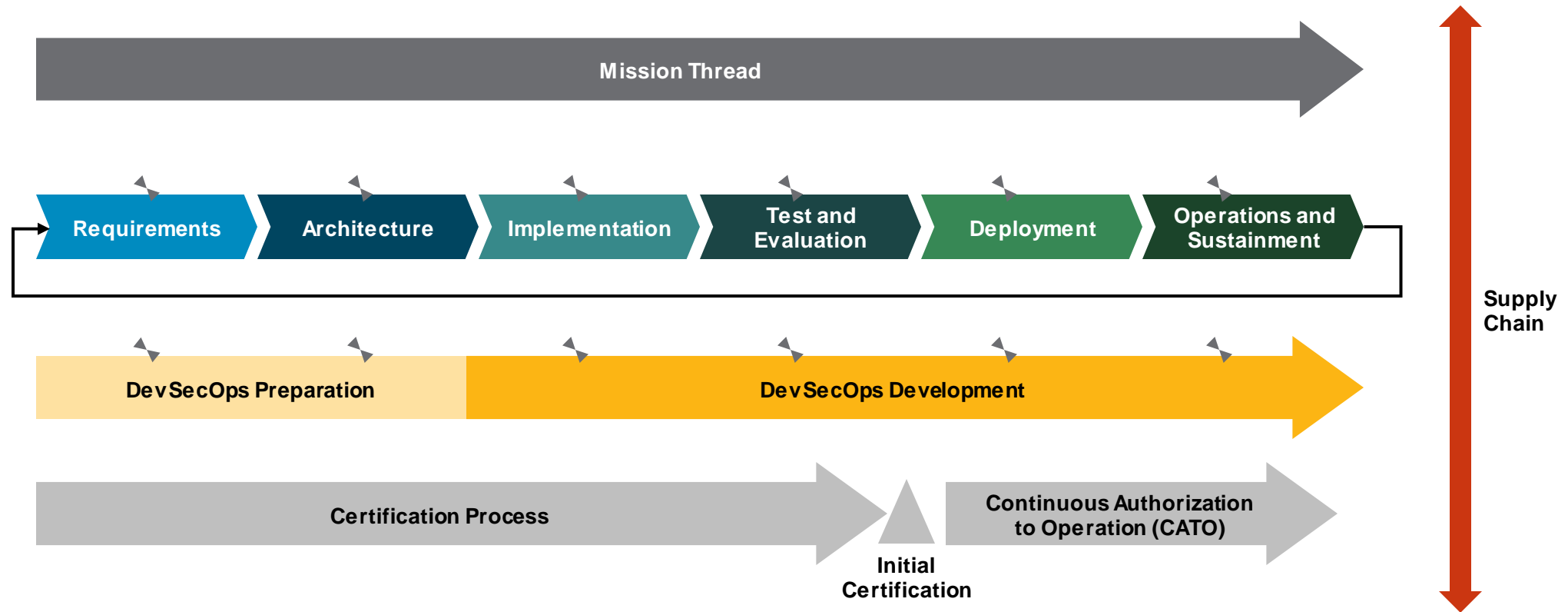


More than 230,000 organizations were examined to discover their relationships with third parties. 98% of organizations have a relationship with a third party that has been breached within the last two years.

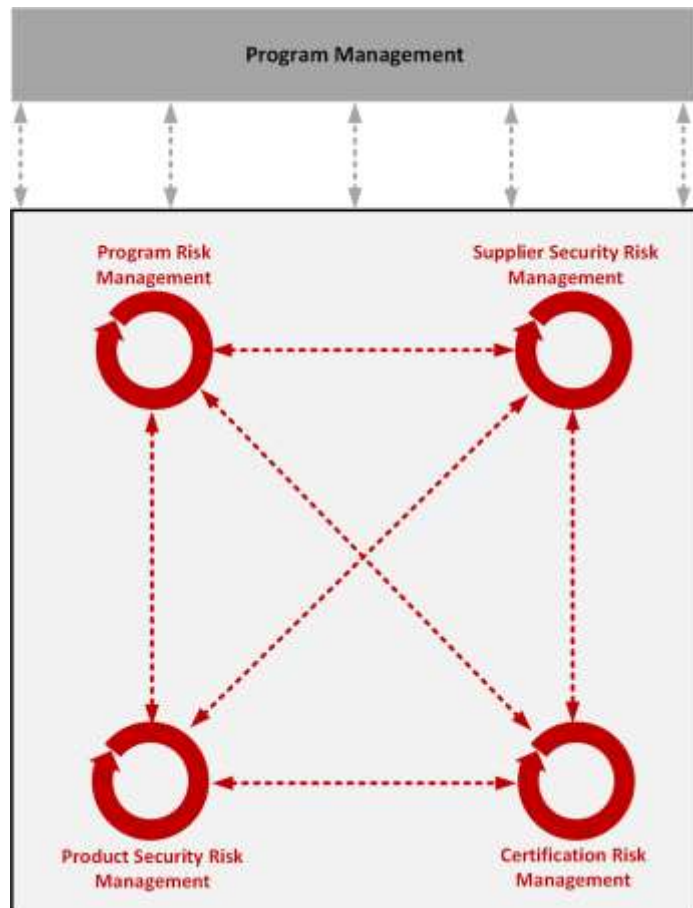
<https://www.securityweek.com/98-of-firms-have-a-supply-chain-relationship-that-has-been-breached-analysis/>

- 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)
- TBD (2022 ...)

# 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.

# What is the Acquisition Security Framework?

The Acquisition Security Framework (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.

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

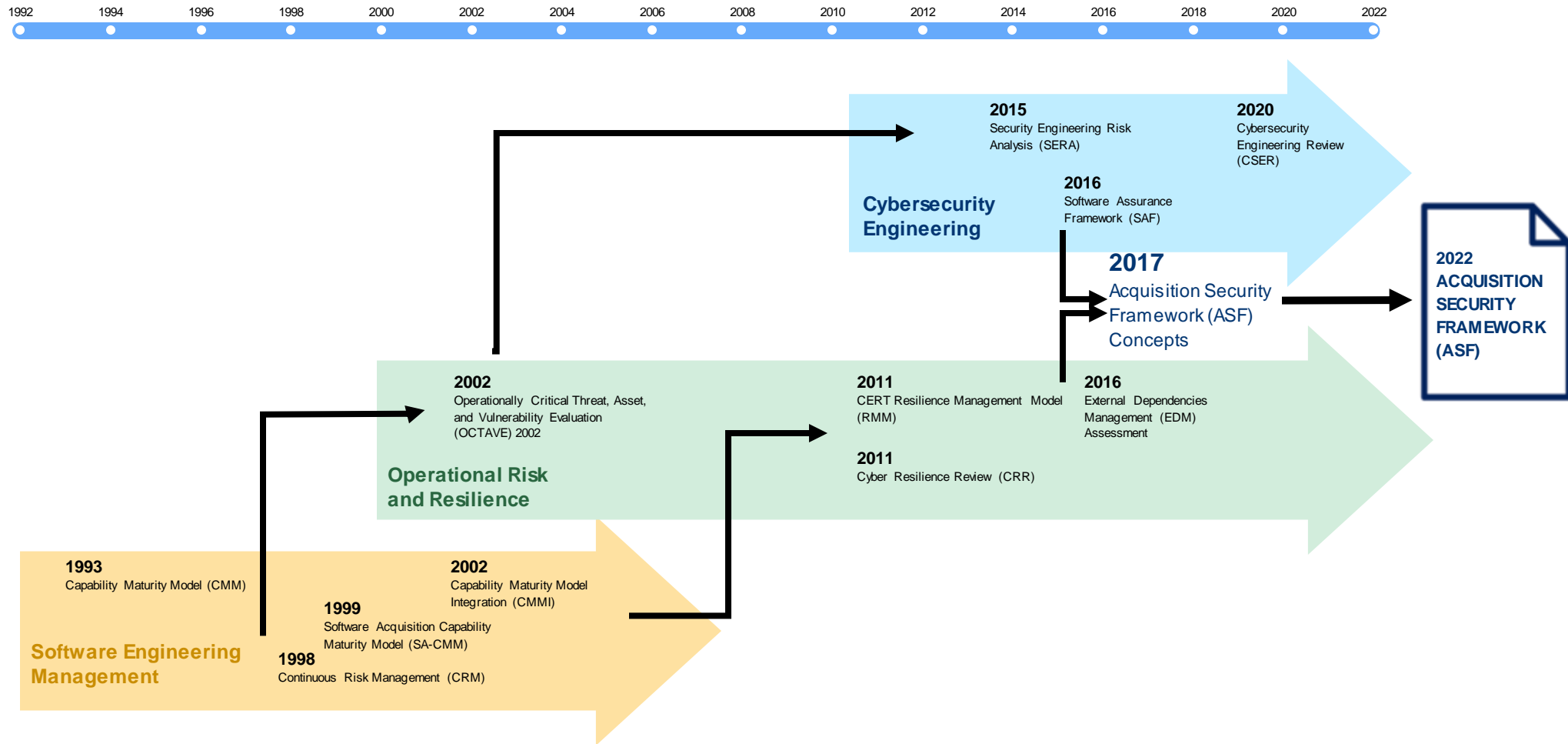
ASF facilitates efficient and predictable systems environments and more manageable delivery and risk outcomes.

# Research Lineage of ASF

2010 Software Engineering Institute (SEI) research showed 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 (Ellison, Goodenough, Weinstock, & Woody, 2010).

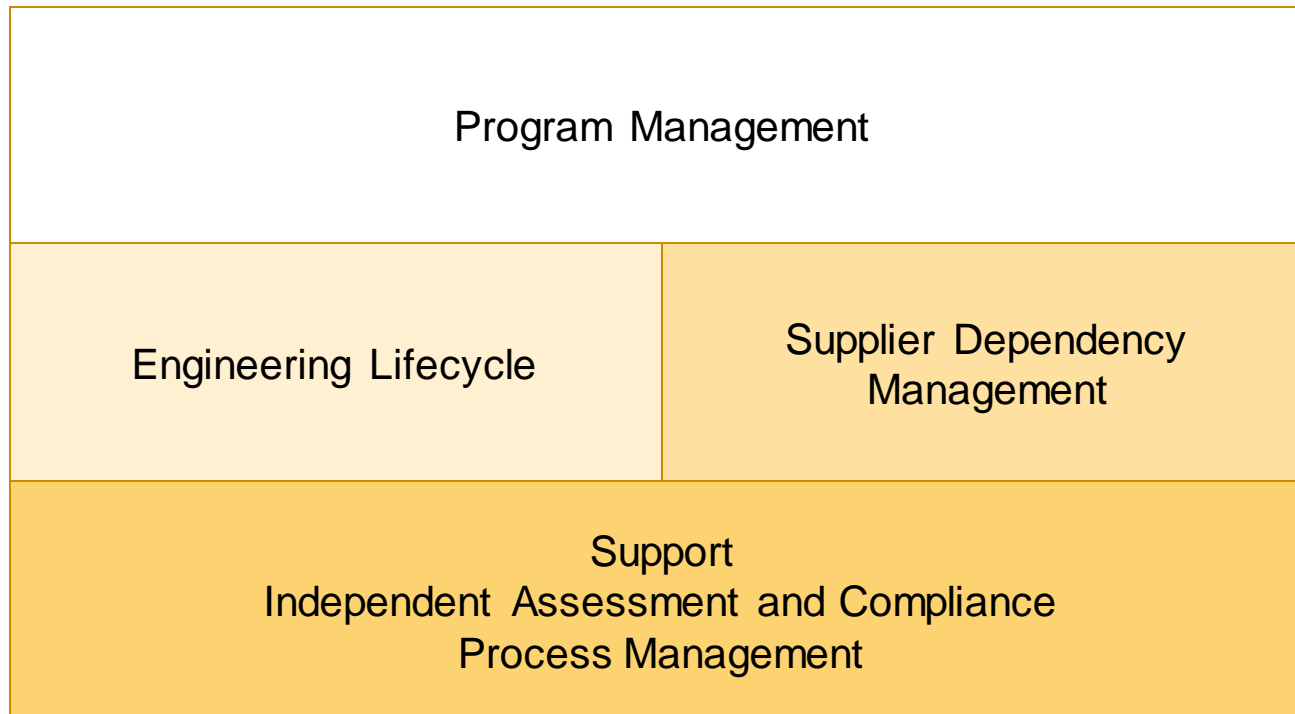
In later research, we investigated the lifecycle issues of supply chain risk and identified that the operational and mission impact of cyber risk increases as organizations become more dependent on suppliers and software.

# ASF Research Lineage



# Acquisition Security Framework (ASF)

## Acquisition Security Framework (ASF)

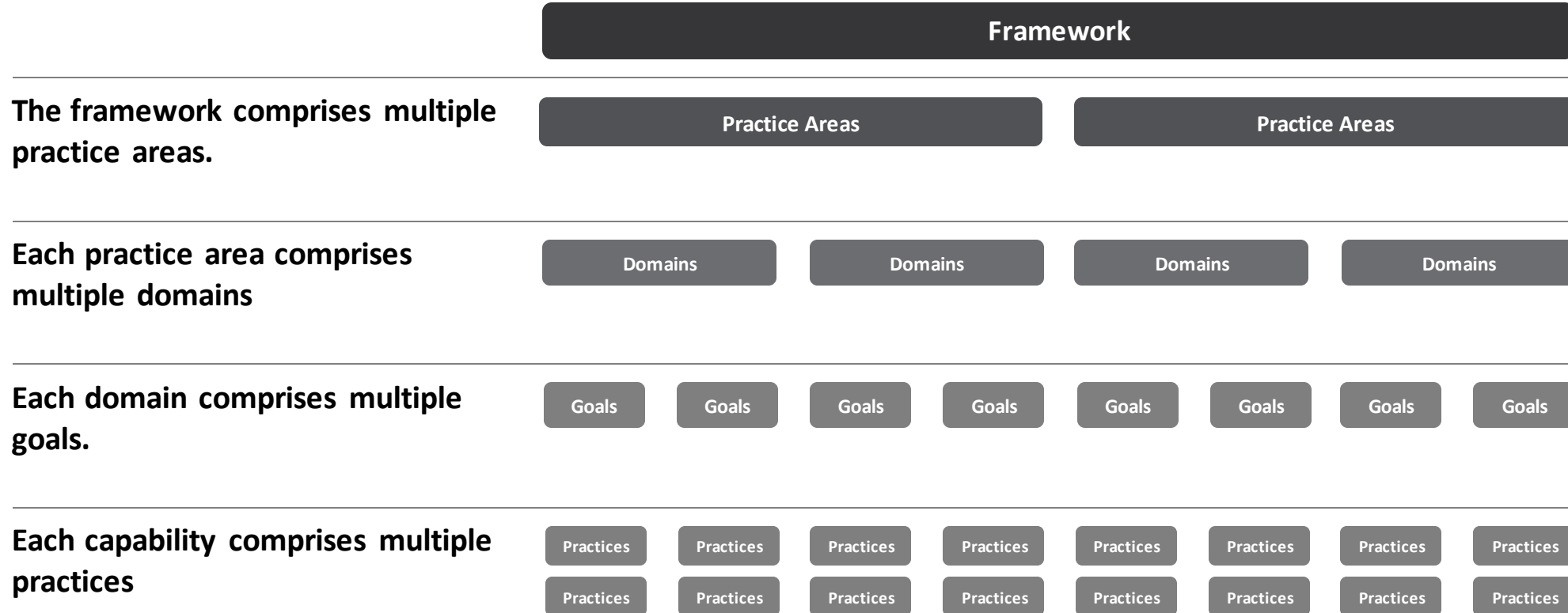


Four of the six areas are published and ready for use:

Program Management, Engineering Lifecycle, Supplier Dependency Management, and Support.

The remaining two areas will be published this fiscal year.

# ASF Structure



# ASF Practice Area: Program Management

Domain	Goal Areas
Program Planning and Management	Program Definition Program Planning Program Monitoring and Management Communication and Coordination
Requirements and Risk	Program Requirements Program Risk Management

# ASF Practice Area: Engineering Lifecycle

Domain	Goal Areas
Engineering Infrastructure	Infrastructure development Infrastructure operation and sustainment
Engineering Management	Technical activity management Product risk management
Engineering Activities	Requirements Architecture Third-party components Implementation Test and evaluation Transition artifacts Deployment Secure product operation and sustainment

# ASF Practice Area: Supplier Dependency Management

Domain	Goal Areas
Relationship Formation	Establishing supplier relationships is planned Formal agreements include resilience requirements Supplier are evaluated Managing supplier risk
Relationship Management	Suppliers are identified and prioritized Supplier performance is governed and managed Supplier risk management is continuous Change and capacity management are applied to suppliers Supplier access to program or system assets is managed Infrastructure and governmental dependencies are managed Supplier transitions are managed
Supplier Protection and Sustainment	Disruption planning includes suppliers Planning and controls are maintained and updated Situational awareness extends to suppliers

# ASF Practice Area: Support

Domain	Goal Areas
Program Support	Security/Resilience Training Measurement and Analysis Configuration and Change Management Resource Coordination and Management
Security Support	Security Administration Asset Management Information and Records Management Access Management Facility Management Disruption Management

# SAMPLE

## Practice Area: Supplier Dependency Management Domain 1: Relationship Formation

### **Goal 1—Establishing supplier relationships is planned.**

The purpose of this goal is to assess whether entering into relationships with suppliers is planned.

1. Is entering into formal agreements with suppliers planned?
2. Are baseline (i.e., boilerplate) requirements that apply to any supplier that supports the program or system identified and documented?
3. Are security/resilience requirements identified and documented for any supplier (e.g., contracted suppliers, infrastructure providers, and governmental services providers) that supports the program or system?
4. Are security/resilience requirements considered before agreeing to relationships with suppliers?

# Process Management and Improvement



- Higher degrees of process management translate to more stable environments that
  - Produces consistent results over time
  - Allows teams to achieve their missions during times of stress
- Each organization/program unit must manage the maturity of its security practices.
- Security practices do not need to be at a uniform level of maturity to be sufficient.

# Summary

The Acquisition Security Framework (ASF) is designed to

- Identify ways to establish more insight and control over your supply chain
- Provide a means to evaluate risks and gaps in current mechanisms for managing your supply chains
- Identify ways to improve your processes for acquiring, engineering, and deploying secure software-reliant systems

# References

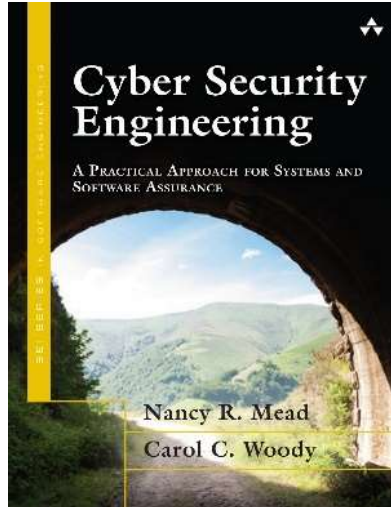
**White Paper** - Acquisition Security Framework (ASF): An Acquisition and Supplier Perspective on Managing Software-Intensive Systems' Cybersecurity Risk

<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>

# Resources



## **Cyber Security Engineering**

*A Practical Approach for Systems and Software Assurance*

Nancy Mead  
Carol Woody

## **Web Resources**

[sei.cmu.edu](http://sei.cmu.edu)

## **CERT Cybersecurity Engineering and Software Assurance Professional Certificate**

[sei.cmu.edu/education-outreach/credentials/credential.cfm?customel\\_datapageid\\_14047=33881](http://sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=33881)