Carnegie Mellon University
Software Engineering Institute

APRIL 04, 2023

Tim Morrow
CMU/SEI CERT Situational Awareness Technical Manager

Document Markings

Examples of Zero Trust Implementation

Carnegie Mellon University Software Engineering Institute

NIST 1800-35B Implementing a Zero Trust Architecture Volume B: Approach, Architecture, and Security Characteristics

- Initial focus on implementing a ZTA for a conventional, general-purpose enterprise information technology (IT) infrastructure that combines users, devices, and enterprise resources.

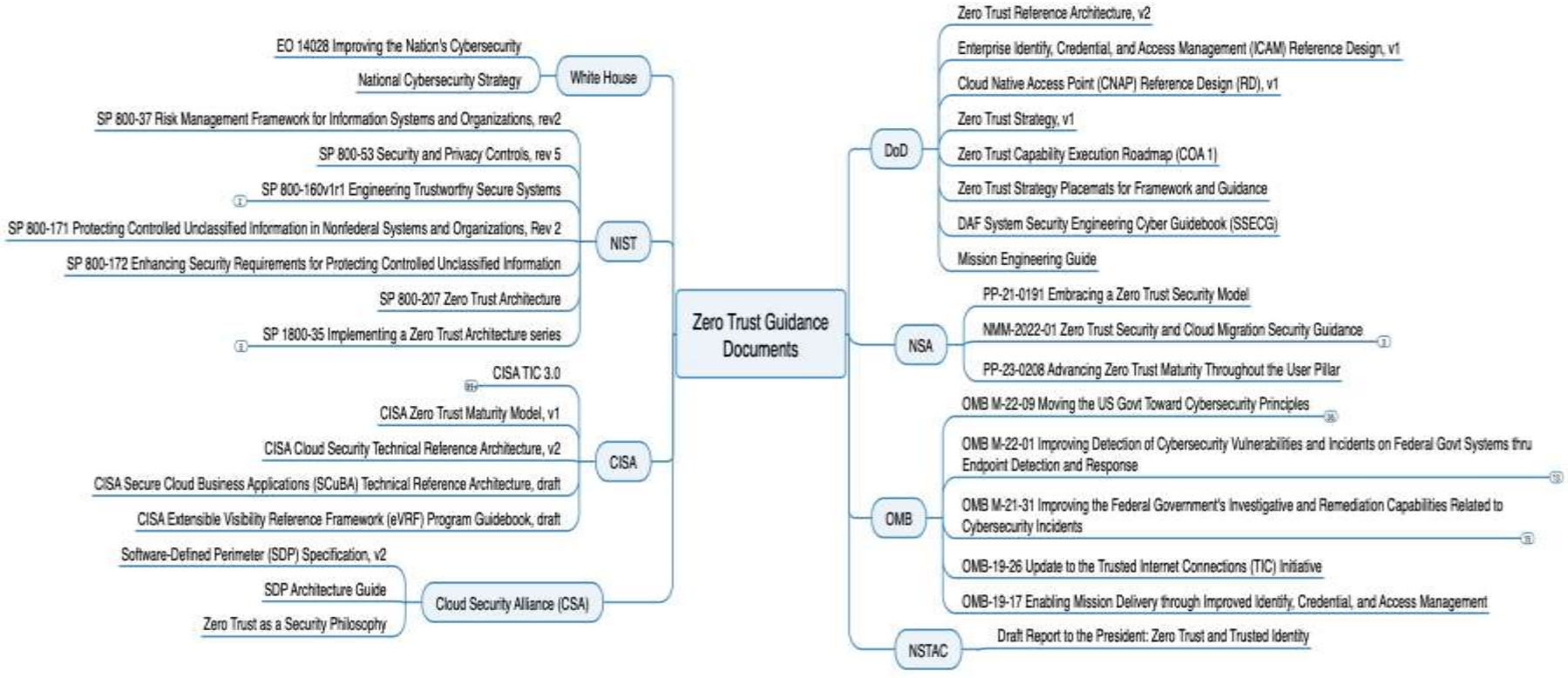
6 use cases with 29 scenarios

Department of the Army 2ID C/G6 Zero Trust Implementation Guide

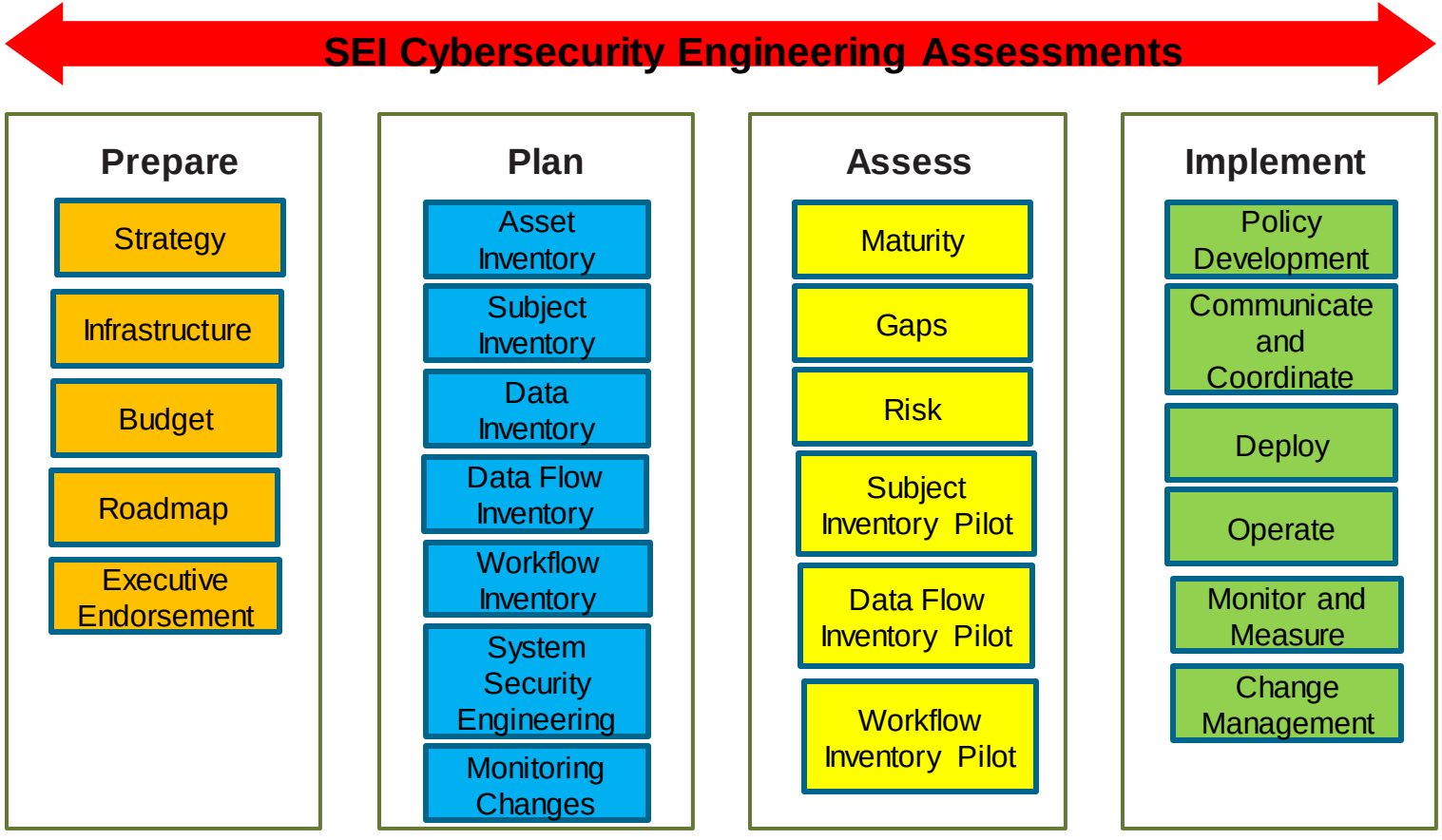
- Step 1 Initial Design and Collection of Data
  - Identify the Protection Surface
  - Map Network and Data Flows
  - Build the Zero Trust Architecture
- Step 2 Zero Trust Policies in Detection Mode
- Step 3 Zero Trust Policies in Prevention Mode

15 use cases

Guidance Documents When Considering a Zero Trust Implementation



Software Engineering Institute (SEI) Zero Trust Journey



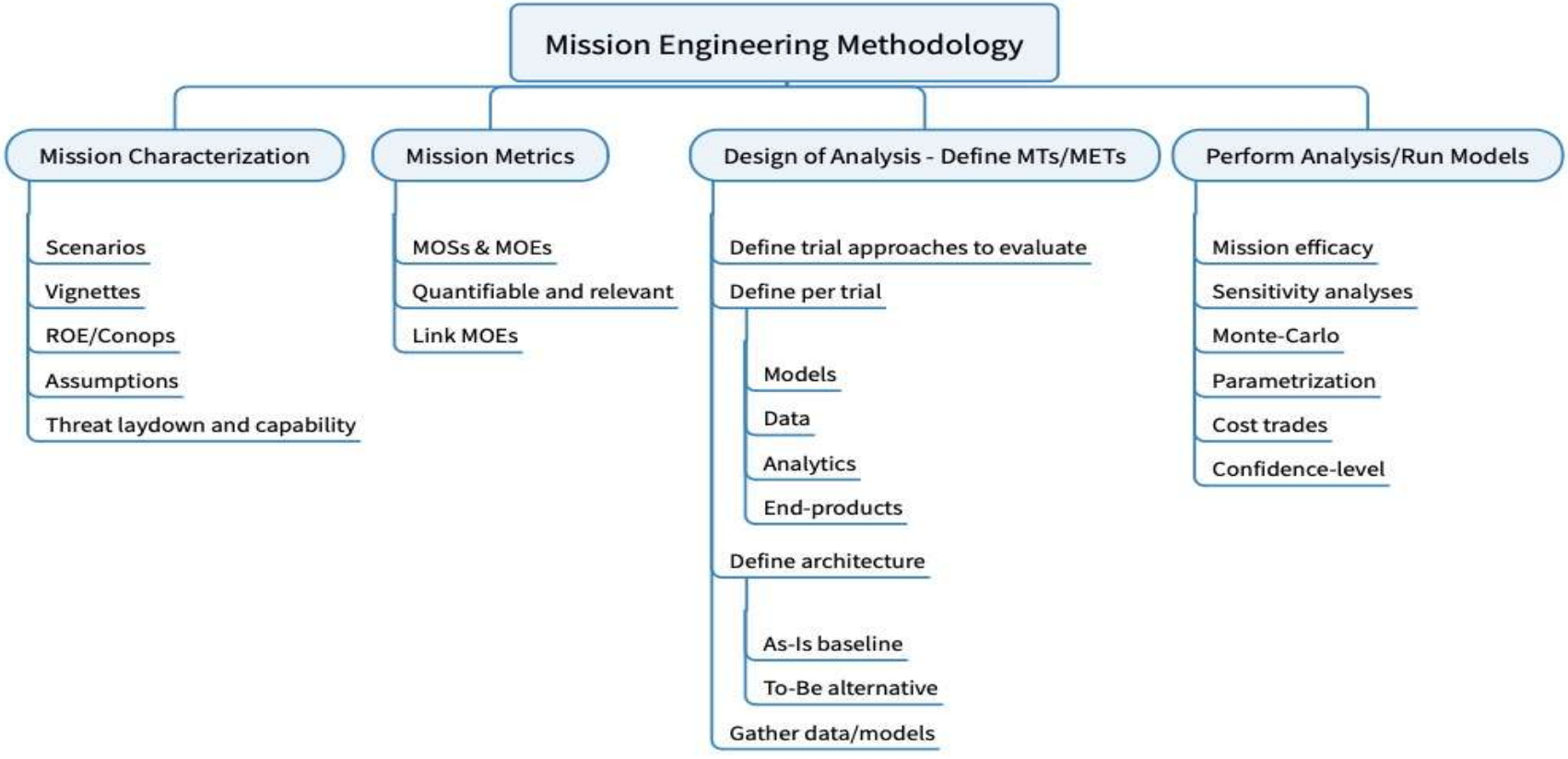
What's Mission Engineering and it's Objectives?

Mission Engineering (ME) is the planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects.

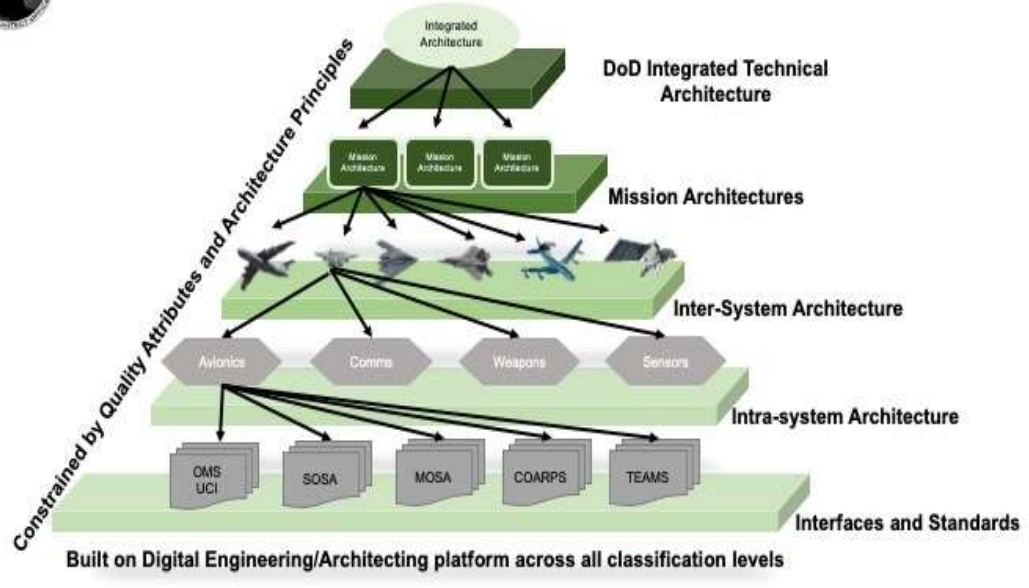
Five Objectives

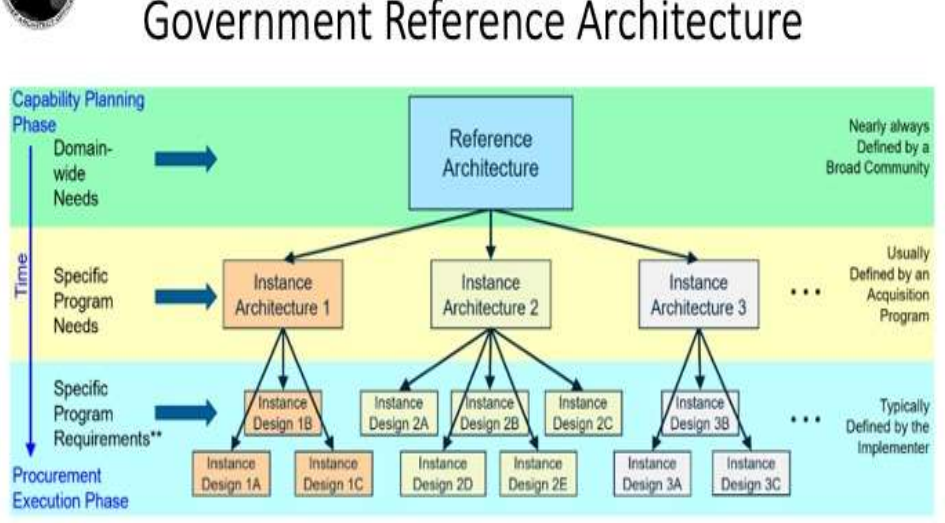
1. Enable mission-focused, threat-informed analysis.
2. Identify and address mission gaps.
3. Develop Government Reference Architectures (GRA) to guide development and prototypes.
4. Inform stakeholders how the architecture is envisioned to address/support the missions.
5. Generate and capture scenarios, assumptions, constraints, system attributes, and data for use during analysis.

Focused View of ME Methodology



Architecture

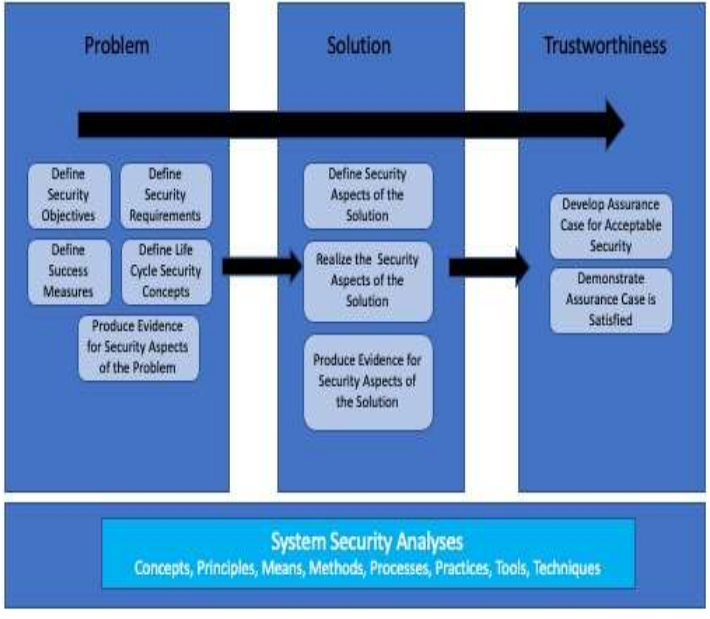




Security Engineering & Cyber Survivability Attributes

Carnegie Mellon University Software Engineering Institute

NIST SP 800-160v1r1 Figure 10

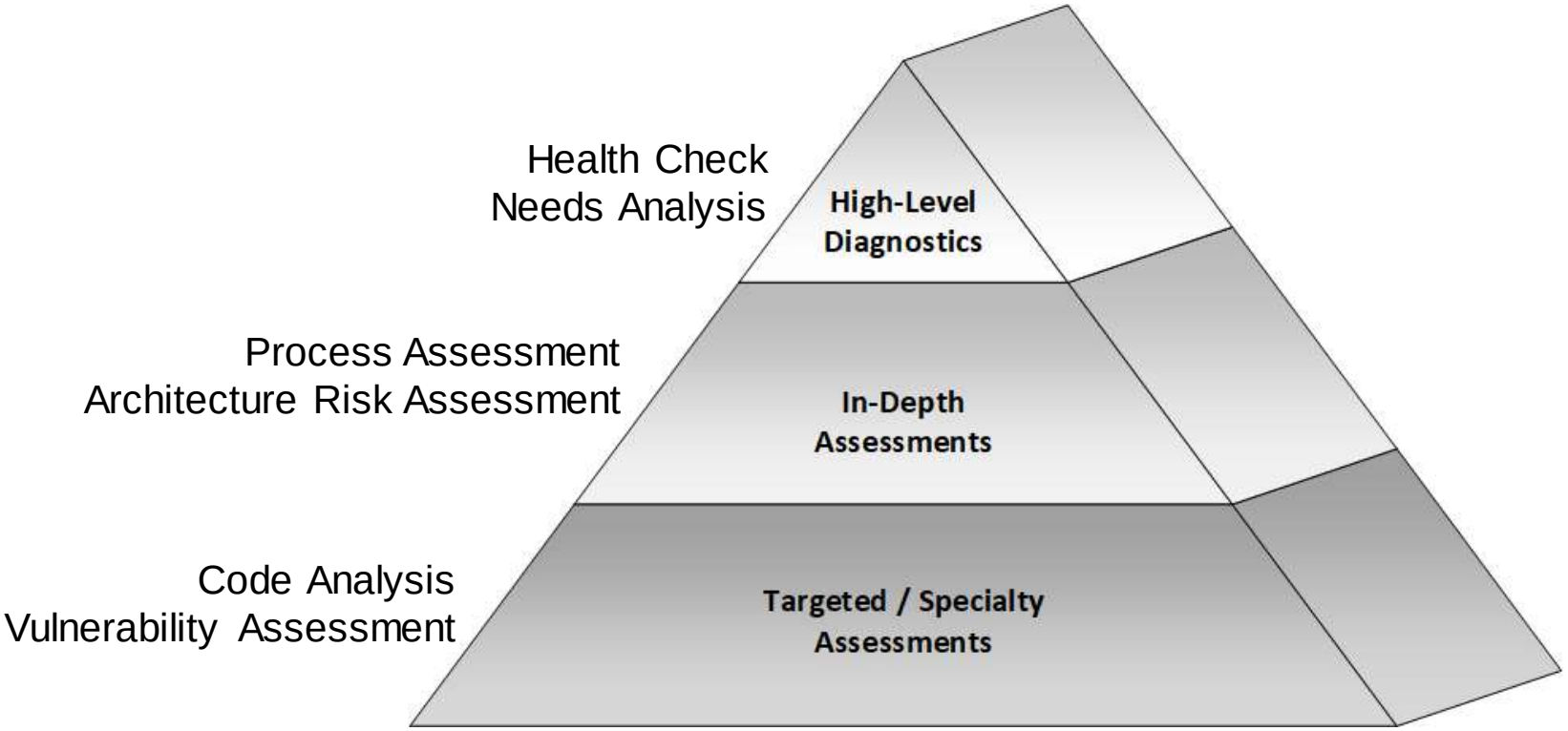


DAF System Security Engineering Cyber Guidebook (SSECG) - Cyber Survivability Attributes

System Survivability Key Performance Parameter

CSA	Pillar	Cyber Survivability Attribute (CSA)
CSA-01	Prevent	Control Access
CSA-02	Prevent	Reduce System's Cyber Detectability
CSA-03	Prevent	Secure Transmissions and Communications
CSA-04	Prevent	Protect System's Information from Exploitation
CSA-05	Prevent	Partition and Ensure Critical Functions at Mission Completion Performance Levels
CSA-06	Prevent	Minimize and Harden Cyber Attack Surfaces
CSA-07	Mitigate	Baseline & Monitor Systems, & Detect Anomalies
CSA-08	Mitigate	Manage System Performance if Degraded by Cyber Events
CSA-09	Recover	Recover System Capabilities; Actively manage System's Configuration to Counter Vulnerabilities at Tactically Relevant Speeds
CSA-10	Adapt	Achieve & Manage System's an operationally relevant Cyber Survivability Risk Posture (CSRP) and to counter risk changes in adversary's capabilities

Types of Assessments and Analysis

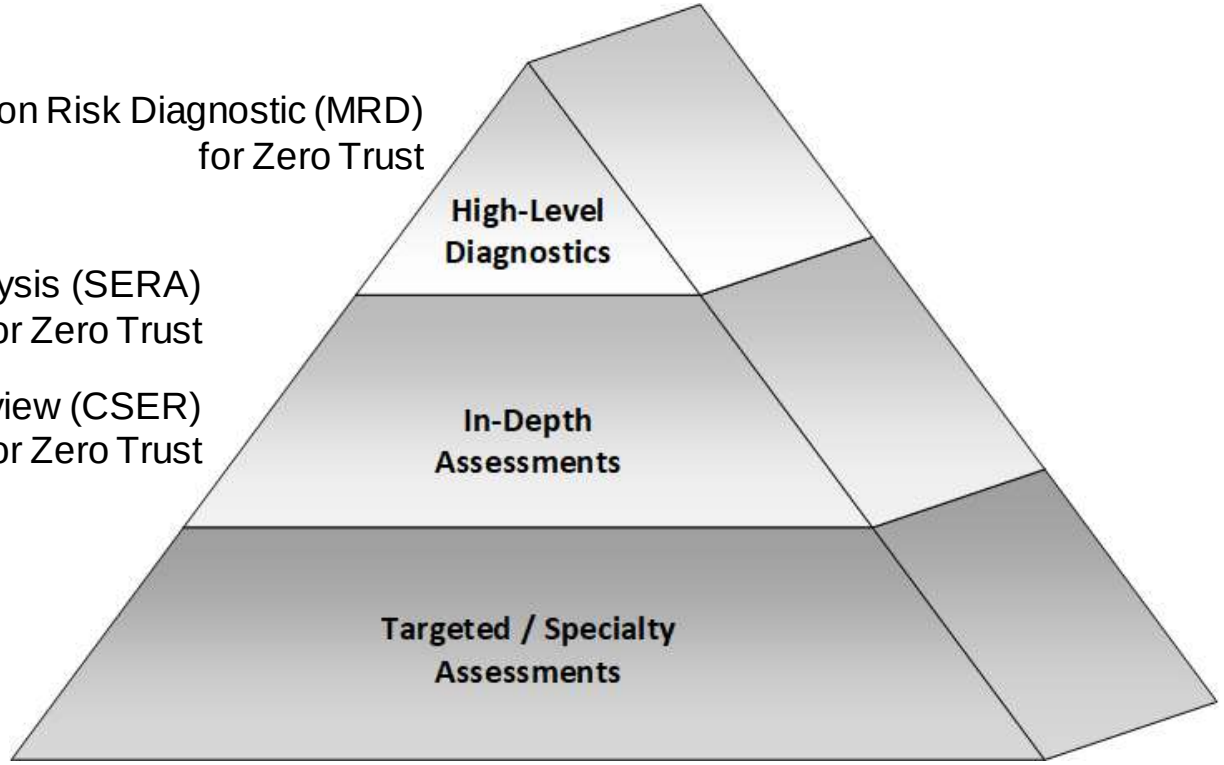


Proposed SA Zero Trust Assessments

Mission Risk Diagnostic (MRD) for Zero Trust

Security Engineering Risk Analysis (SERA) for Zero Trust

Cybersecurity Engineering Review (CSER) for Zero Trust



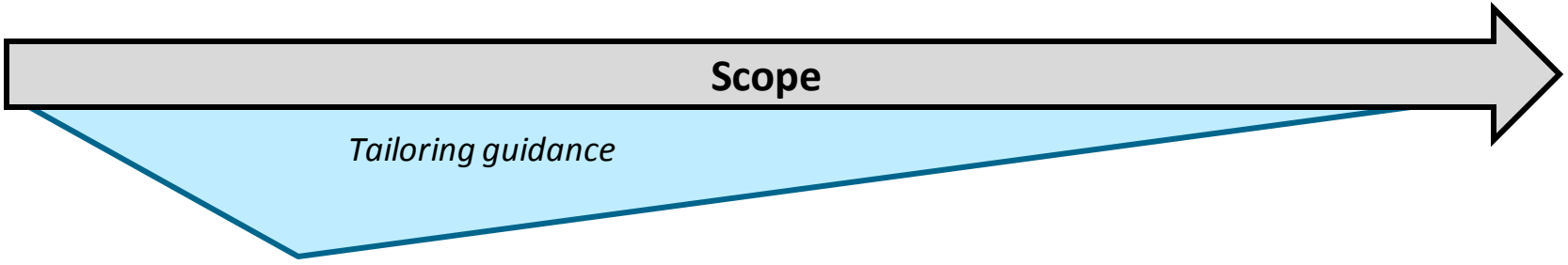
What is the Acquisition Security Framework (ASF)?

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

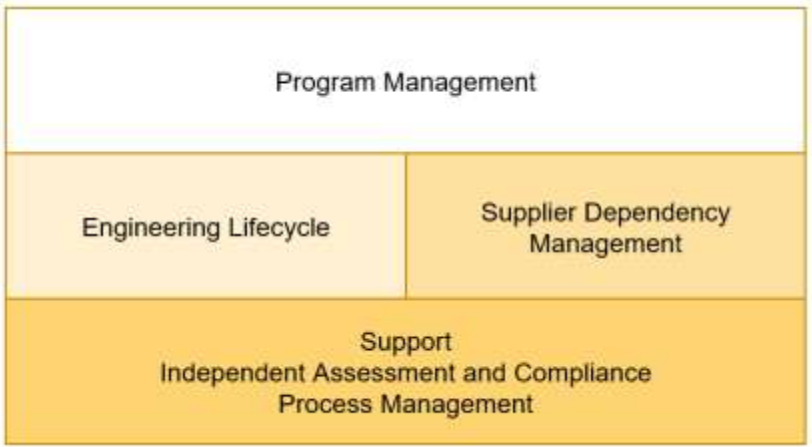
The ASF is designed to proactively enable system security and resilience engineering across the lifecycle and supply chain.

- 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

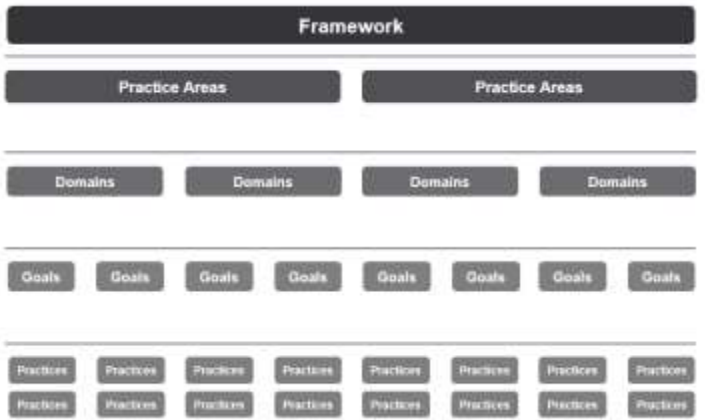
Creating Tailored Risk Frameworks



ASF Principles and Concepts



Tailored Framework



Envisioned Zero Trust Framework: Guidance

Carnegie Mellon University Software Engineering Institute

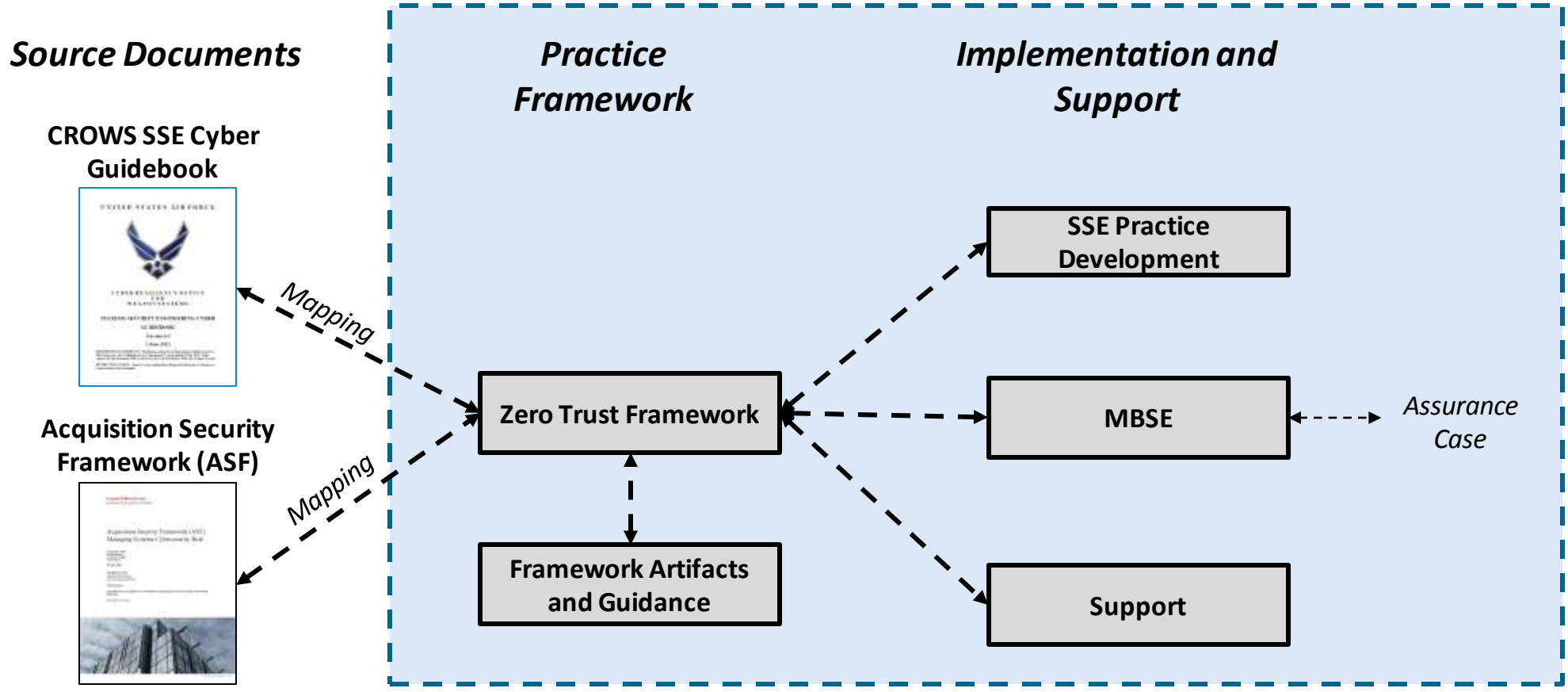
Goal-Level Guidance

- Context
- Competencies
- SSECG WBS mapping
- Additional SSECG References
- Notes

Practice-Level Guidance

- Question Intent
- Typical Work Products
- Criteria for “Yes” Response
- Criteria for “Incomplete” Response

Notational ZT Framework Application



Summary

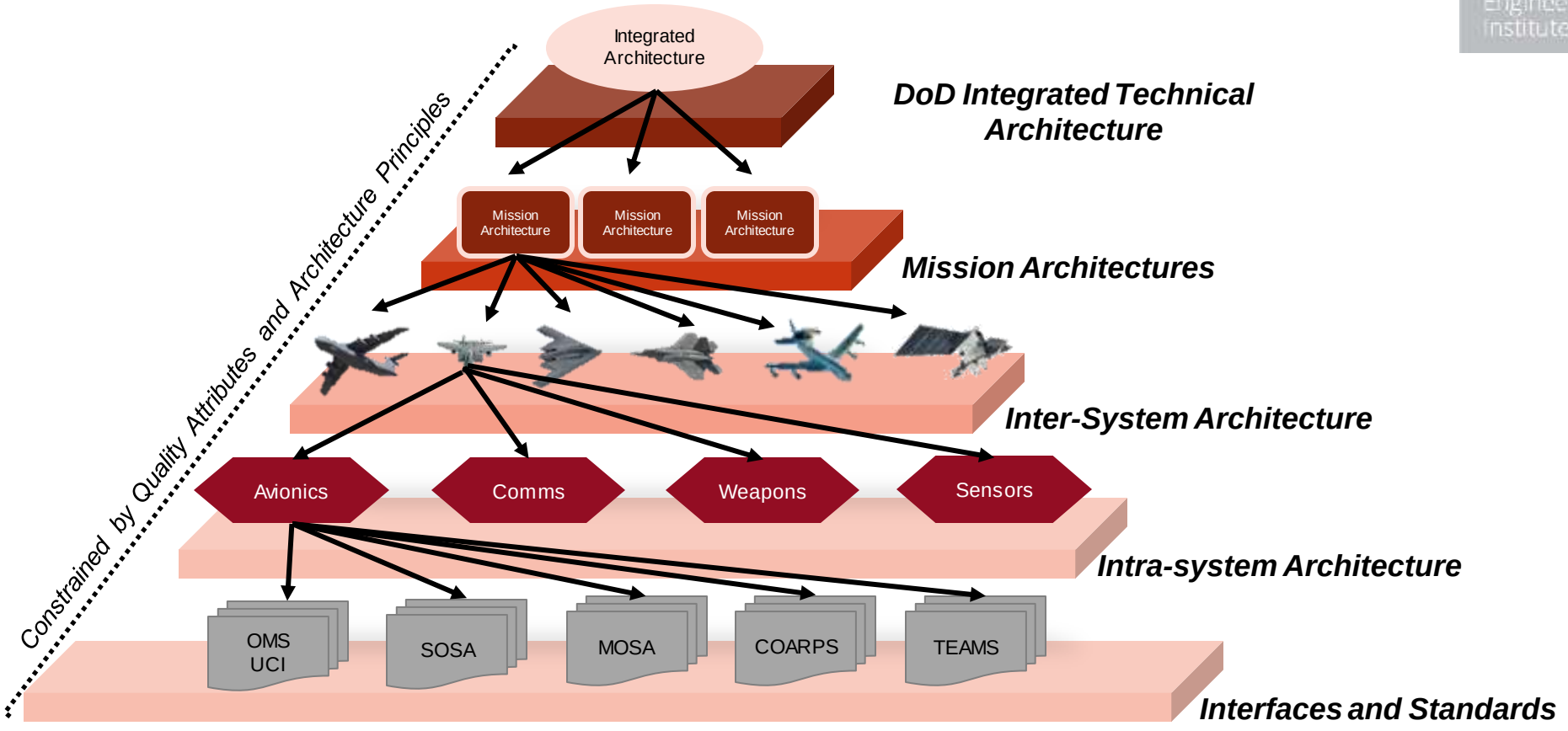
Developing context using mission engineering approach enables security architectures to reason about zero trust strategy, design, and possible implementations for weapon systems, as well as enterprises.

Set of zero trust assessments need to be developed to support the life cycle of weapon system/enterprise.

Need to use an approach like ASF to build in security and resilience into weapon systems/enterprise in support of efforts like CROWS SSECG to provide the artifacts to enable zero trust assessments

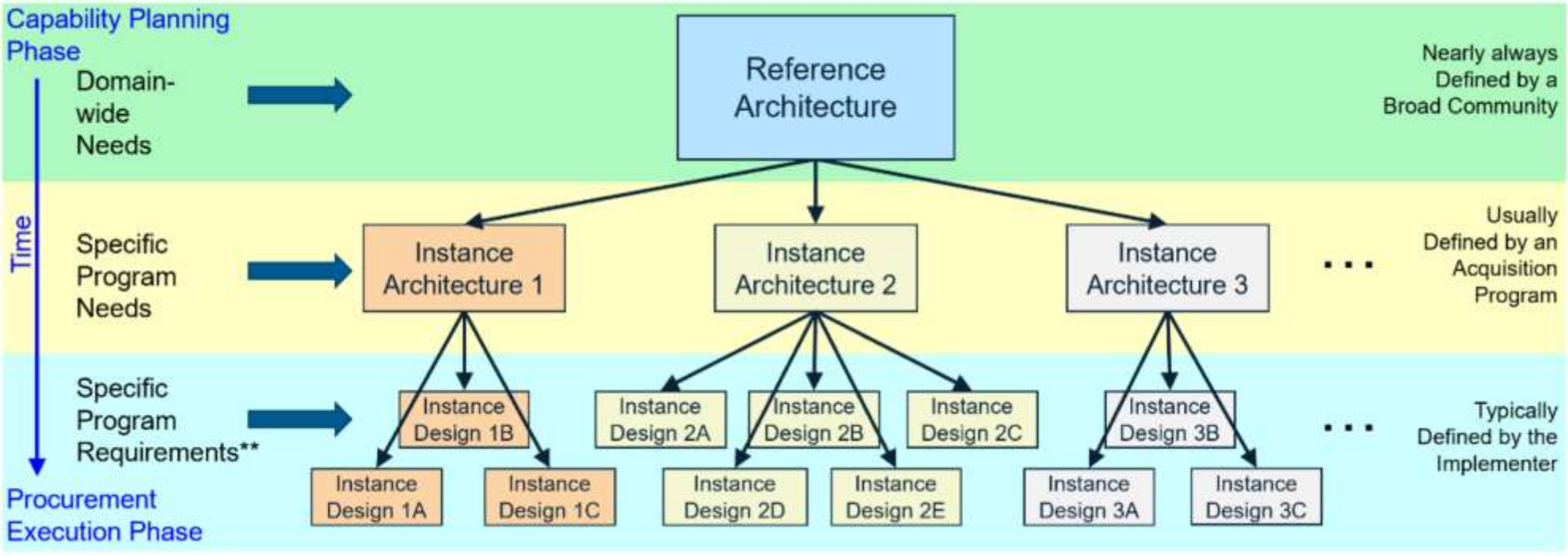
Backup

DoD Architecture Layers



Built on Digital Engineering/Architecting platform across all classification levels

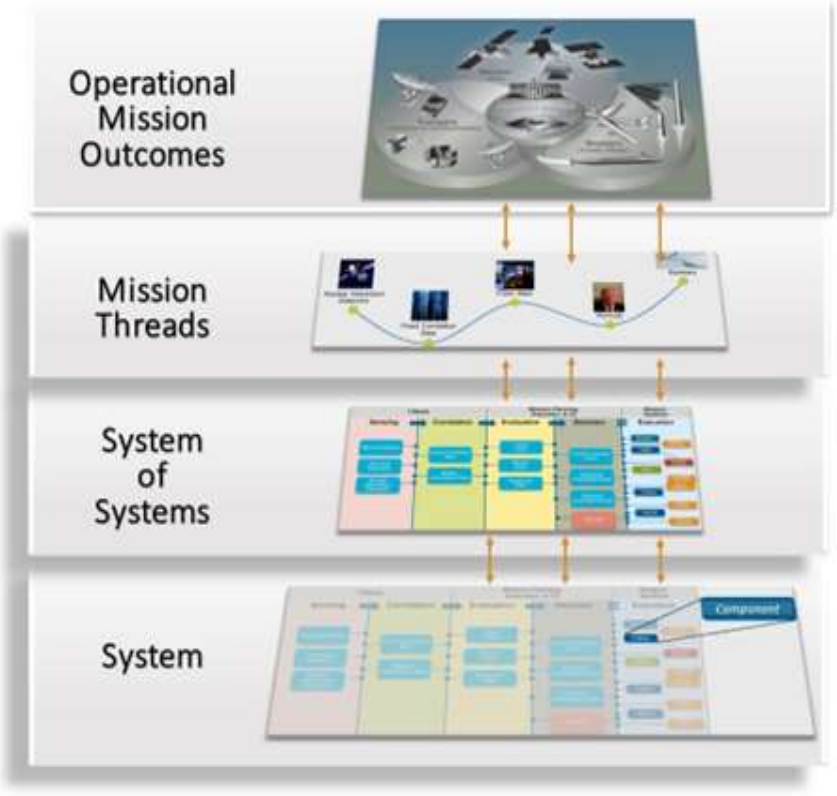
Government Reference Architecture



[Mark Daniels's diagram]

JFHQ-DODIN Mission Threads

1. Perform DODIN Cyber Analysis
   - Execute the threat analysis, terrain analysis, mission analysis, event analysis, mitigation analysis, risk analysis, and tasking stages.
2. Perform DODIN Checkout
   - Execute a checkout of DODIN and its interfaces to AOs, …
3. Add a new DODIN Capability
   - Define the steps used to add a new capability to DODIN.

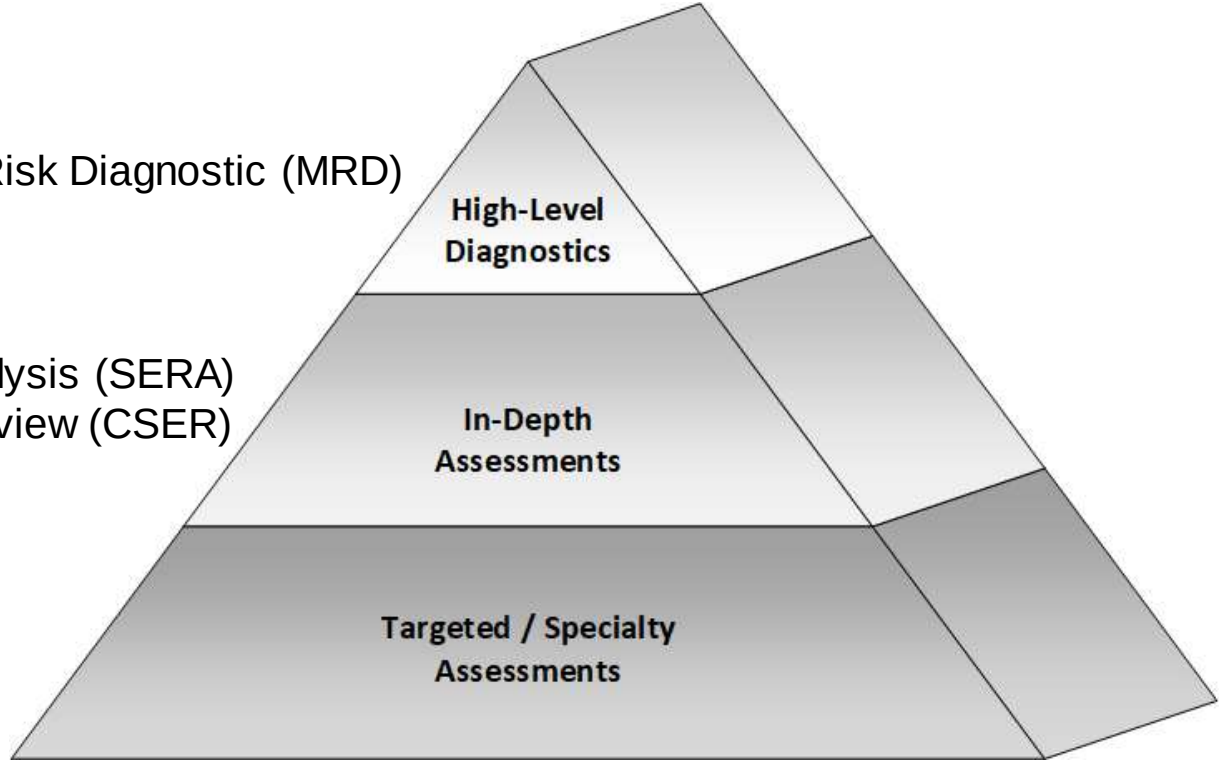


Note: The threats to JFHQ-DODIN will constantly change, therefore the GMRA must be able to be updated based on the scenarios and evolving threat.

SA Cybersecurity Engineering (CSE) Assessments

Mission Risk Diagnostic (MRD)

Security Engineering Risk Analysis (SERA)
Cybersecurity Engineering Review (CSER)



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

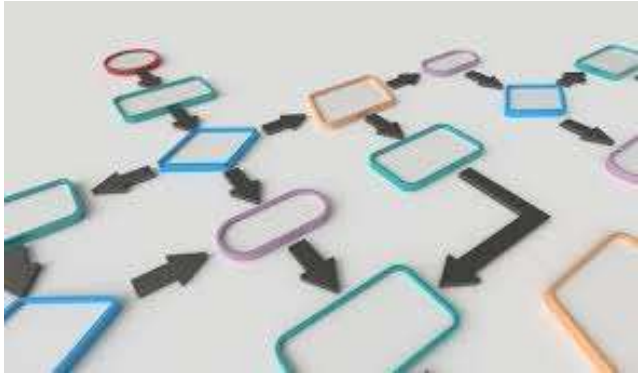
- Correct design weaknesses before a system is deployed
- Reduce residual cybersecurity risk in deployed systems
- Ensure consistency with NIST Risk Management Framework (RMF)

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

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).