Carnegie Mellon University
Software Engineering Institute

Acquisition Security Framework (ASF)

NOVEMBER 16, 2022

Carol Woody, Ph.D.
Principal Researcher

Carnegie Mellon University Software Engineering Institute

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.

DM20-1061

Supply Chain/Acquisition Risk is Increasing as Impact Increases

Heartland Payment Systems (2009)

Silverpop (2010)

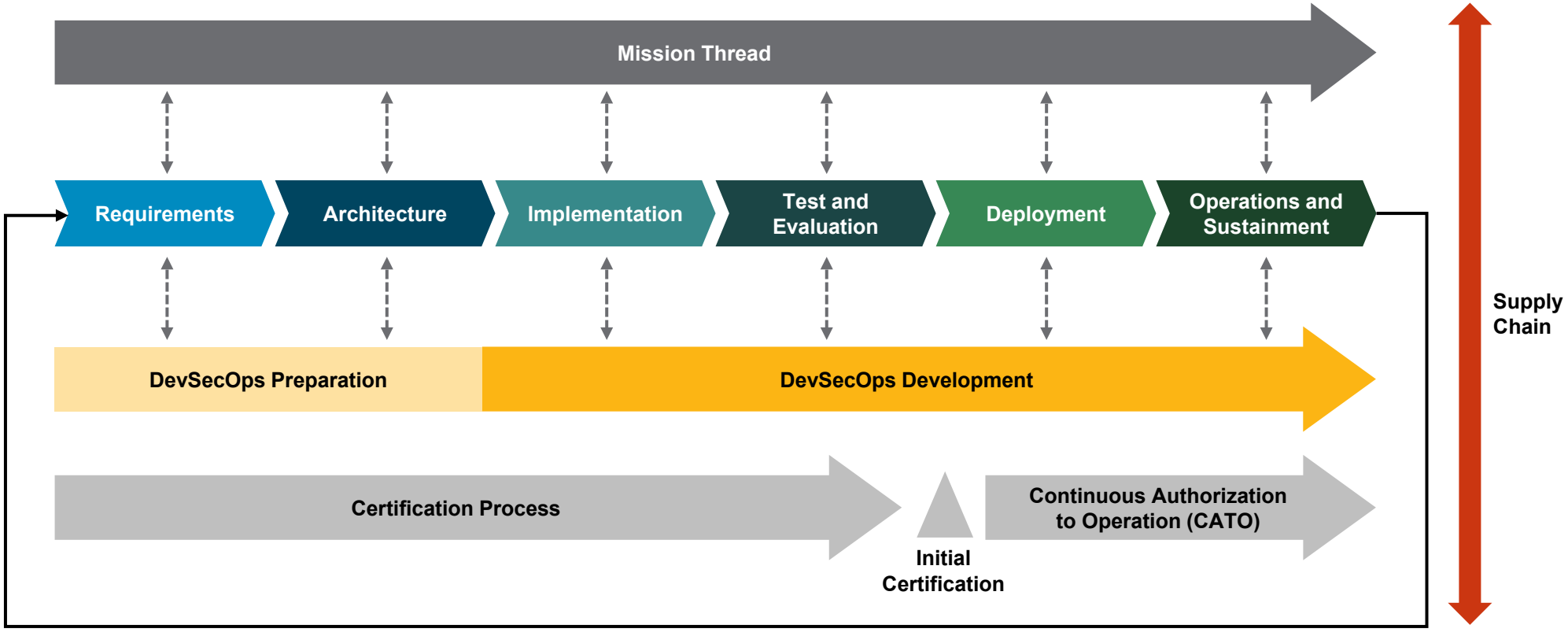
Epsilon (2011)

New York State Electric and Gas (2012)

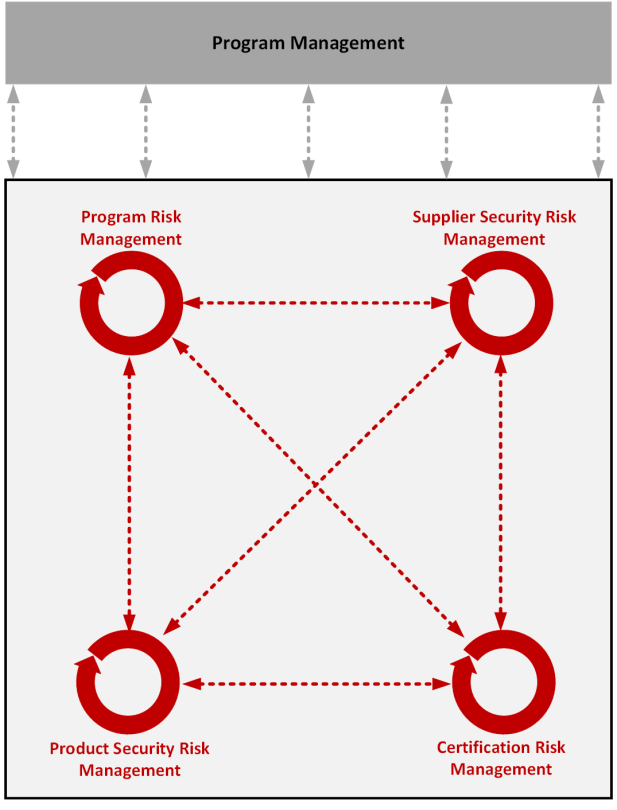
California Department of Child Support Services (2012)

- Thrift Savings Plan (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)
- 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.

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 ASF?

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.

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

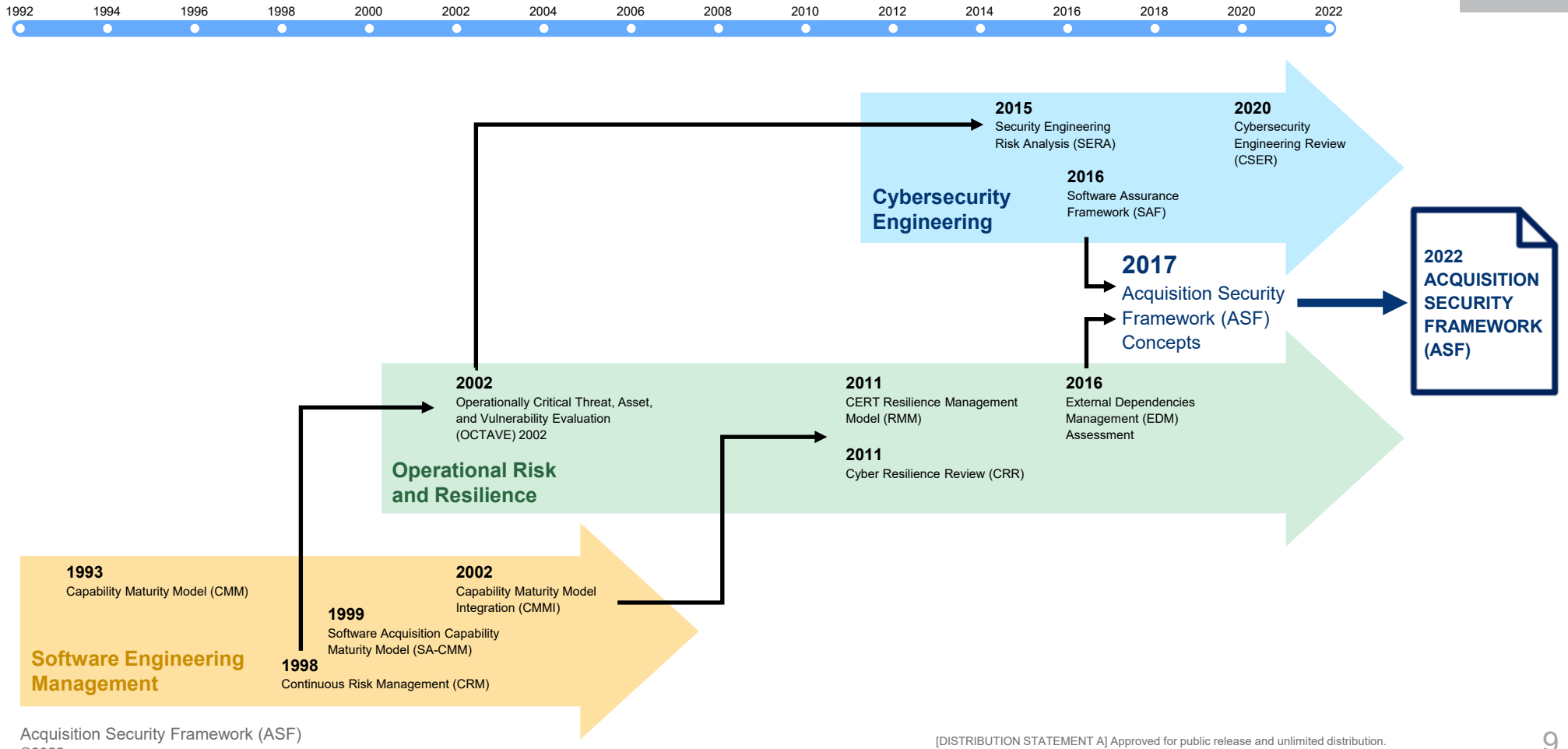
The ASF-based leading practice roadmap, in conjunction with its use of proactive consistent processes, facilitates efficient and predictable systems environments and more manageable delivery and risk outcomes.

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).

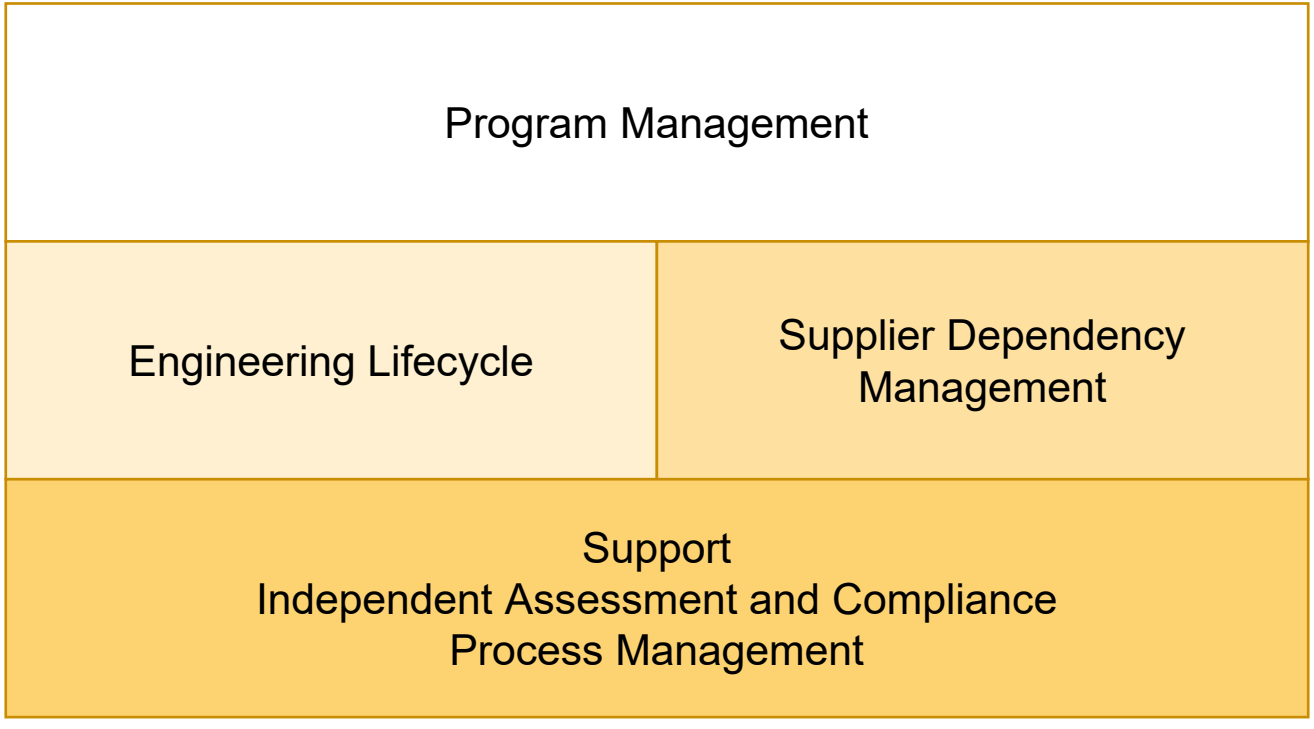
In later research, we investigated the lifecycle issues of supply chain risk and identified that the operational and mission impact of cyber risk increases as organizations become more dependent on suppliers and software.

ASF Research Lineage



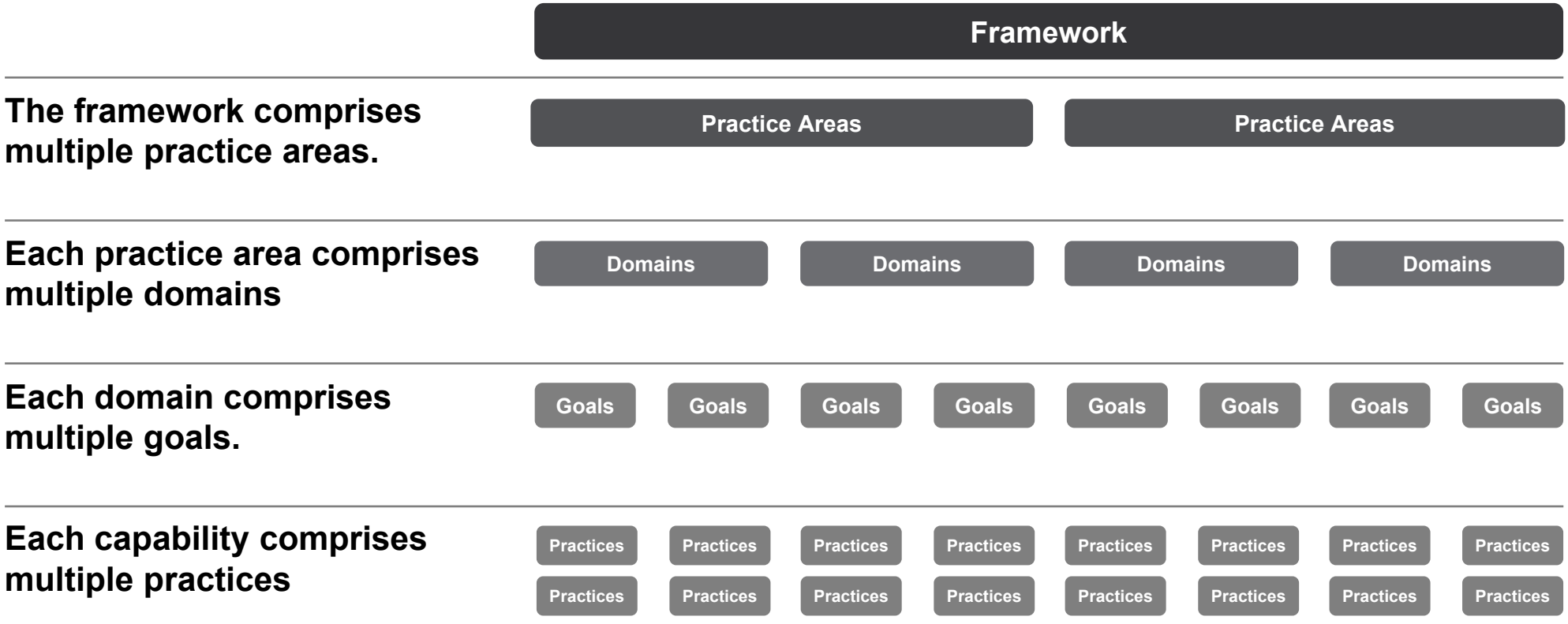
Acquisition Security Framework (ASF)

Acquisition Security Framework (ASF)



Four of the six areas are ready for use: Program Management, Engineering Lifecycle, Supplier Dependency Management, and Support. The remaining areas will be completed this calendar 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?

Summary

The Acquisition Security Framework (ASF), is designed to not only give you more insight and control over your supply chain, but also help you evaluate risks and gaps in how you manage your supply chains, including your processes for acquiring, engineering, and deploying secure software-reliant systems.

Reference: 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

The Team

Carol Woody
Principal Researcher
CERT Division
cwoody@cert.org

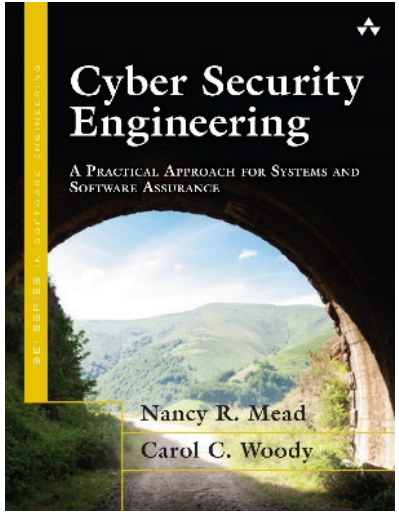
Chris Alberts
Principal Cyber Security Analyst
CERT Division

Charles Wallen
Information and Infrastructure Security Analyst
CERT Division

Mike Bandor
Senior Software Engineer
Software Solutions Division

.

Resources



Cyber Security Engineering

A practical Approach for Systems and Software Assurance

Nancy Mead

Carol Woody

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

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