Carnegie Mellon University
Software Engineering Institute

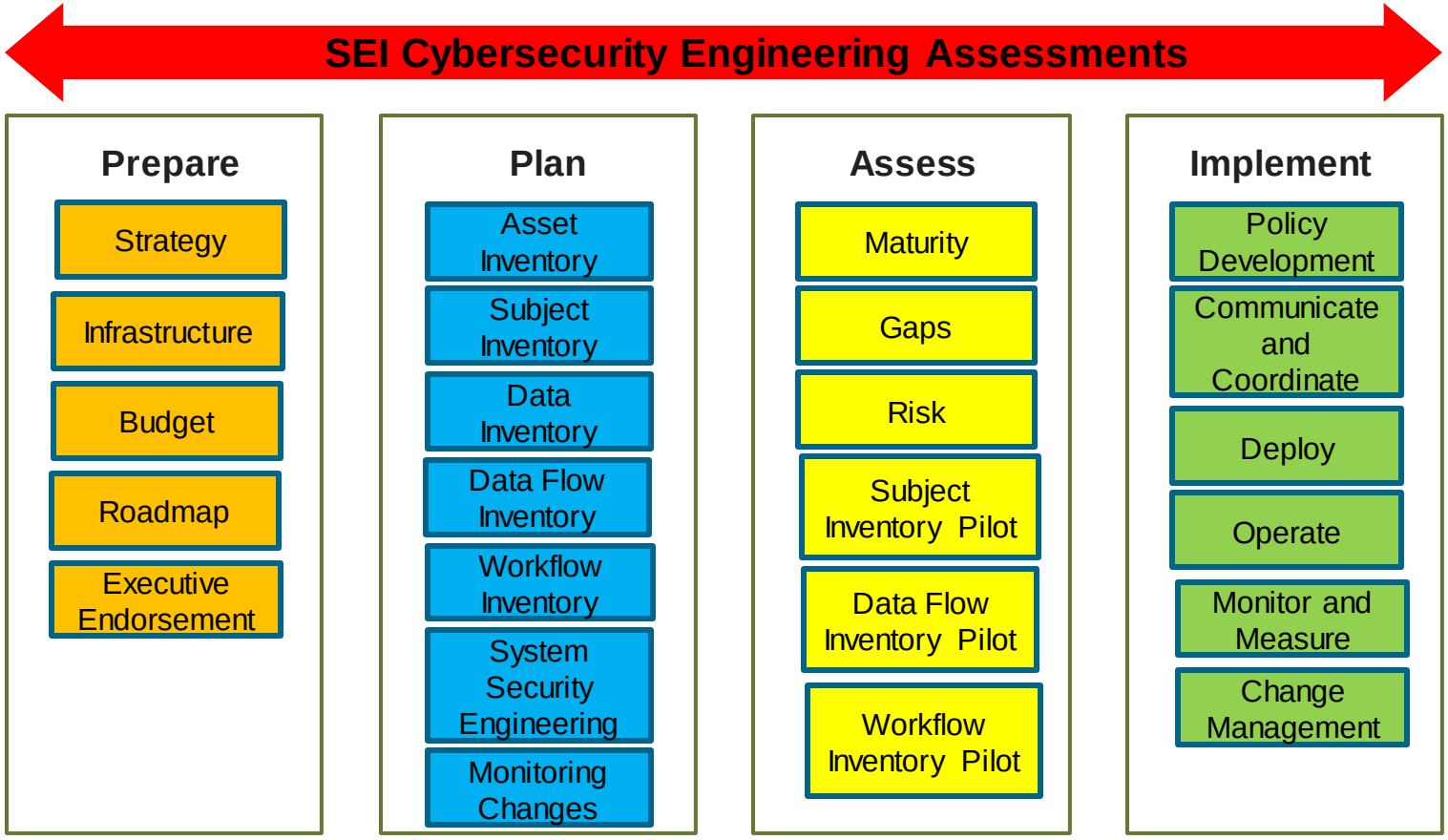
Discussing Best Practices for Implementing a Zero Trust Architecture

JULY 20, 2023

Tim Morrow
CMU/SEI CERT Situational Awareness Technical Manager

Document Markings

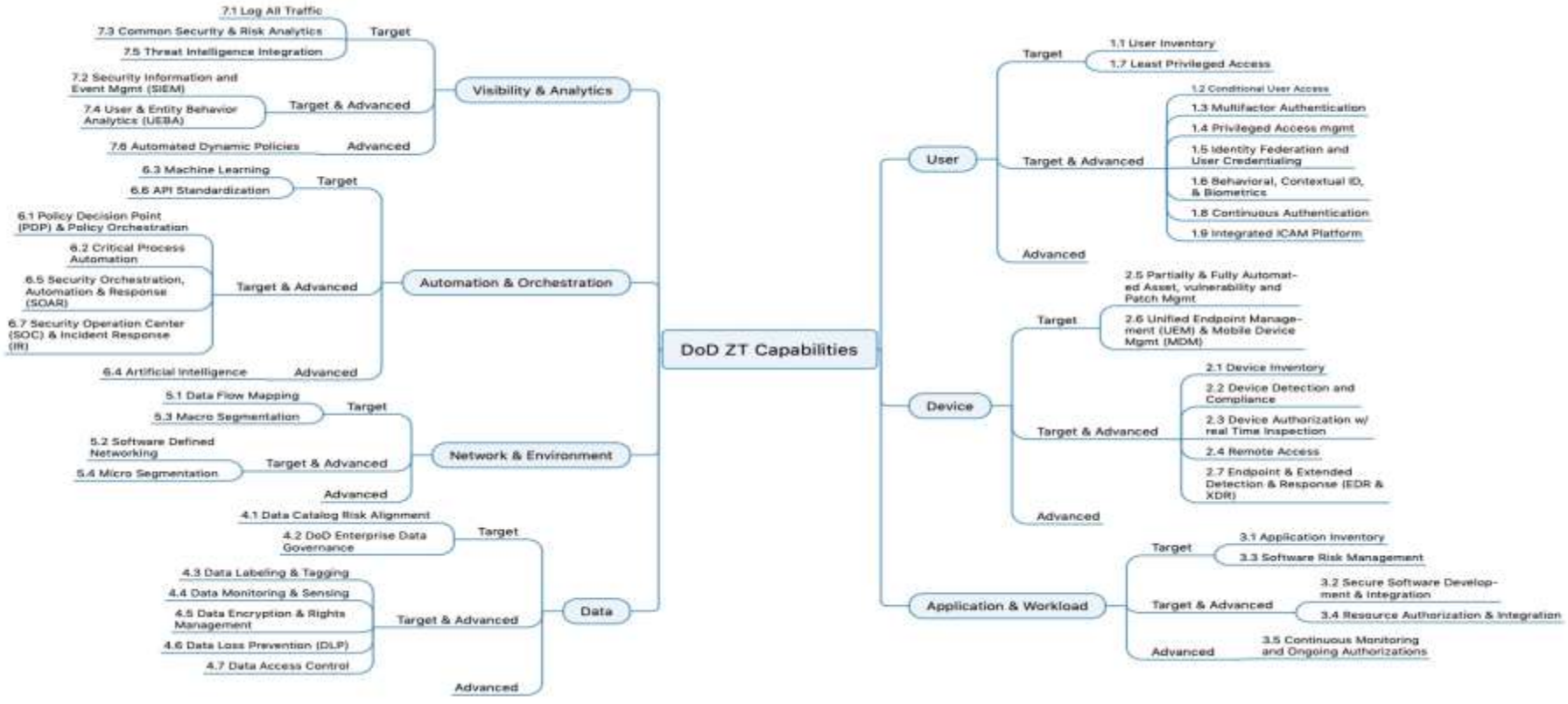
Software Engineering Institute (SEI) Zero Trust Journey



Prepare

1. Strategy
2. Infrastructure
3. Budgeting

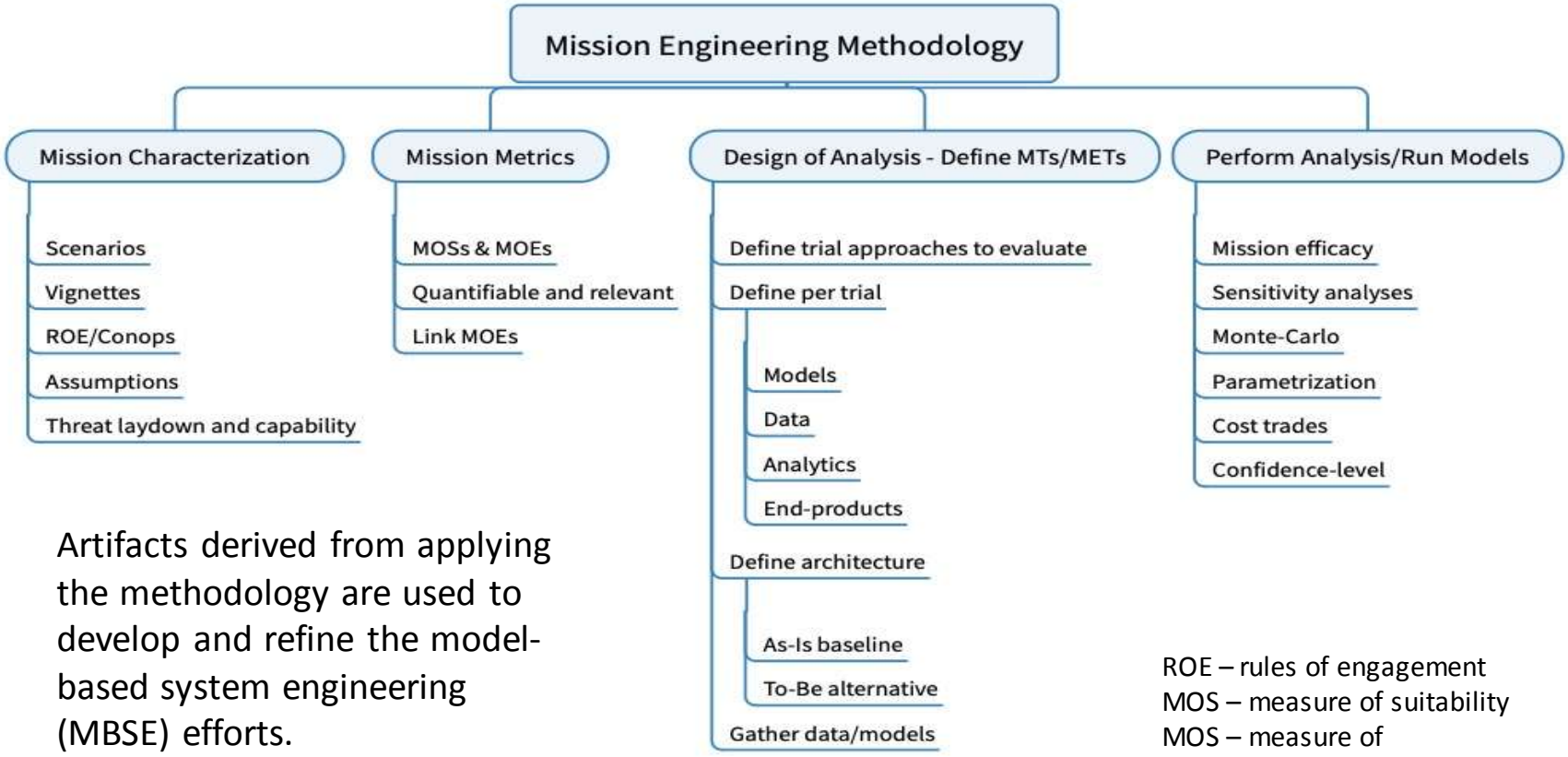
DoD Zero Trust Strategy



Plan

1. Inventories
2. System Security Engineering
3. Acquisition

Developing a Contextual Understanding

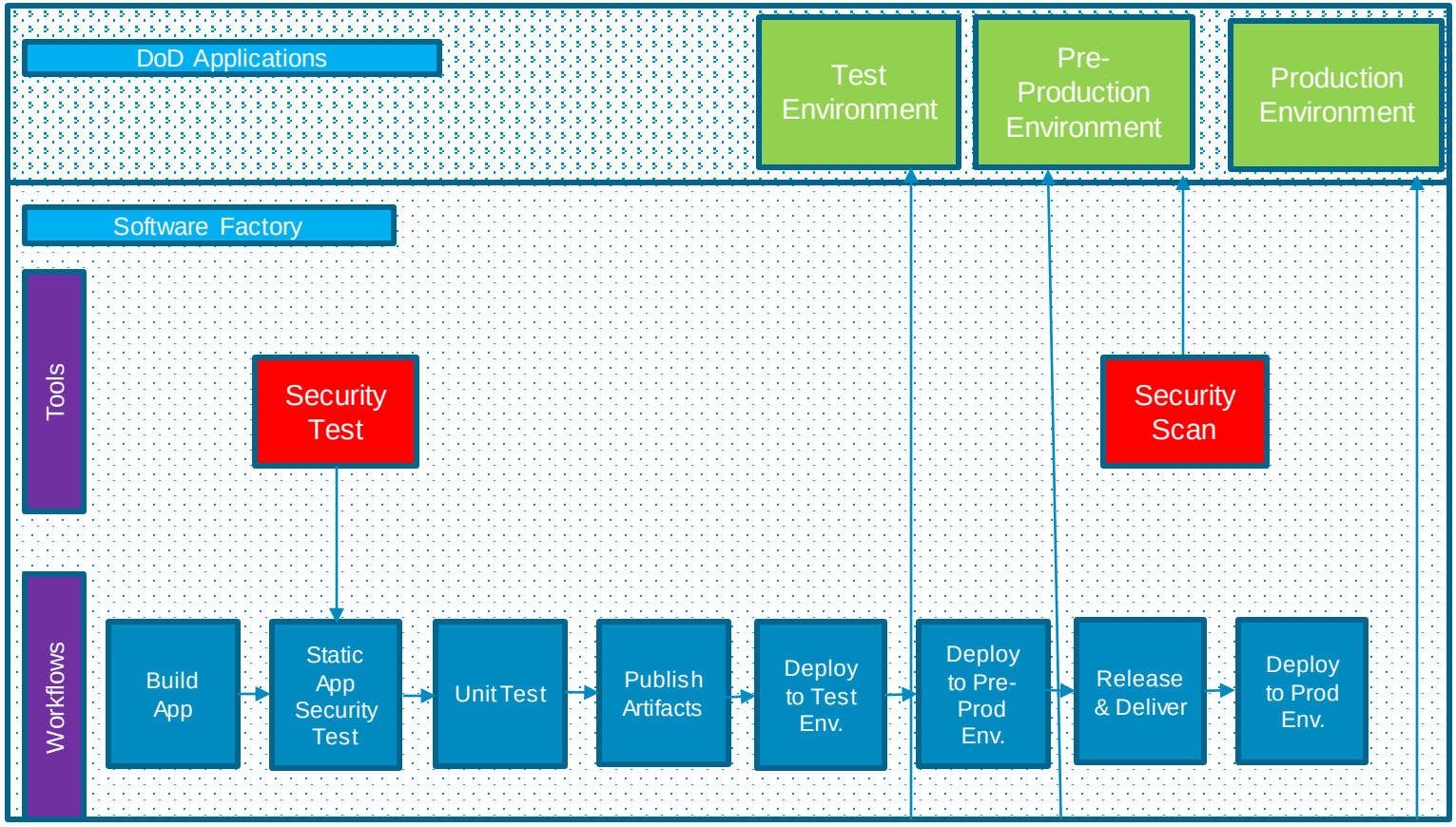


Artifacts derived from applying the methodology are used to develop and refine the model-based system engineering (MBSE) efforts.

[MEG]

ROE – rules of engagement
MOS – measure of suitability
MOS – measure of effectiveness

Software Factory



[DoD 2019]

NIST SP 800-160v1r1 Engineering Trustworthy Secure Systems

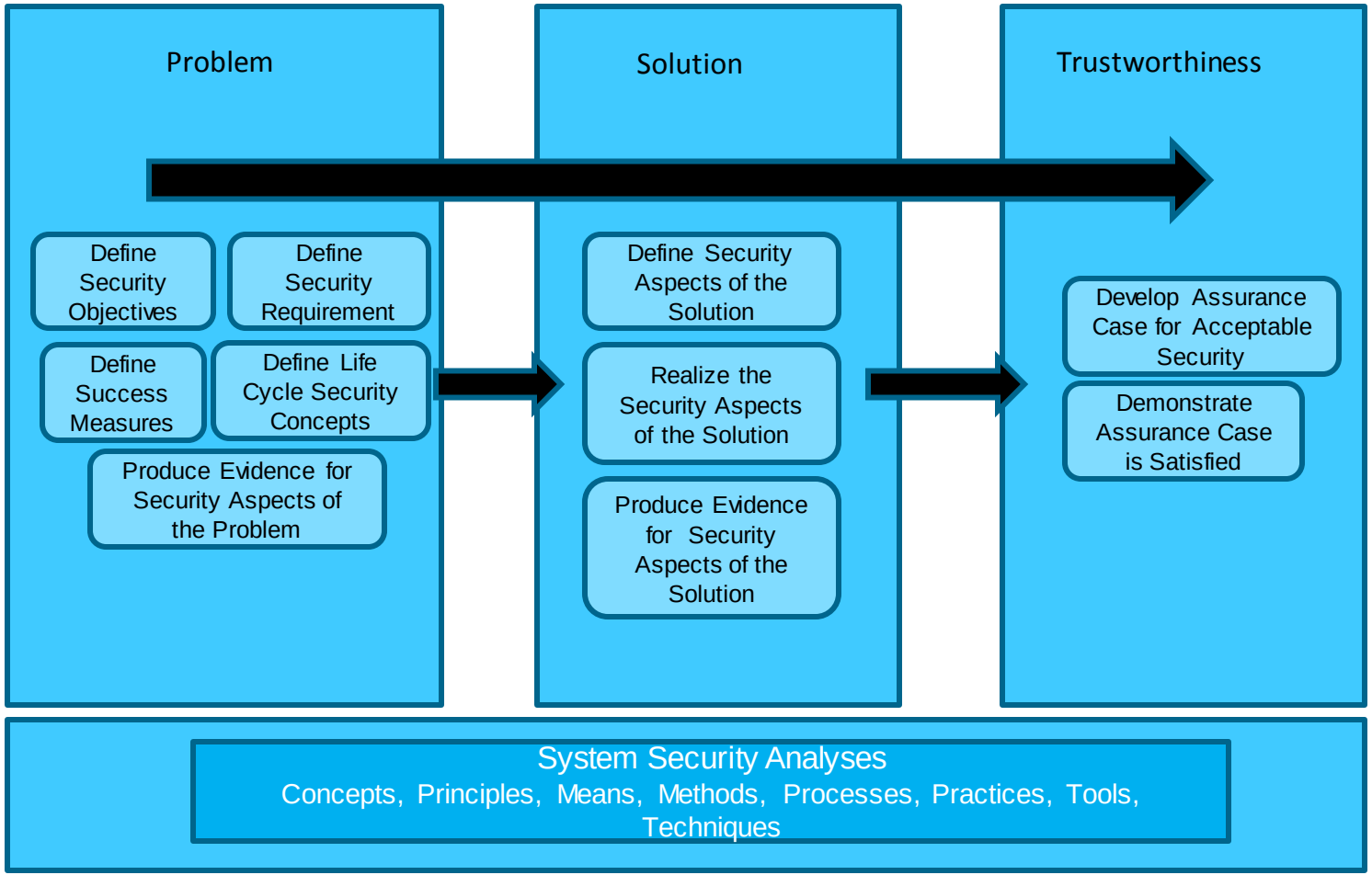


Figure 10

What is the Acquisition Security Framework (ASF)?

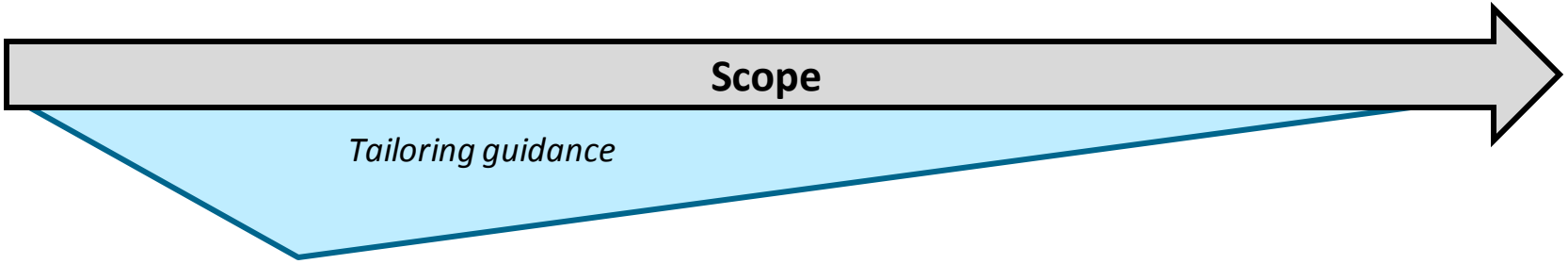
Carnegie Mellon University Software Engineering Institute

The ASF is a collection of leading practices for building and operating secure and resilient software-reliant systems.

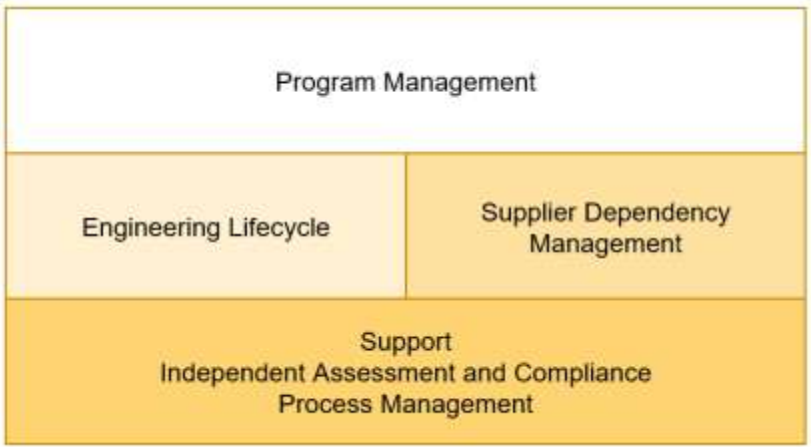
The ASF is designed to proactively enable system security and resilience engineering across the lifecycle and supply chain.

- Provides a roadmap for building security and resilience into a system rather than "bolting it on" after deployment
- Facilitates efficient and predictable systems environments and more manageable delivery and risk outcomes

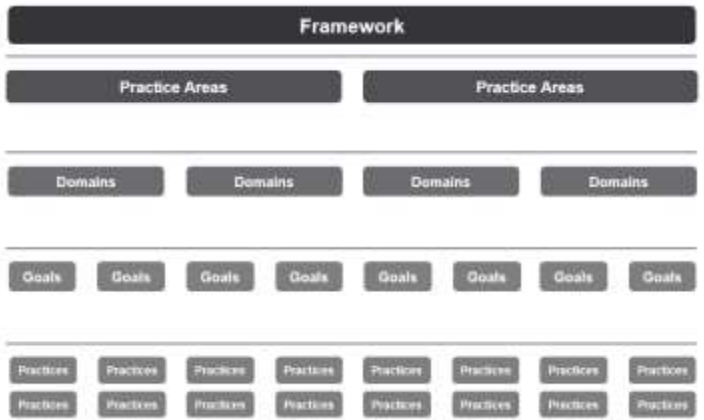
Creating Tailored Risk Frameworks



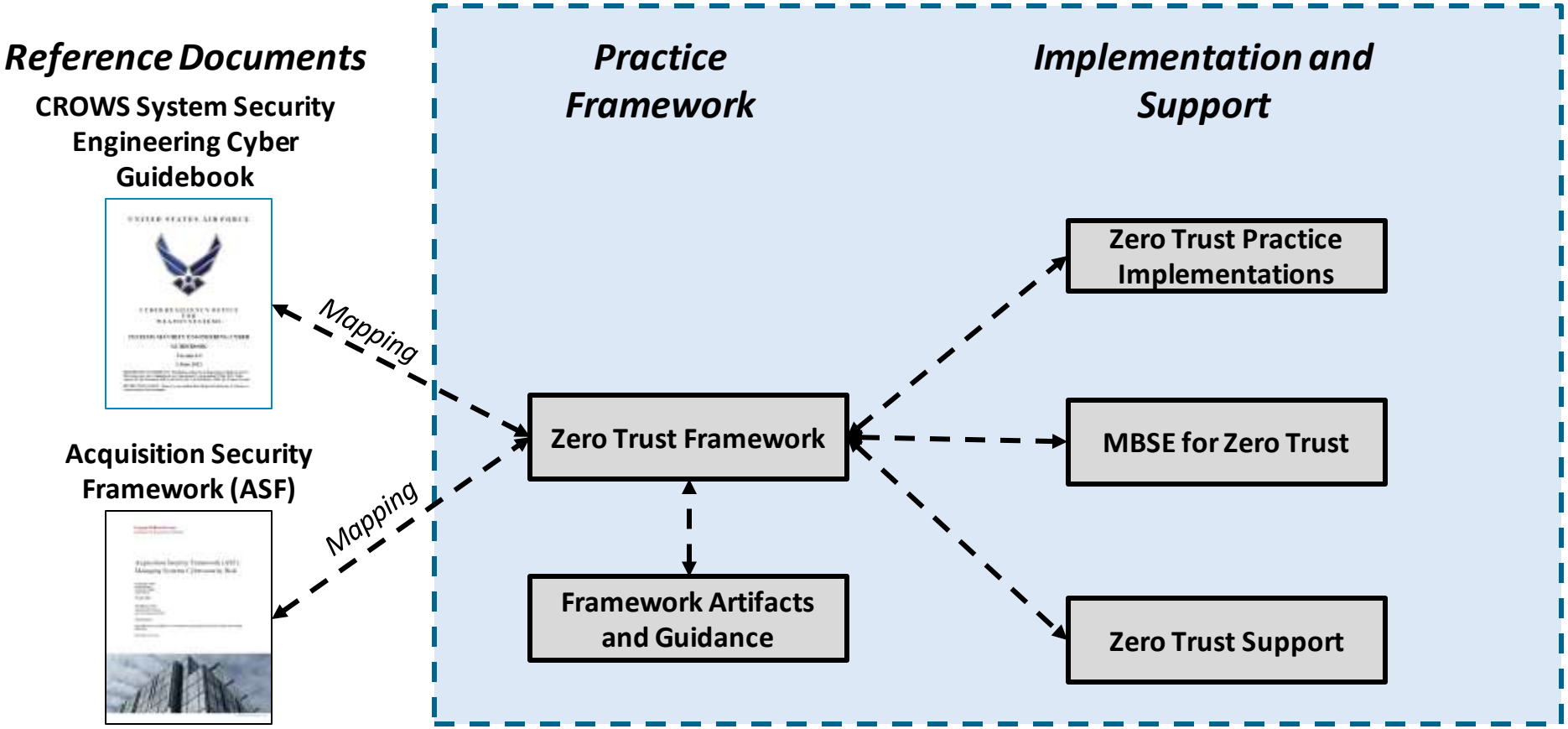
ASF Principles and Concepts



Tailored Framework



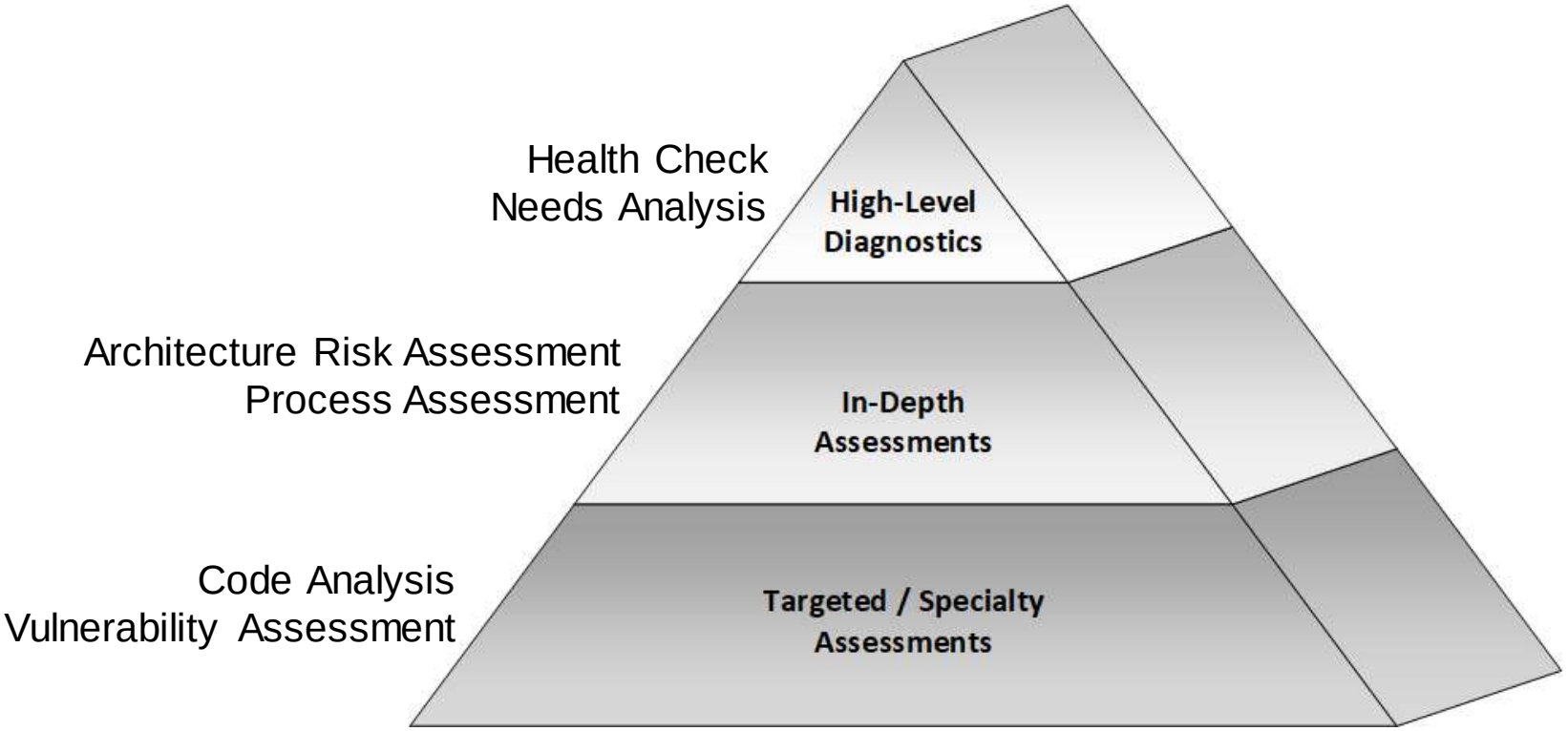
Notional ZT Framework Application



Assess

1. Zero trust assessments
2. Risk management

Types of Assessments and Analysis

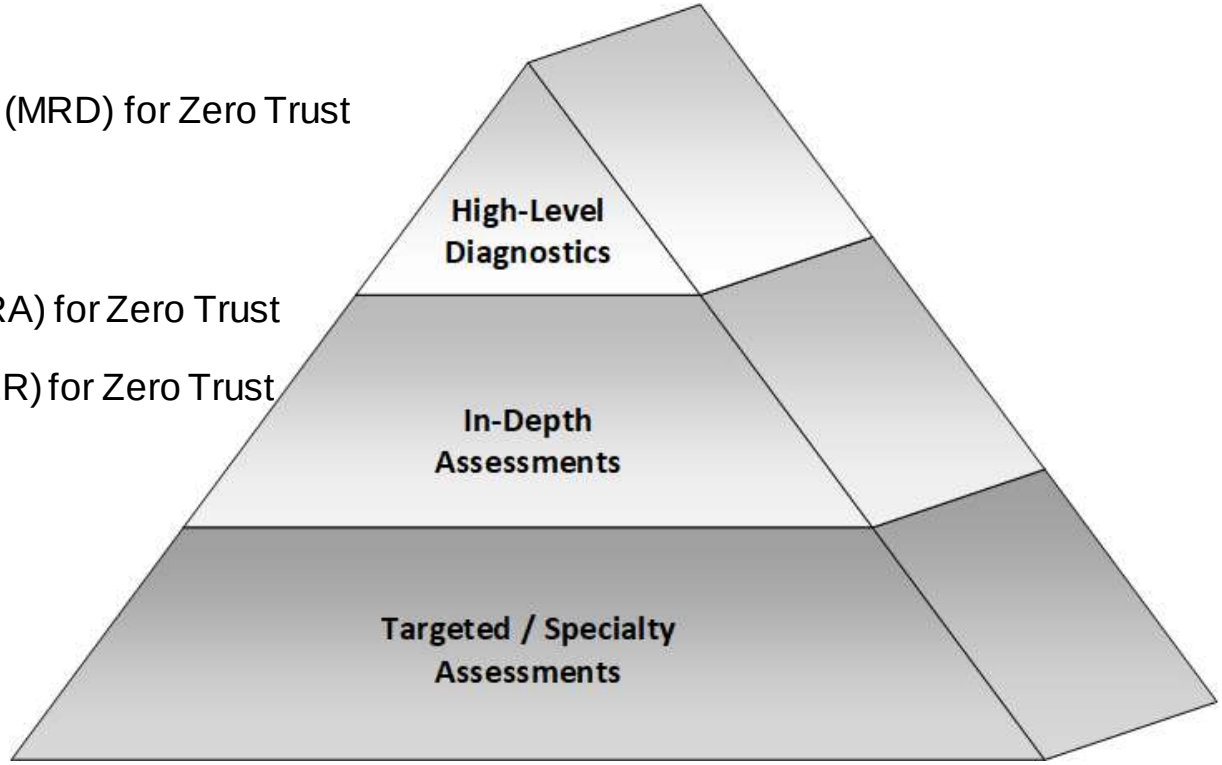


Proposed Zero Trust Assessments

Mission Risk Diagnostic (MRD) for Zero Trust

Security Engineering Risk Analysis (SERA) for Zero Trust

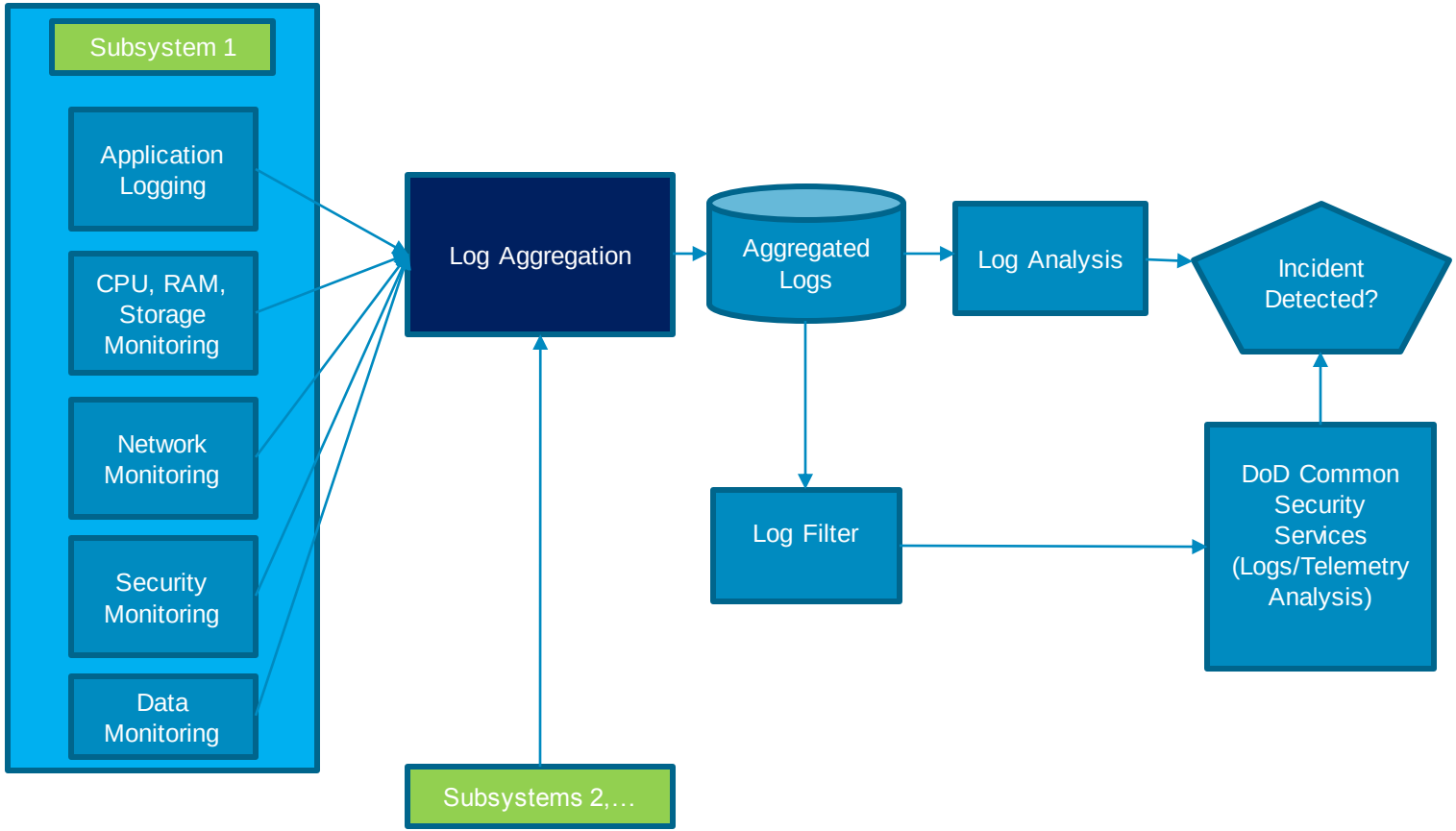
Cybersecurity Engineering Review (CSER) for Zero Trust



Implement

1. Policies
2. Operate

Logging and Log Analysis Process



What Was Missed or Needs Beefed Up in SEI ZT Journey?

Carnegie Mellon University Software Engineering Institute

1. API inventory
2. Developing contextual awareness
3. Visibility of data to support continuous monitoring and logging
4. Focus on automation activities
5. Identification of competencies to enable/support zero trust implementation
6. Goals for policy decision point analytics for organizations

Additional Information

Department of Defense References

[DoD 2019]
Department of Defense (DoD). *DoD Enterprise DevSecOps Reference Design, Version 1.0*. August 2019.
https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf

[MEG]

DoD. *Mission Engineering Guide*, November 2020.

https://ac.cto.mil/wp-content/uploads/2020/12/MEG-v40_20201130_shm.pdf

ASF Information

Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=889215

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

Acquisition Security Framework (ASF)

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=889453

Addressing Supply Chain Risk and Resilience for Software-Reliant Systems

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=974293

Asking the Right Questions to Coordinate Security in the Supply Chain

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=974136

ASF Engineering Lifecycle: Domains and Goals

Domain	Goal Name
Domain 1—Engineering Infrastructure	Infrastructure Development
	Infrastructure Operation
Domain 2—Engineering Management	Technical Activity Management
	Product Risk Management
Domain 3—Engineering Activities	Requirements
	Architecture
	Third-Party Components
	Implementation
	Test and Evaluation
	Transition Artifacts
	Deployment
	Secure Product Operation

Our initial development is focused on Engineering Activities (Domain 3).

Mission Risk Diagnostic (MRD)

What

- An approach for assessing mission risk in interactively complex, socio-technical systems (e.g., acquisition programs, development projects, enterprise initiatives, organizational capabilities)

Why

- Assess a mission's current potential for success in relation to a set of known risk factors
- Develop a plan for managing risk and increasing the potential for mission success

Benefits

- Provides a time-efficient means of assessing acquisition programs, development projects, initiatives, and capabilities
- Establishes confidence in the ability to achieve mission objectives
- Can be self-applied or expert led

Security Engineering Risk Analysis (SERA)

Carnegie Mellon University Software Engineering Institute

What

- A systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain

Why

- Build security into software-reliant systems by addressing design weaknesses as early as possible (e.g., requirements, architecture, design)
- Assemble a shared organizational view (business and technical) of cybersecurity risk

Benefits

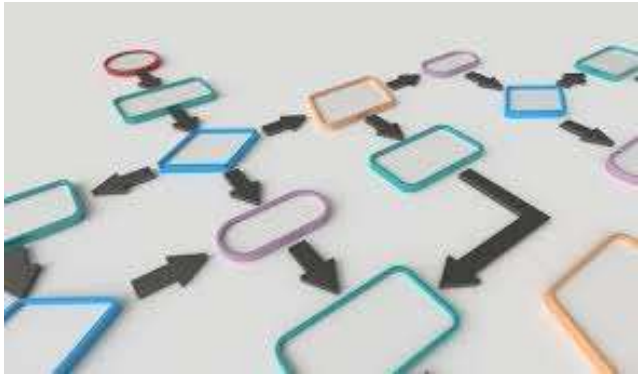
- Correct design weaknesses before a system is deployed
- Reduce residual cybersecurity risk in deployed systems
- Ensure consistency with NIST Risk Management Framework (RMF)

Cybersecurity Engineering Review (CSER)

Carnegie Mellon University Software Engineering Institute

What

- Evaluates an acquisition program's security practices for conformance to accepted CSE practices



Why

- Understand the effectiveness of an acquisition program's cybersecurity practices
- Develop a plan for improving a program's cybersecurity practices

Benefits

- Establish confidence in a program's ability to acquire software-reliant systems across the lifecycle and supply chain
- Reduce cybersecurity risk of deployed software-reliant systems

Assessment Information

Mission Risk Diagnostic (MRD) Method Description

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=10075

Security Engineering Risk Analysis (SERA) Collection

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485410