P22-005 Acquisition Security Framework (ASF)

Carol Woody, Ph.D.
Principal Researcher

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

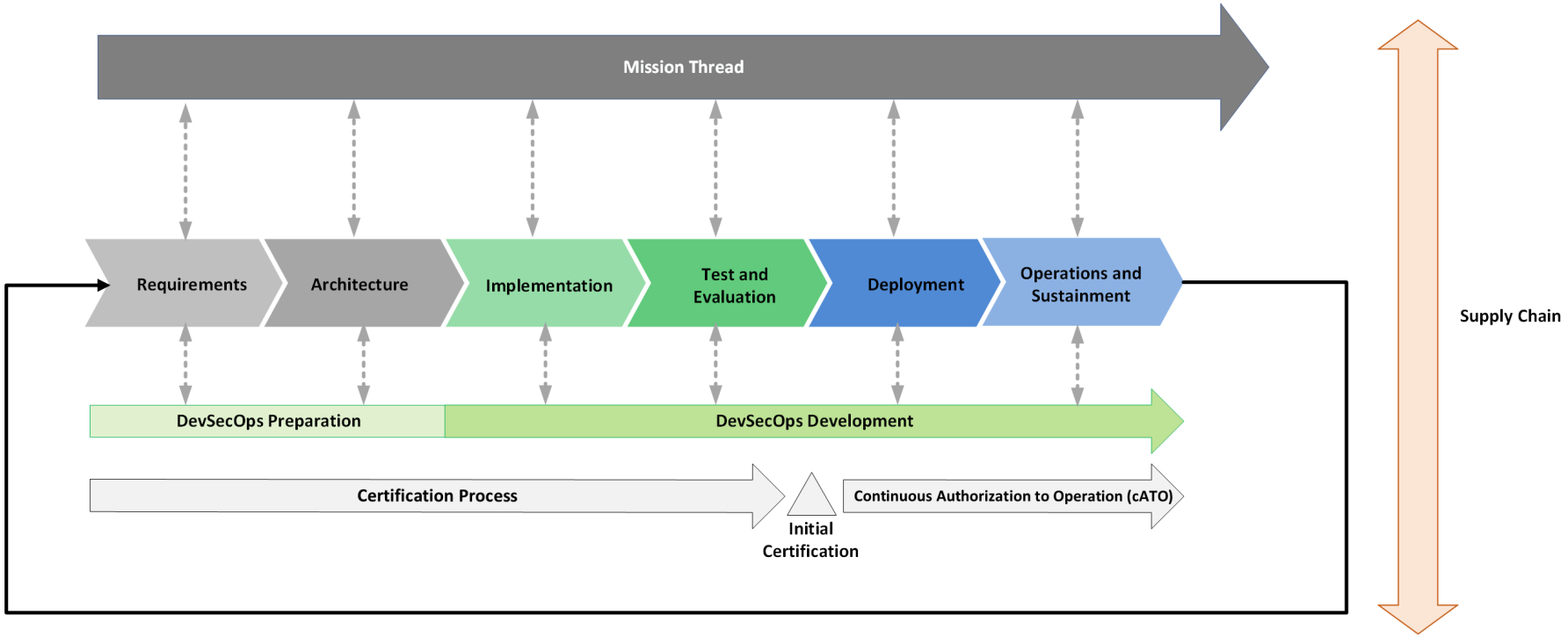
DM20-1061

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

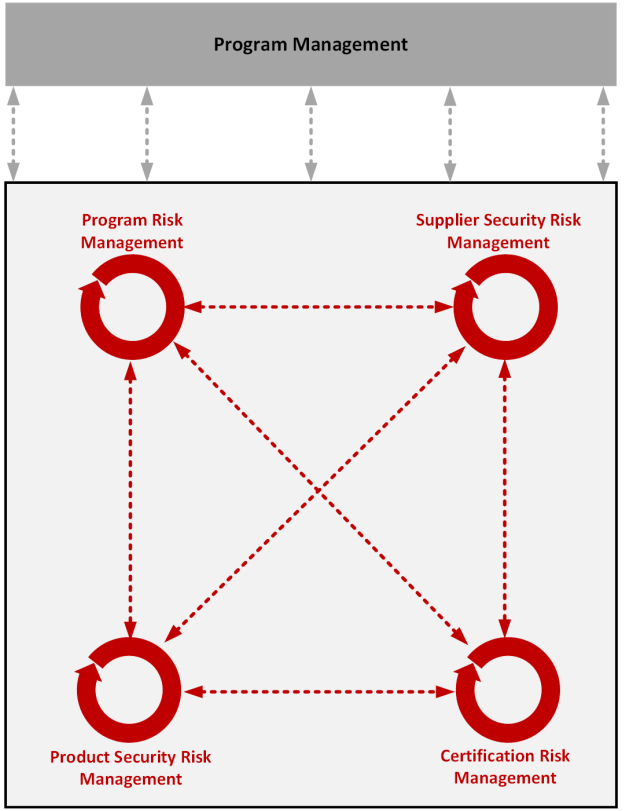


Challenge: Integrated Security and Supplier Risk Management across the Organization

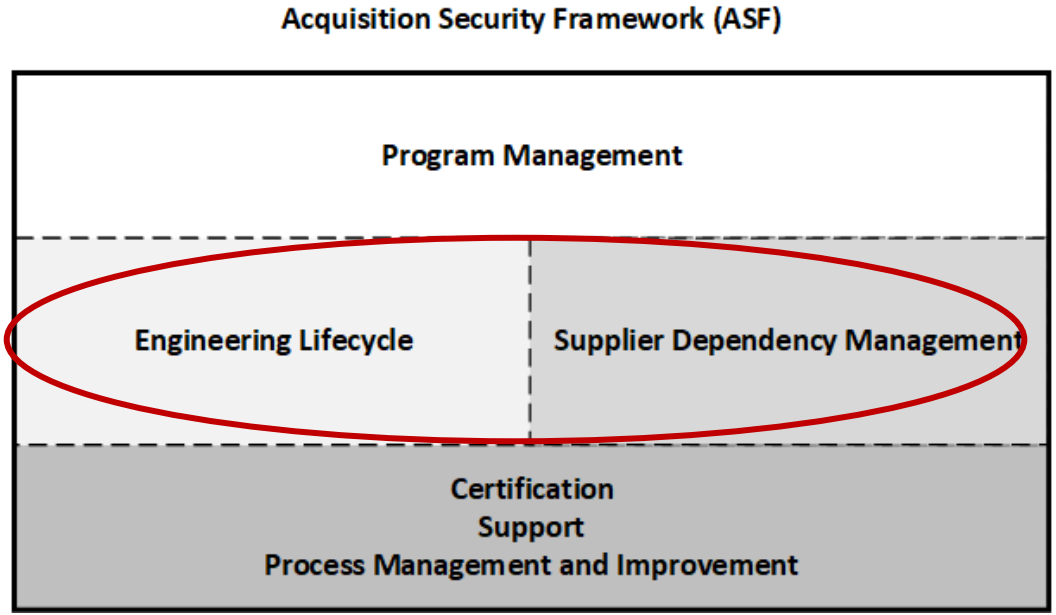
Security and supplier risk management are typically outside of the program risk management.

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 integrate with program risk management

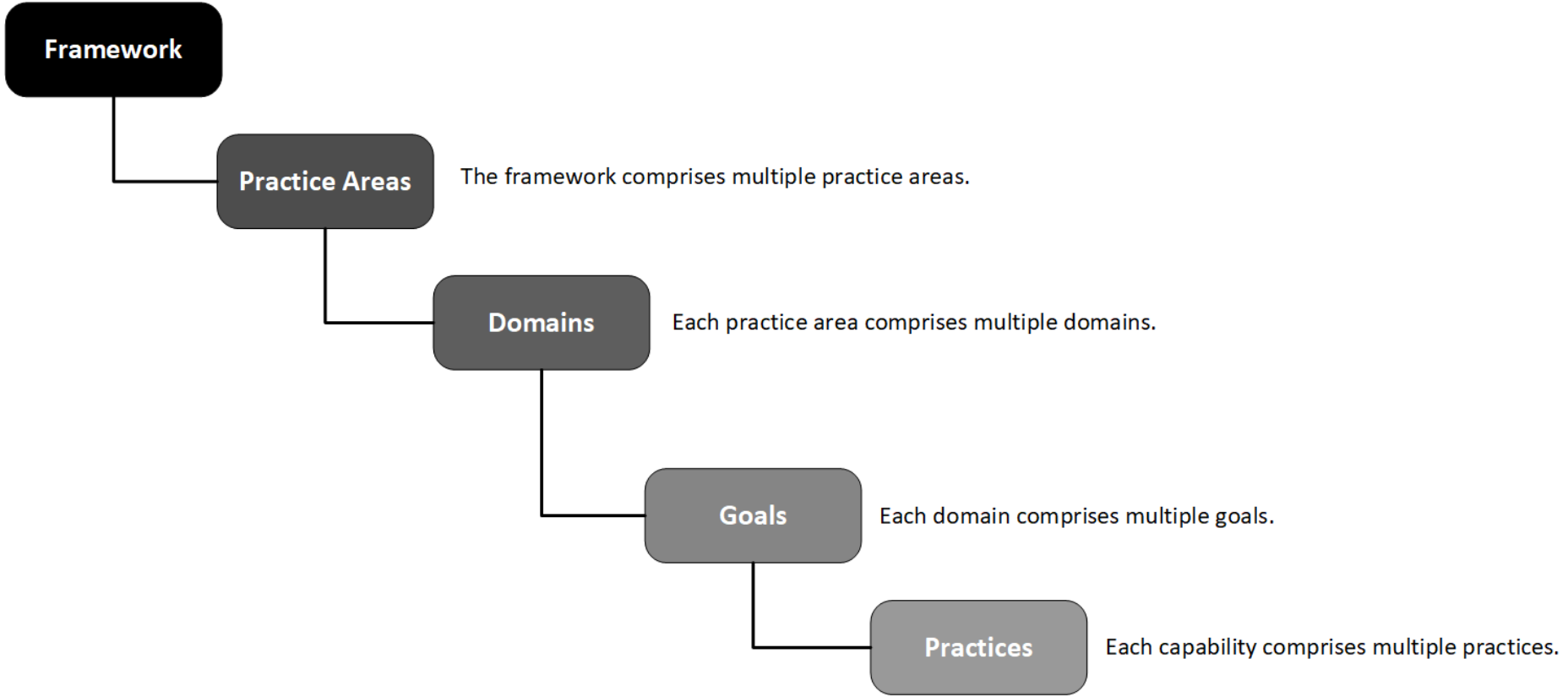


Acquisition Security Framework (ASF)



Initially we are focused on Engineering and Supplier Areas leveraging existing practices from Security Engineering Risk Analysis (SERA) and External Dependencies Management (EMD), in use for over 10 years.

ASF Structure



ASF Practice Area: Engineering Lifecycle

Domain	Key Concepts
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	Key Concepts
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

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

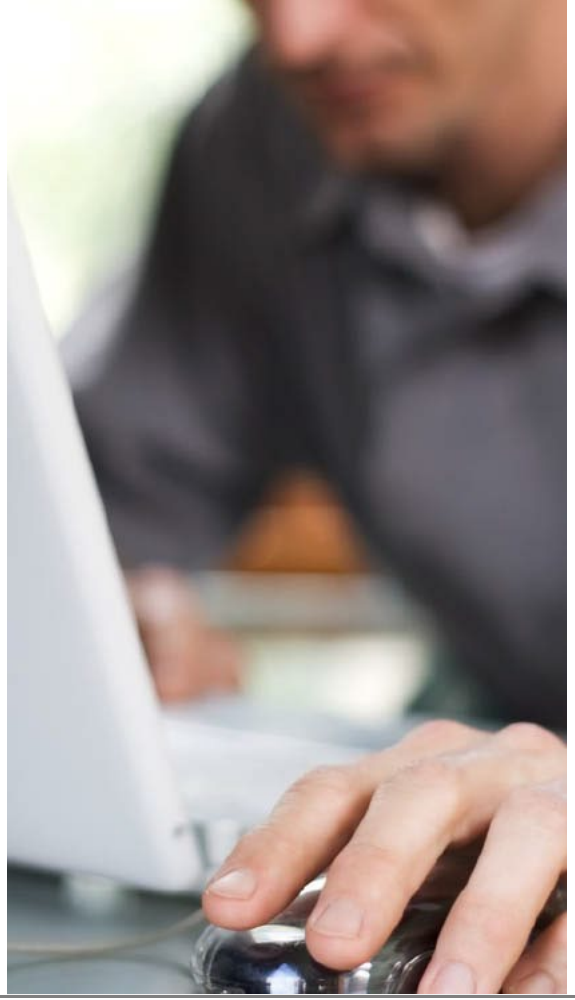
Goal 1—Establishing supplier relationships is planned.
The purpose of this goal is to assess whether entering into relationships with suppliers is planned.

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?

Details for each Supplier Dependency Management Goal are provided in the paper

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.



Key Points

Systems are increasingly software intensive and complex.

3rd 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 by itself.
- Supply chain risk management is a team sport.

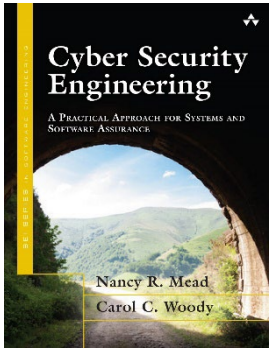
We welcome your feedback on the framework contents, which is currently based on our direct experience

- Which ASF concepts and practices are the most important?
- What concepts and practices that have not been addressed
- Submit any feedback to asf-info@sei.cmu.edu.

Contact Information

Carol Woody, Ph.D.

cwoody@cert.org



Web Resources

https://sei.cmu.edu/

CERT Cybersecurity Engineering and Software Assurance Professional Certificate
https://sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=33881