Addressing Supply Chain Risk and Resilience for Software Reliant Systems

Dr. Carol Woody
Charles M. Wallen

February 21, 2023

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.

DM23-0142

Barriers to Effective Management of Risk and Resilience

Complexity

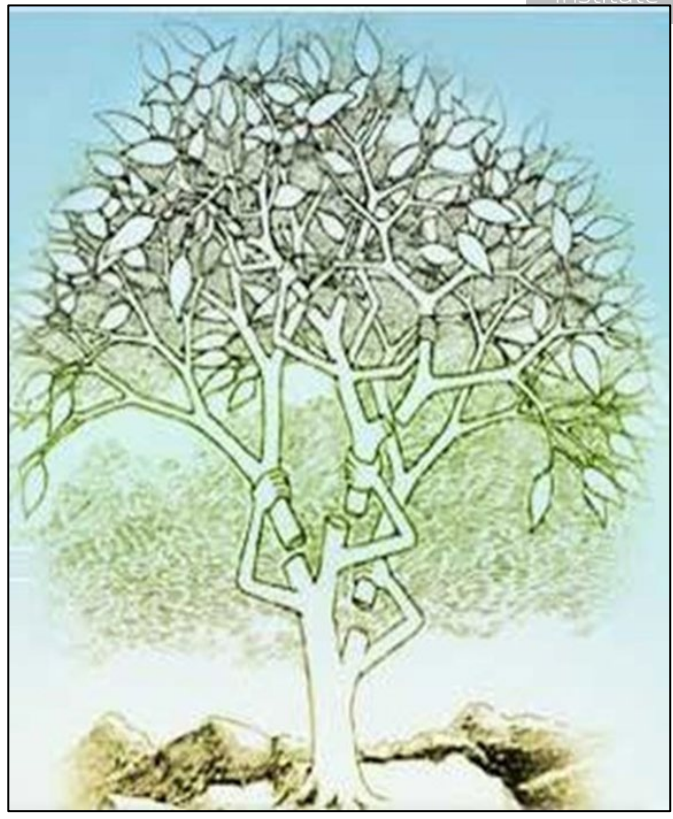
Siloed departments operating under different poorly defined and managed requirements

- Engineering
- Supplier/acquisition
- Operations

Reliance on outdated technical/management approaches

Reactive vs proactive risk management processes

Lack of coordinated planning, measurement, and reporting across the system lifecycle



Increasing Cyber Risks Require Attention

Growing role of 3rd party and open-source components using software-intensive solutions

- Supplier/acquisition dependencies are pervasive.
- Software driven system-of-systems environments are becoming the norm.

Shift in development strategies to DevSecOps increases the pace of change accelerating the system threat environment.

- Proactive management is essential to keep pace.
- Iterative development requires iterative security solutions.
- Automated solutions are critical to handle the scale of change

Leadership roles and coordination points change and evolve throughout the lifecycle and lack integration with security engineering.

- Pace of change makes integration and collaboration a necessity.
- Coordinated measurement, reporting, and management is critical for addressing cyber challenges.

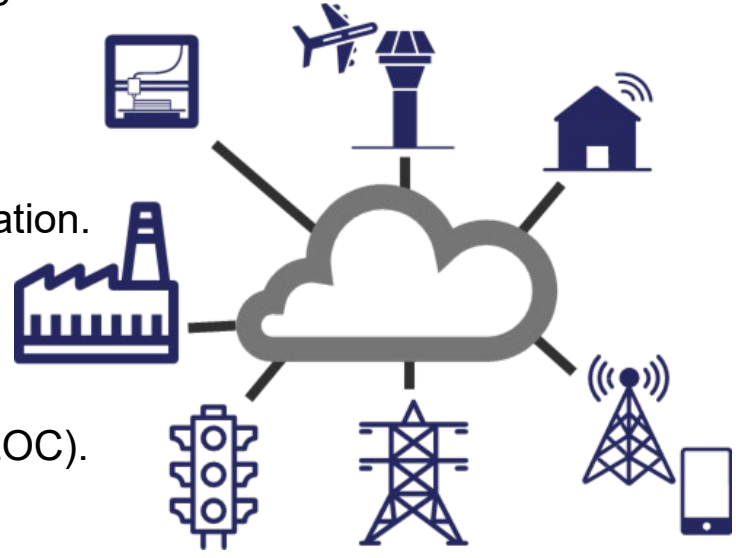
Software is Everywhere

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.

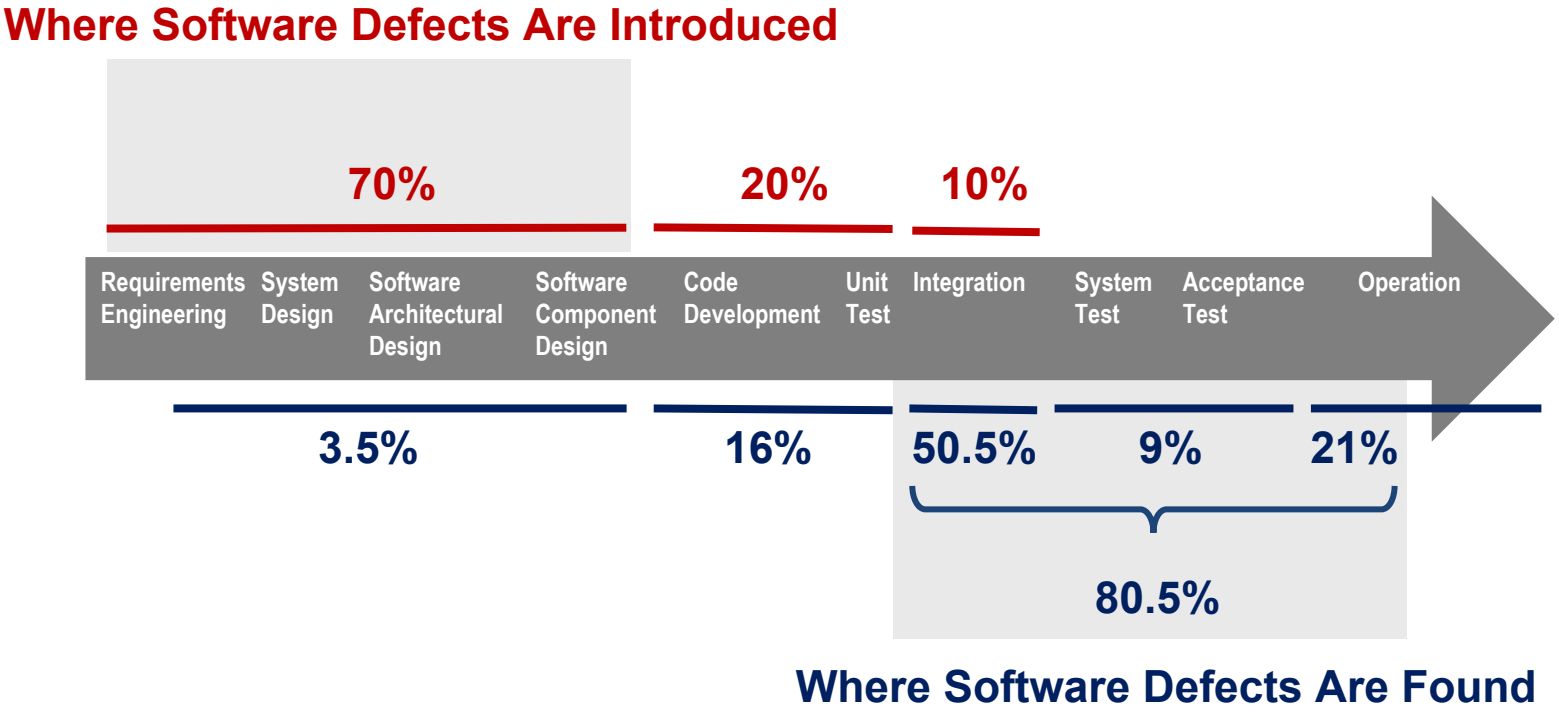


All software has defects:

- 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)

Most Software Defects Are Found Long After They Are Introduced



Sources: *Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies

Supply Chain/Acquisition Risk is Increasing

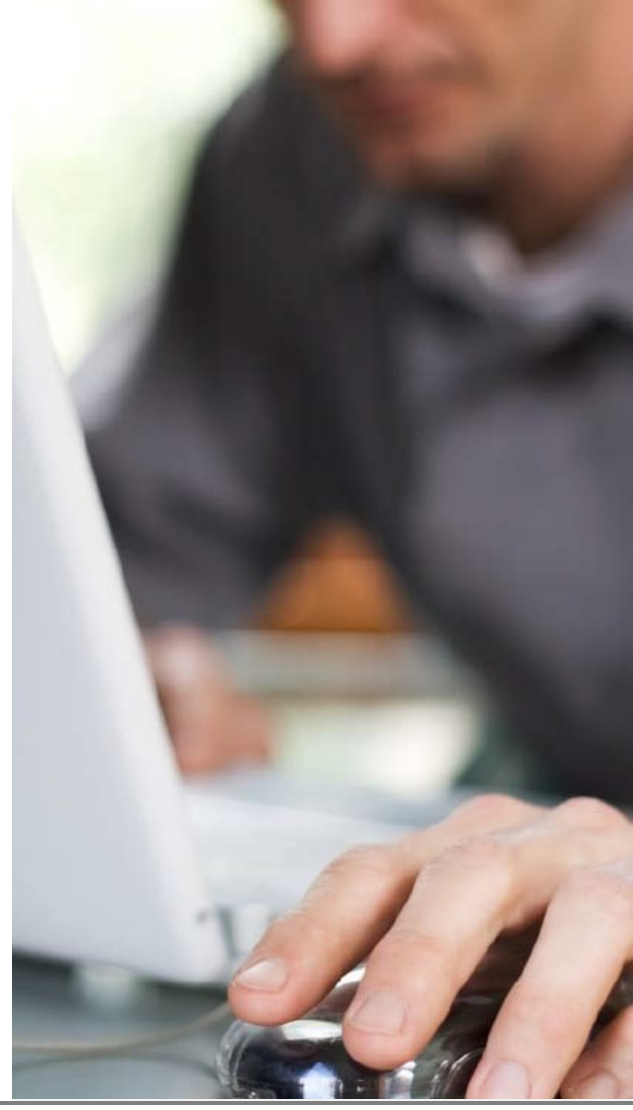
More than 230,000 organizations were examined to discover their relationships with third parties. 98% of organizations have a relationship with a third party that has been breached within the last two years.
https://www.securityweek.com/98-of-firms-have-a-supply-chain-relationship-that-has-been-breached-analysis/

- 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

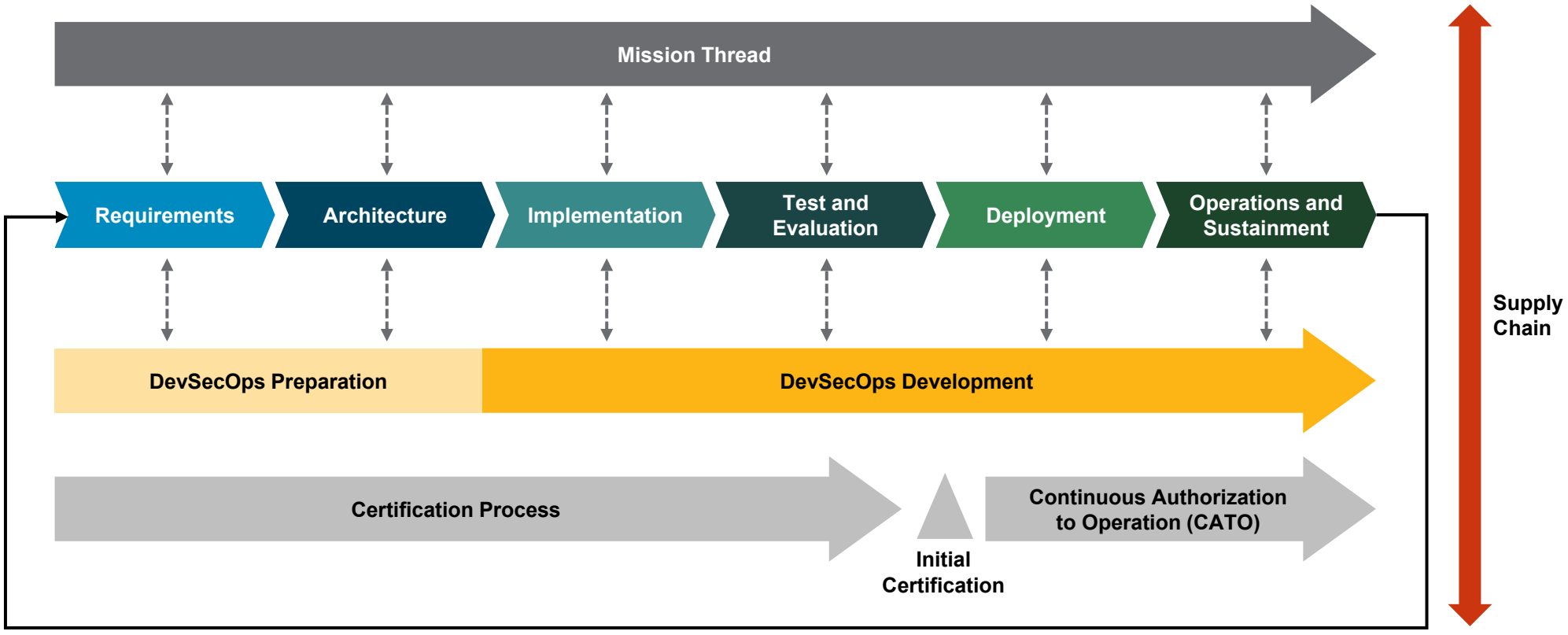
Acquisition Security Framework (ASF):

Introduction

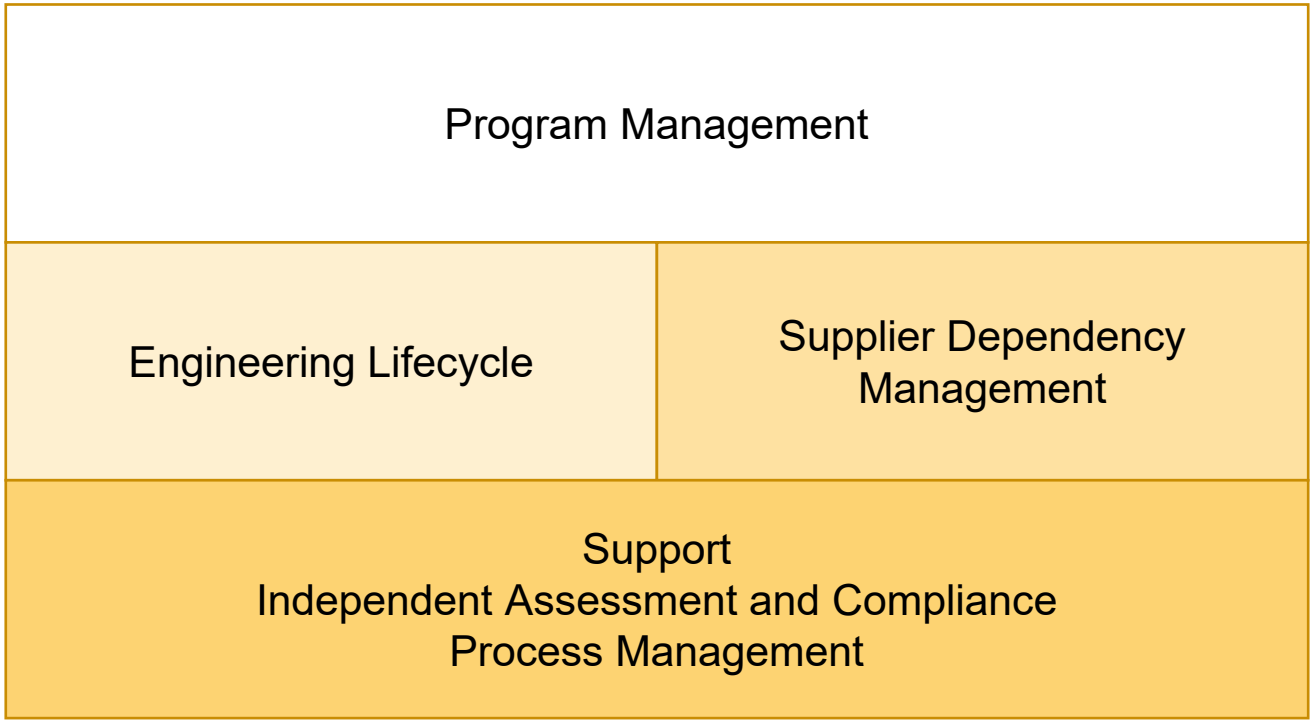
Virtually all products or services that an organization acquires are supported by or integrated with information technology that include third-party components and services. Practices critical to monitoring and managing these risks are scattered across many parts of the organization and typically isolated in stove-pipes resulting in inconsistencies, gaps, and slow response.



Acquisition Cybersecurity Problem Space

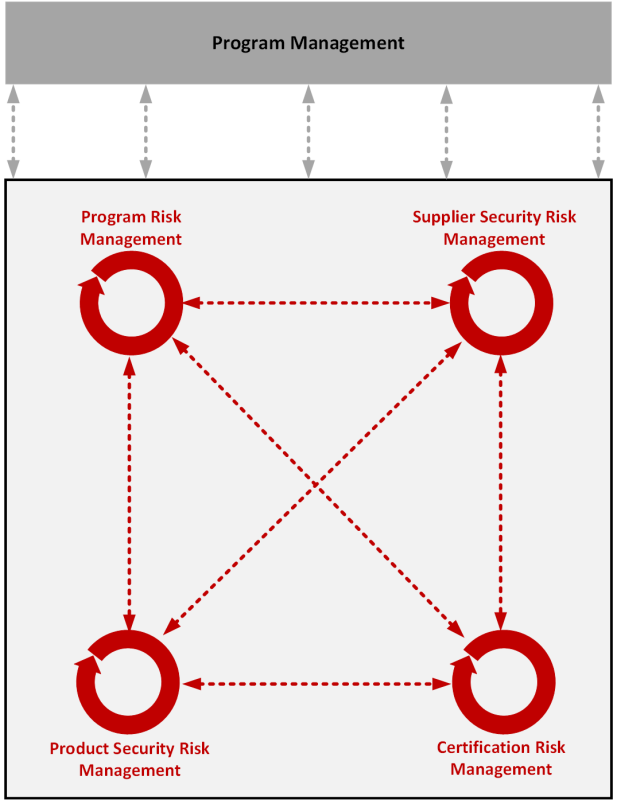


Acquisition Security Framework (ASF)



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

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.

Challenge: Process Management and Improvement

Higher degrees of process management translate to more stable environments that

- Produce consistent results over time
- Are able to achieve their missions during times of stress

The challenge is to implement an appropriate level of maturity for security practices across

- Multiple organizations/program units
- All lifecycle activities

Research Lineage of ASF

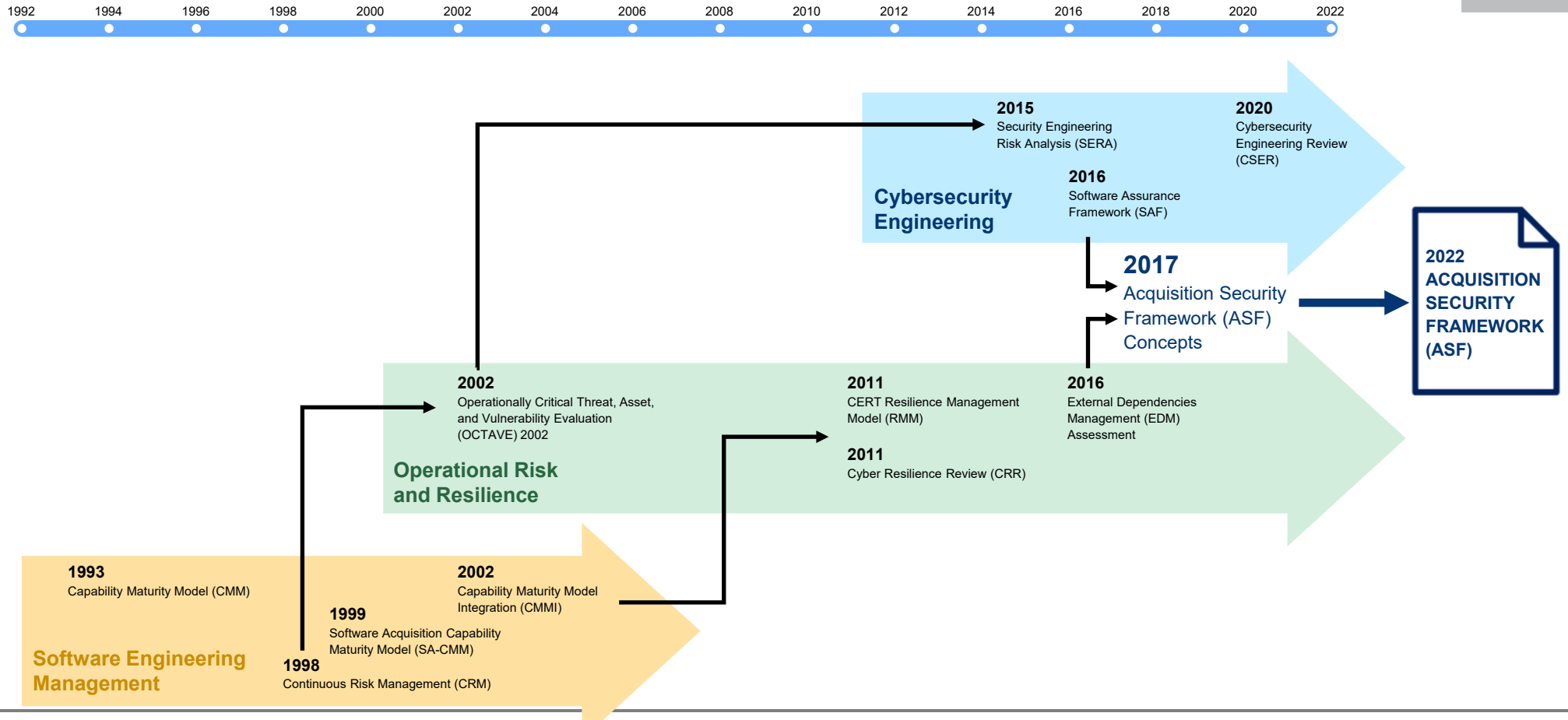
2010 Software Engineering Institute (SEI) research showed few organizations considered supply chain risk within the acquisition and development lifecycle beyond a narrowly defined vetting of the supplier's capabilities at the time of an acquisition (Ellison, Goodenough, Weinstock, & Woody, 2010*).

Risk stems from the reality that virtually all products or services are supported by or integrated with information technology. Software controls virtually everything we use today... (Alberts, Haller, Wallen and Woody 2017*)

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.

* Found at http://sei.cmu.edu

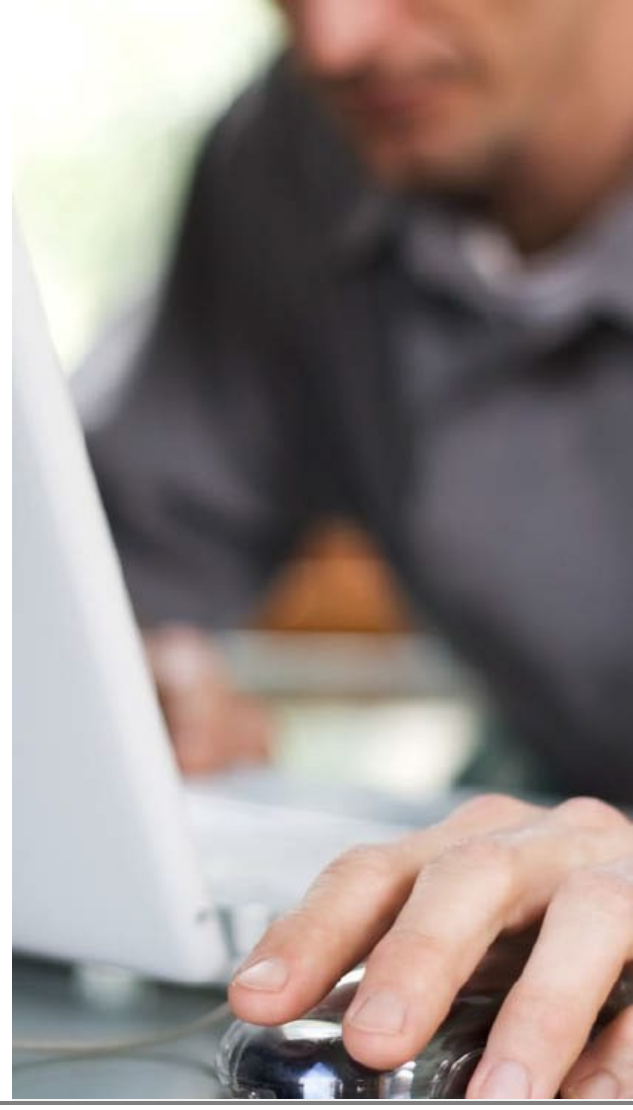
ASF Research Lineage



Acquisition Security Framework (ASF):

ASF Overview and Structure

The ASF helps correlate the management of supply chain risk across the many components of a system, including hardware, network interfaces, software interfaces, and mission capabilities. Simplifying assumptions that focus only part of this risk space have continually failed. We must plan for and manage the complexity.



What is the ASF?

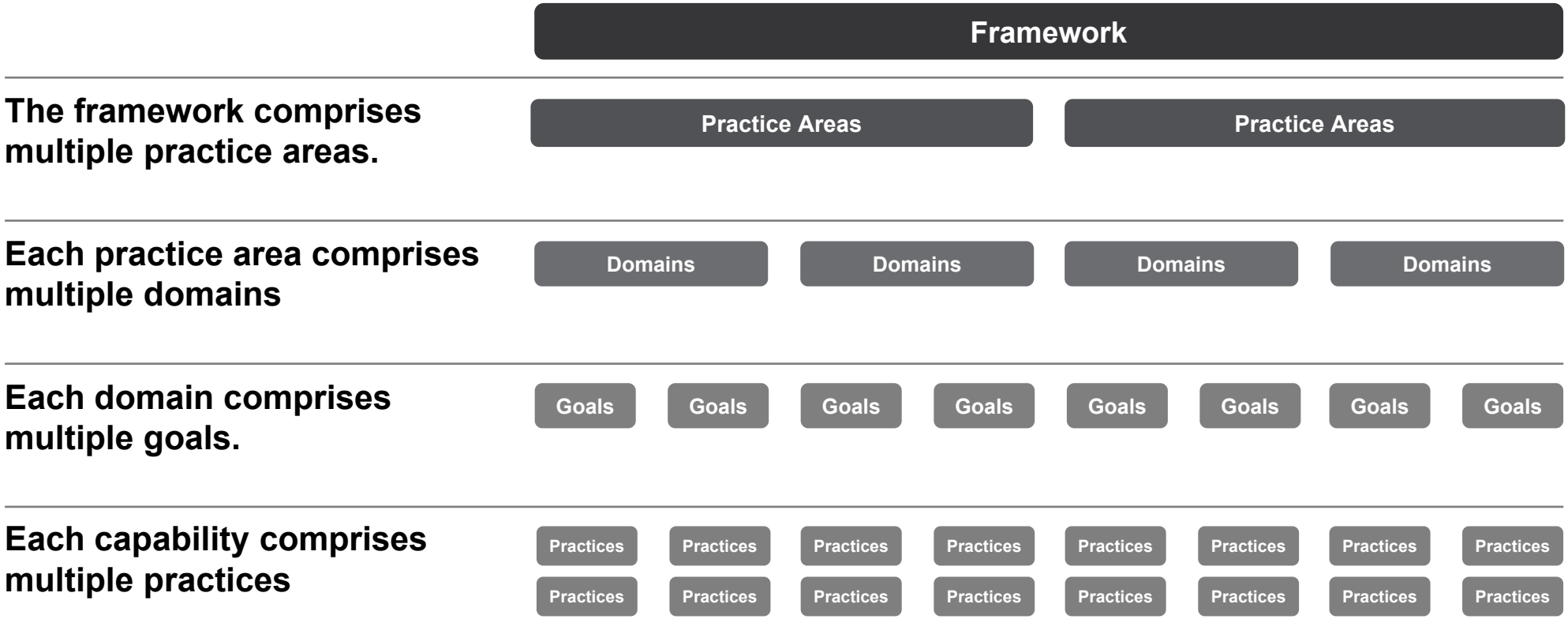
The Acquisition Security Framework (ASF) is a collection of leading practices for building and operating secure and resilient software-reliant systems.

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

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

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

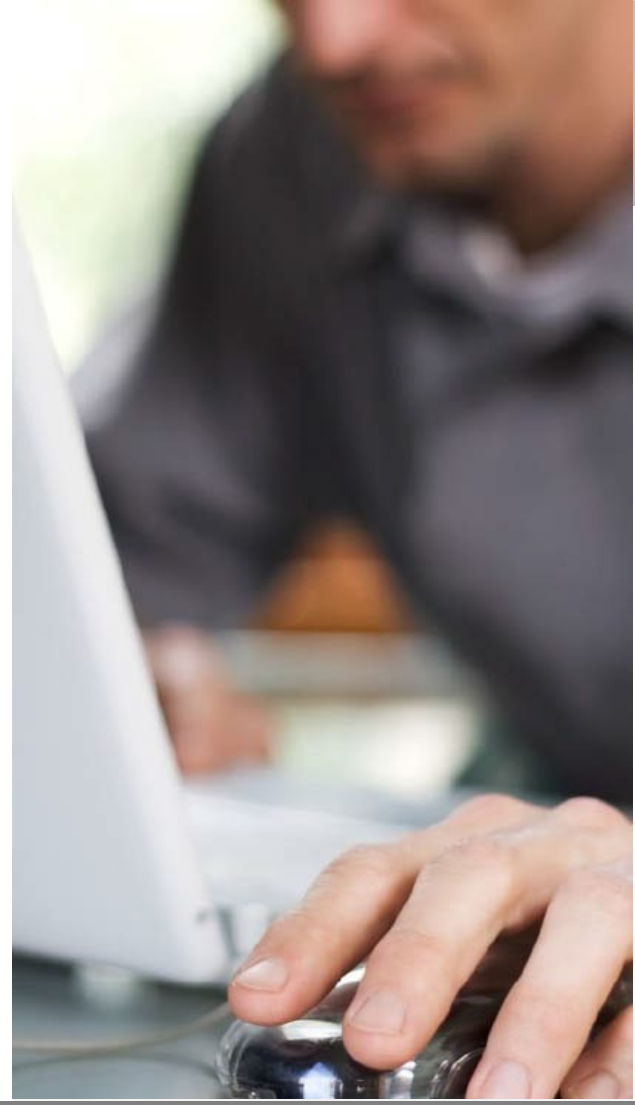
ASF Structure



Acquisition Security Framework (ASF):

ASF Practice Area: Program Management

To avoid becoming a victim of the latest attack, vigilance is required on multiple fronts. Strategic decisions must be made on the appropriate balance of protection and sustainment, as well as the level of risk that can be tolerated.



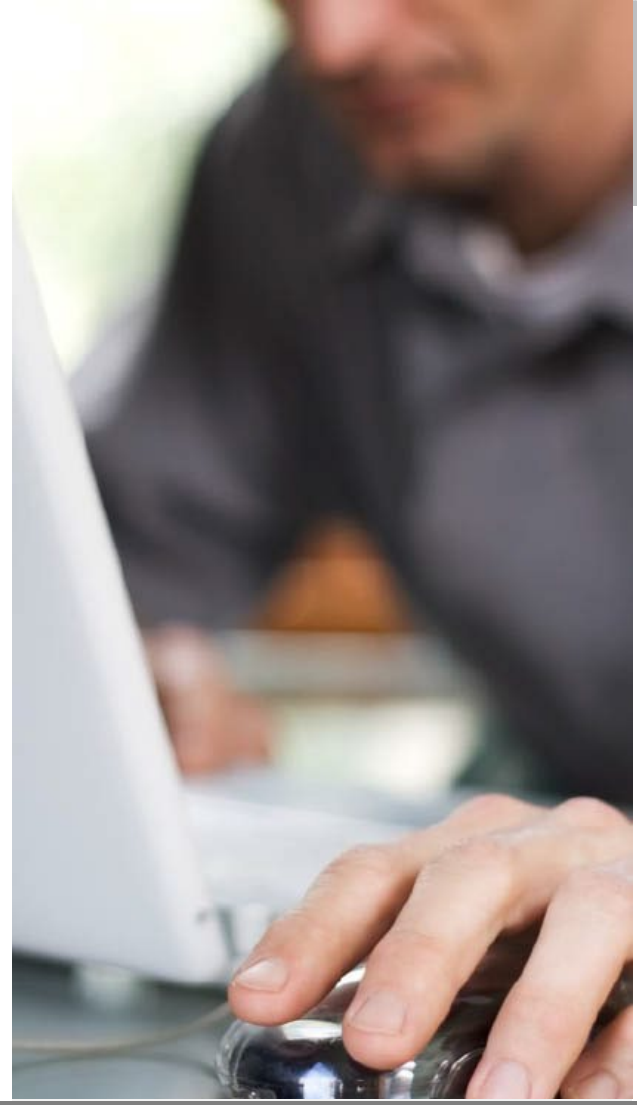
ASF Practice Area: Program Management

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

Acquisition Security Framework (ASF):

ASF Practice Area: Engineering Lifecyle

Cyber attacks are designed to exploit weaknesses and vulnerabilities in a system's software components, which makes software the focal point for early lifecycle cyber-risk analysis. Software must be designed and architected with the knowledge that it must function as intended in an increasingly contested, challenging, and interconnected cyber environment.



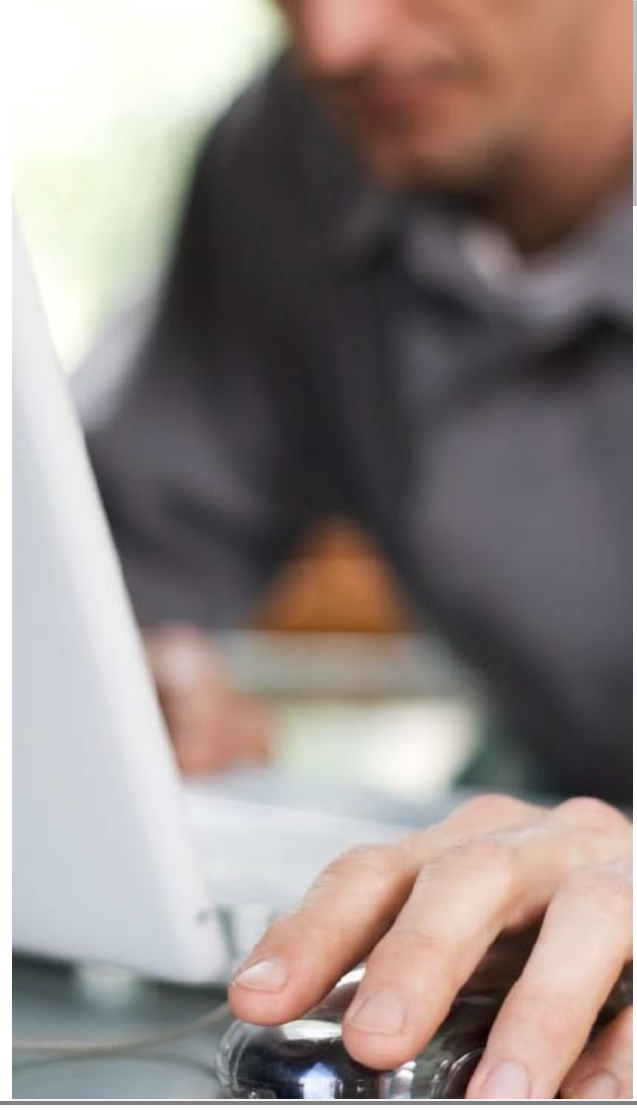
ASF Practice Area: Engineering Lifecycle

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

Acquisition Security Framework (ASF):

ASF Practice Area: Supplier Dependency Management

Supply chain cyber risks stem from a variety of dependencies, and in particular from the processing, transmittal, and storage of data, as well as on information and communications technology. These cyber risks in the supply chain are broad and significant. Important mission capabilities can be undermined by an adversary's cyber-attack on third parties, even in situations where the organization is not explicitly contracting for technology or services like data hosting.



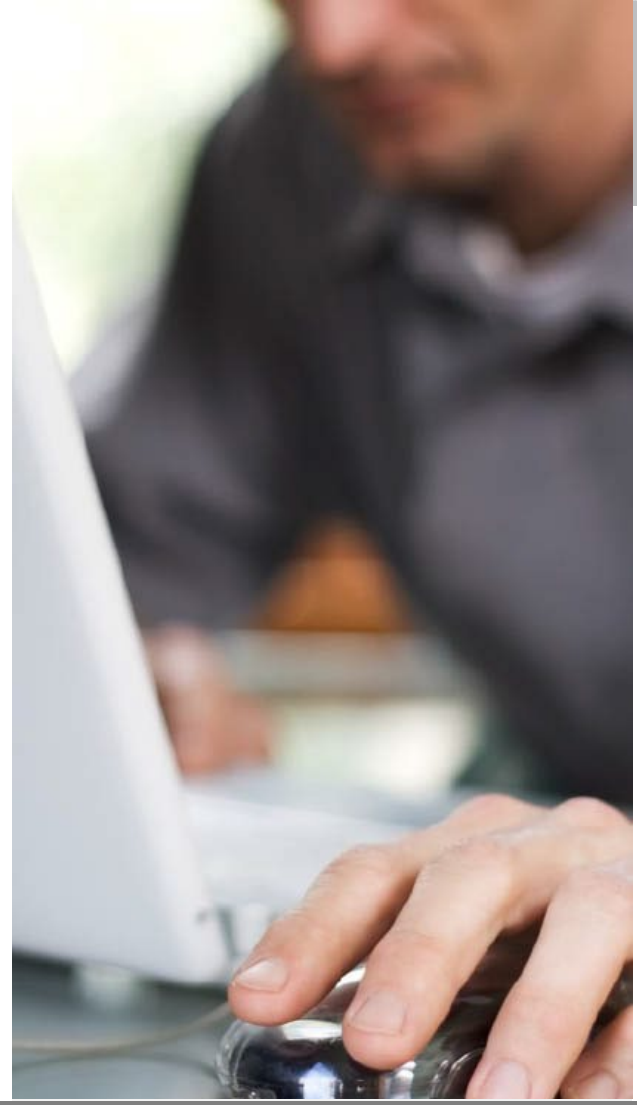
ASF Practice Area: Supplier Dependency Management

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

Acquisition Security Framework (ASF):

ASF Practice Area: Support

Organizational support activities provide a broad range of services, including security management, facility management, access management, measurement and analytics, and training. The Support practice area outlines leading practices that facilitate integrated support for acquiring, developing, and managing secure/resilient systems across their lifecycle.

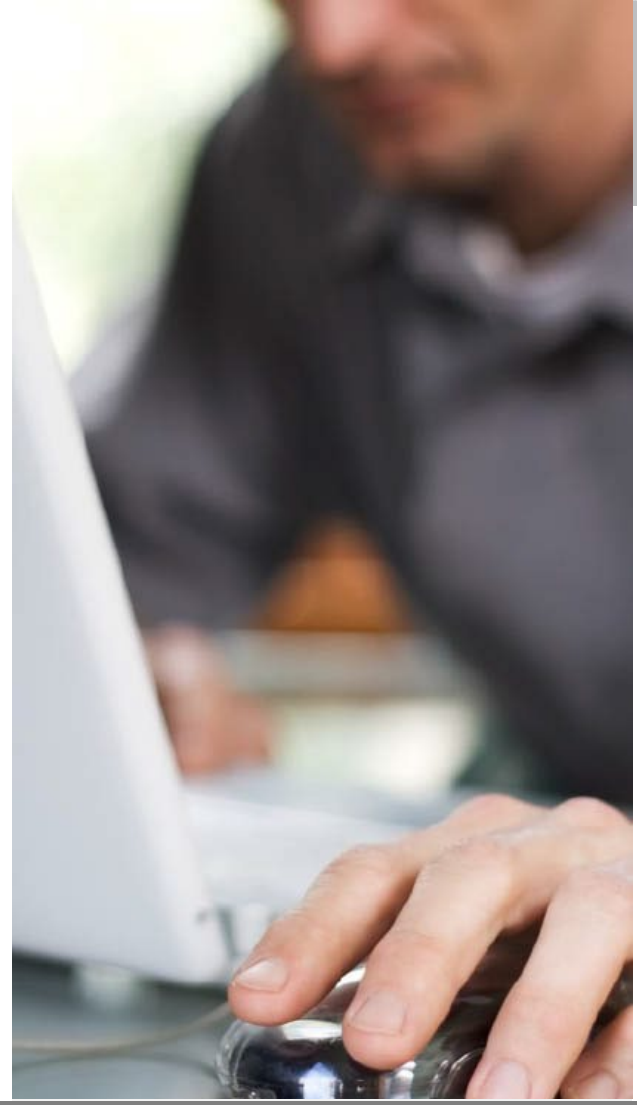


ASF Practice Area: Support

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

Acquisition Security Framework (ASF):

ASF Considers the Management of System Risk Across the Lifecycle



ASF – A Resource for Managing Areas of Risk

Apply the ASF principles, concepts and approach to manage software intensive system risk across a range of key lifecycle challenges including:

1. Systems Engineering
2. System Supplier Oversight
3. Program Security/Resilience Oversight
4. Support for Measurement Activities

ASF Target Risk Area Example – Systems Engineering

Technical Activity Management

Goal 1—Engineering activities are planned and managed.

The purpose of this goal is to oversee the execution of engineering activities, including those performed by third-party contractors.

1.	Is a plan for conducting the engineering activity developed and implemented?
2.	Is progress against the plan tracked and reported?
3.	Are criteria established for reviewing and accepting acquisition and engineering work products?
4.	Are acquisition and engineering work products reviewed and accepted?
5.	Are issues and risks that can affect engineering activities identified and resolved?
6.	Are issues and risks that can affect engineering activities escalated to program management and other stakeholders as appropriate?

ASF Target Risk Area Example – System Supplier Oversight

Supplier Performance Management

Goal 2—Supplier performance is governed and managed.

The purpose of this goal is to assess whether performance is considered when evaluating suppliers that support the security/resilience of the program or system.

1.	Is the performance of suppliers monitored against the security/resilience requirements of the program or system?
2.	Is the responsibility for monitoring and managing the supplier established and maintained?
3.	Are supplier performance issues documented and reported to the appropriate stakeholders?
4.	Are corrective actions taken to address issues with supplier performance?
5.	Are corrective actions evaluated to ensure issues are remedied?

ASF Target Risk Area Example – Program Security/Resilience Oversight

Program Monitoring and Management

Goal 3—Security/resilience activities are monitored and managed.

The purpose of this goal is to monitor and manage security/resilience activities across all program teams.

1.	Are security/resilience tasks allocated and managed across all program teams?
2.	Is the progress of the program's security/resilience tasks monitored and updated as needed?
3.	Is the security/resilience budget tracked and updated?
4.	Is program compliance with security/resilience policies, laws, and regulations monitored and managed?
5.	Are security/resilience reviews of program tasks performed?
6.	Are the results of security/resilience reviews prioritized and addressed?
7.	Is program decision making supported by security/resilience measurement and metrics?
8.	Are stakeholders' inputs for security/resilience included when making program management decisions?
9.	Is the delivery of security/resilience capabilities into the user environment managed and facilitated?

ASF Target Risk Area Example – Support for Measurement Activities

Measurement and Analysis

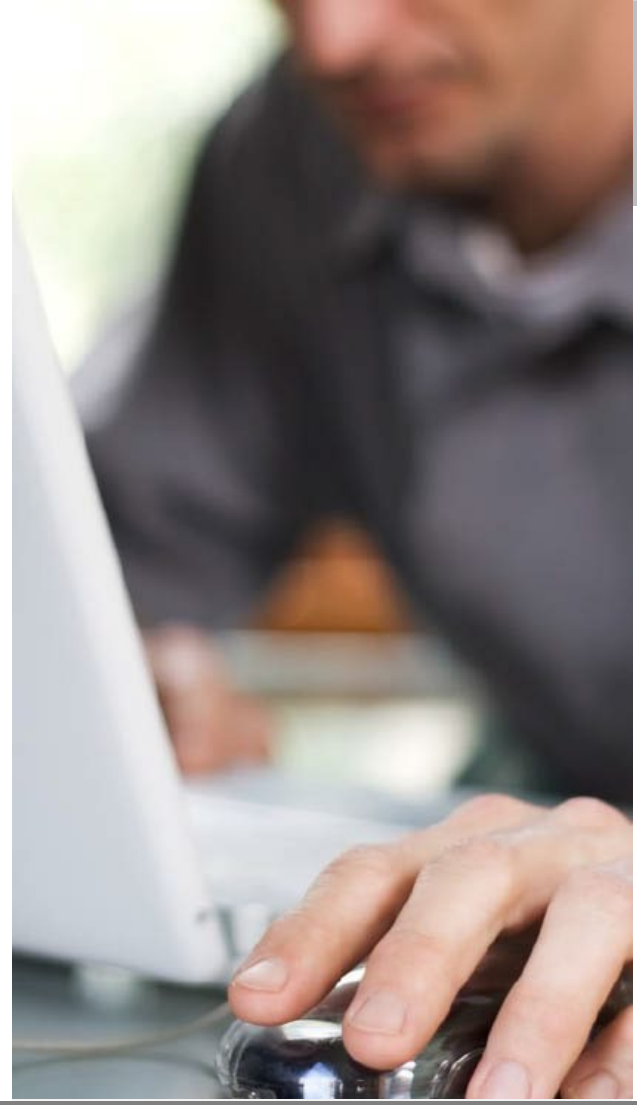
Goal 2—Security/resilience measurement data is collected, analyzed, and used to support decisions.

The purpose of this goal is to support monitoring and effective decision making based on security/resilience measurement.

1.	Is there a plan for the measurement and analysis of security/resilience activities?
2.	Is data about security/resilience measurement collected and communicated to relevant stakeholders according to the plan?
3.	Are measurement and analysis gaps in the plan identified?
4.	Are plan measurement and analysis gaps communicated to relevant stakeholders?
5.	Is data about security/resilience measurement managed according to the plan?
6.	Is data about security/resilience measurement analyzed and interpreted to support risk decisions?
7.	Are security/resilience measurement objectives identified?
8.	Are security/resilience measures that address measurement objectives identified?

Acquisition Security Framework (ASF):

Wrapping Up



Imperatives for Deploying the Acquisition Security Framework (ASF)

Today's threat landscape requires proactive management of cyber risk across the system lifecycle.

Systems are increasingly software intensive and complex, requiring an integrated engineering, development, and operational focus to ensure security and resilience in the known threat landscape.

Comprehensive acquisition management is essential to support effective management of cyber risk.

Traditional management approaches are failing to meet today's cyber risk challenges.

Summary

The Acquisition Security Framework (ASF) is designed to:

- Identify ways to improve and coordinate your processes for acquiring, engineering, and deploying secure software-reliant systems
- Provide a means to evaluate risks and gaps in existing activities used to manage systems across their lifecycle
- Establish more insight and control over your supply chain

Next Steps

The scope of the practices needed for effective supply chain risk management can be overwhelming. Where should an organization/program start?

We will develop tailored versions of ASF for targeted needs such as:

- Software Bill of Materials (SBOM)
- Zero Trust (ZT)

Two practice areas remain to be finalized:

- Process Management
- Independent Assessment and Compliance

Plans are underway for an update to the ASF technical note in FY23 to complete the framework.

The Team

Carol Woody
Principal Researcher
CERT Division

Chris 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

Review and Feedback Opportunity

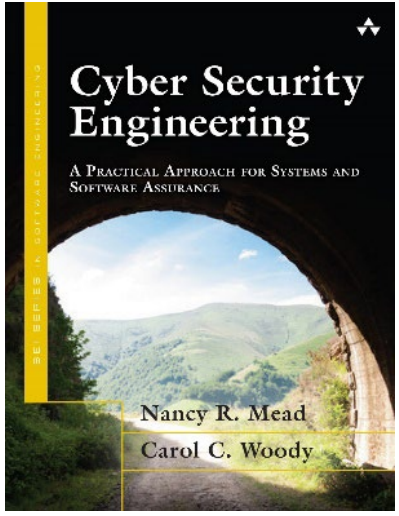
We welcome your feedback regarding

- ASF concepts and practices
- Concepts and practices that have not been addressed

Submit any feedback to asf-info@sei.cmu.edu.

The SEI will be hosting a Supply Chain Risk Management Symposium Oct 10-11 in Arlington this Fall. All who have interest are welcome. For any questions or interest in sponsorship, please reach out to Brett Tucker at batucker@cert.org

Additional Cybersecurity 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