Cybersecurity Engineering (CSE): *Situational Awareness Assessments*

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

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.

DM20-1055

Topics

Introduction

Mission Risk Diagnostic (MRD)

Security Engineering Risk Analysis (SERA)

Cybersecurity Engineering Review (CSER)

Summary

CSE: SA Assessments

Introduction

Systems Security Engineering (SSE)

"An element of Systems Engineering (SE) that applies scientific and engineering principles in a standardized, repeatable, and efficient manner to identify security vulnerabilities, requirements, and methods of verifications that minimize risks."[1]

- SSE processes are used to design systems that are resilient to cyber-attacks.
- SSE delivers systems that satisfy stakeholder security needs for weapon system operation in today's cyber-contested environments.

1. United States Air Force Weapon System Program Protection / Systems Security Engineering Guidebook, Version 2.0

USAF Program Protection (PP) and Systems Security Engineering (SSE) Guidebook

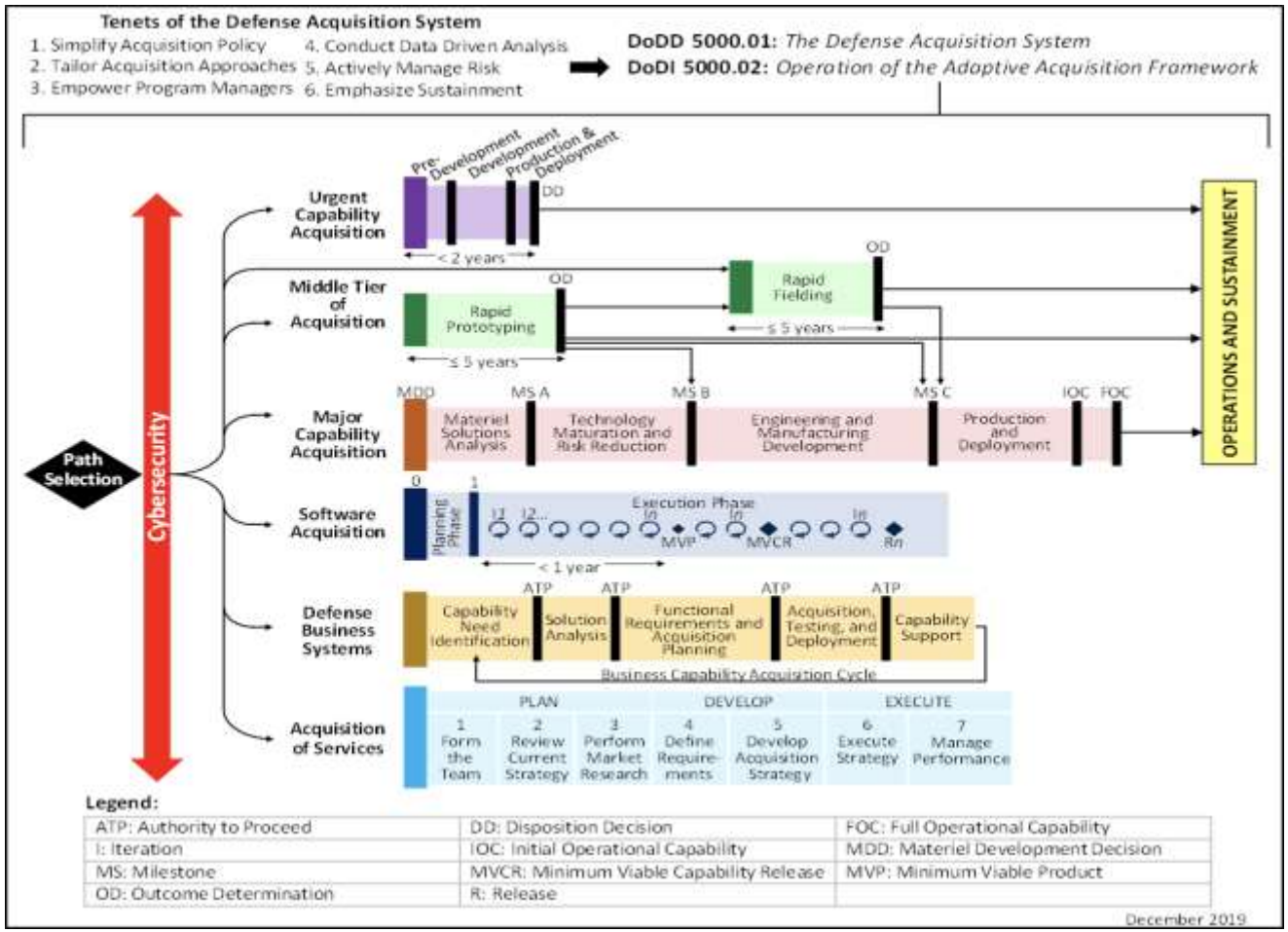
The USAF Weapon System PP/SSE Guidebook defines an integrating process for implementing security countermeasures in weapon systems:

- Anti-counterfeit practices
- Anti-tamper (AT)
- Cybersecurity
- Exportability features
- Hardware assurance (HwA)
- Procurement strategies
- Secure system design
- Security management / information protection (IP)
- Software assurance (SwA)
- Supply chain risk management (SCRM)

Key gap: Software security engineering is not addressed sufficiently in the USAF Weapon System PP/SSE Guidebook.

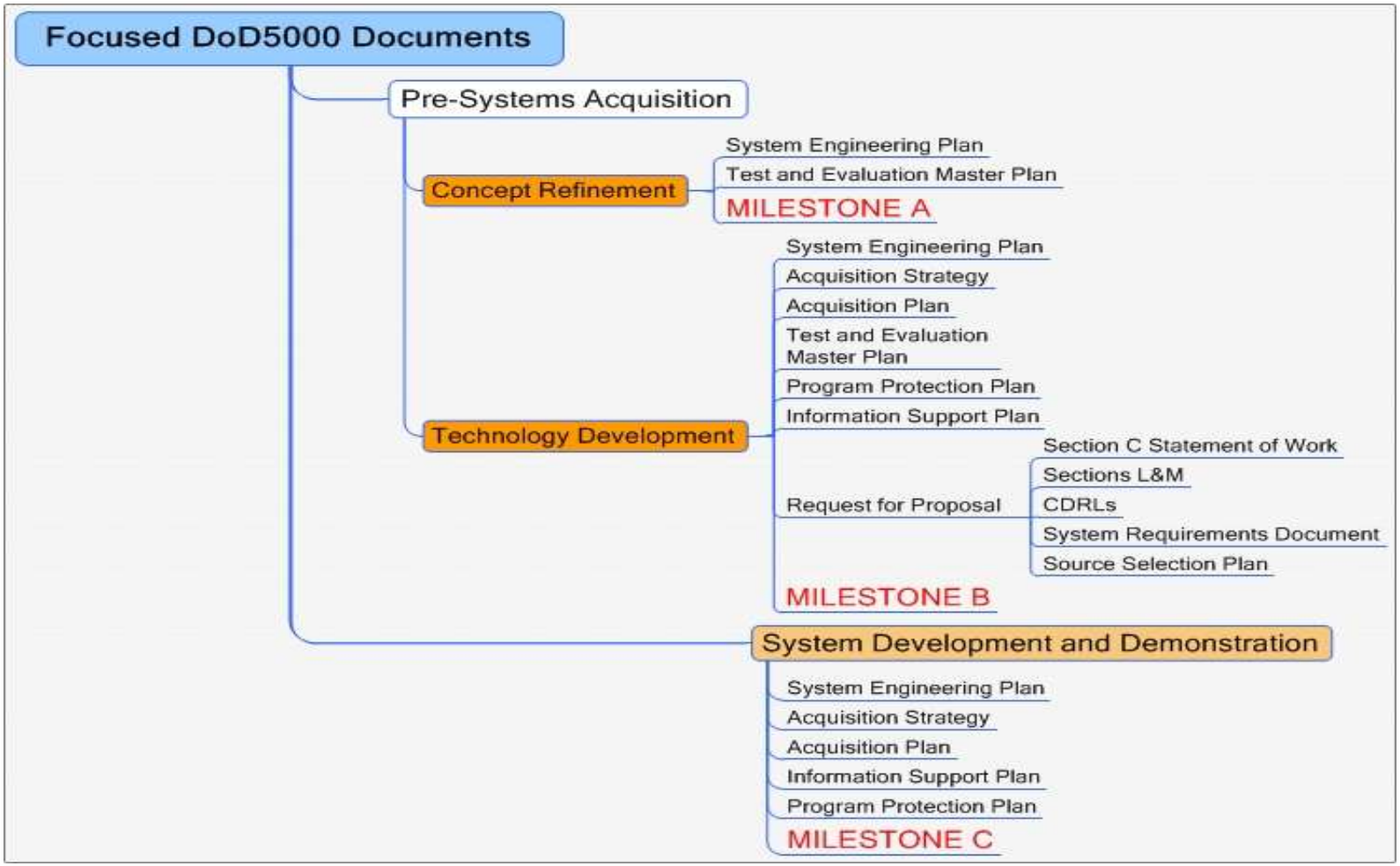
Adaptive Acquisition Framework: *Multiple Acquisition Pathways*

SA cybersecurity assessments can be tailored to multiple types of acquisitions.



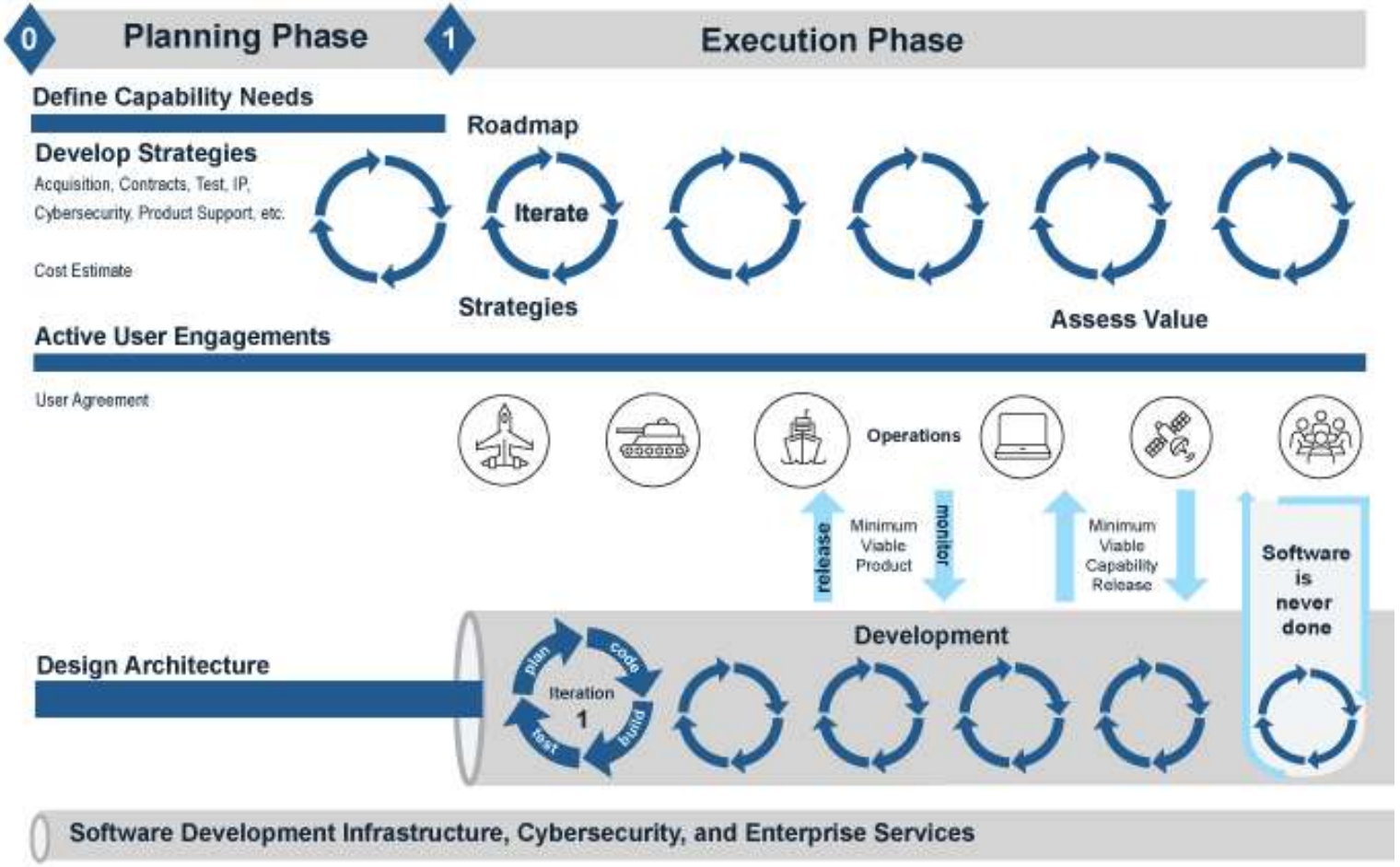
Major Capability Acquisition: *Acquisition Documents*

Acquisition documents provide management data used in SA cybersecurity assessments.



The Software Acquisition Pathway

(DoD Instruction 5000.87 dated 10/2/20)



The Software Acquisition Pathway

(DoD Instruction 5000.87 dated 10/2/20)

Requires govt and contractors sw teams to use modern iterative sw dev methodologies, modern tools and techniques (DevSecOps) and human-centered design practices to iteratively deliver sw to meet the user's priority needs.

Cybersecurity and program protection will be addressed from program inception throughout the program's lifecycle.

A risk-based management approach will be an integral part of the program's strategies, processes, designs, infrastructure, development, test, integration, delivery and operations.

The Software Acquisition Pathway
(DoD Instruction 5000.87 dated 10/2/20)

Planning Phase

Artifacts required to enter Execution Phase

- Capability Needs Statement (CNS), user agreement (UA), acquisition strategy, test strategy, and cost estimate

Focus is on DevSecOps

"Cybersecurity strategies includes recurring assessment of the supply chain, development environment, processes and tools, continuous automated cybersecurity test and operational evaluation to provide a system resilient to Offensive Cyber Operations (OCO)."

Gap – SoS/System context for architecture, non-functional requirements to support analysis, test & evaluation (T&E), and modeling & simulation (M&S) to support risk-based approach.

The Software Acquisition Pathway
(DoD Instruction 5000.87 dated 10/2/20)

Execution Phase

Sw dev team further refines capability and features with the users to decompose capabilities into a prioritized backlog of functional and performance requirements, features, mission threads, and/or user stories, use cases.

Test strategy includes system-level performance requirements, non-functional requirements, and the metrics that will be used too verify that the system will meet user needs.

CNS Table of Contents
(Advanced Battle Management System (ABMS))

SEI Cybersecurity Engineering (CSE)

An approach for integrating software security engineering with SSE across the acquisition lifecycle.

Key areas of focus:

- Procurement strategies
- Secure system design
- Security management / information protection (IP)
- Software assurance (SwA)
- Supply chain risk management (SCRM)
- Anti-tamper (AT)
- Model-based system engineering (MBSE)
- Reference architectures with associated documentation to support assessments

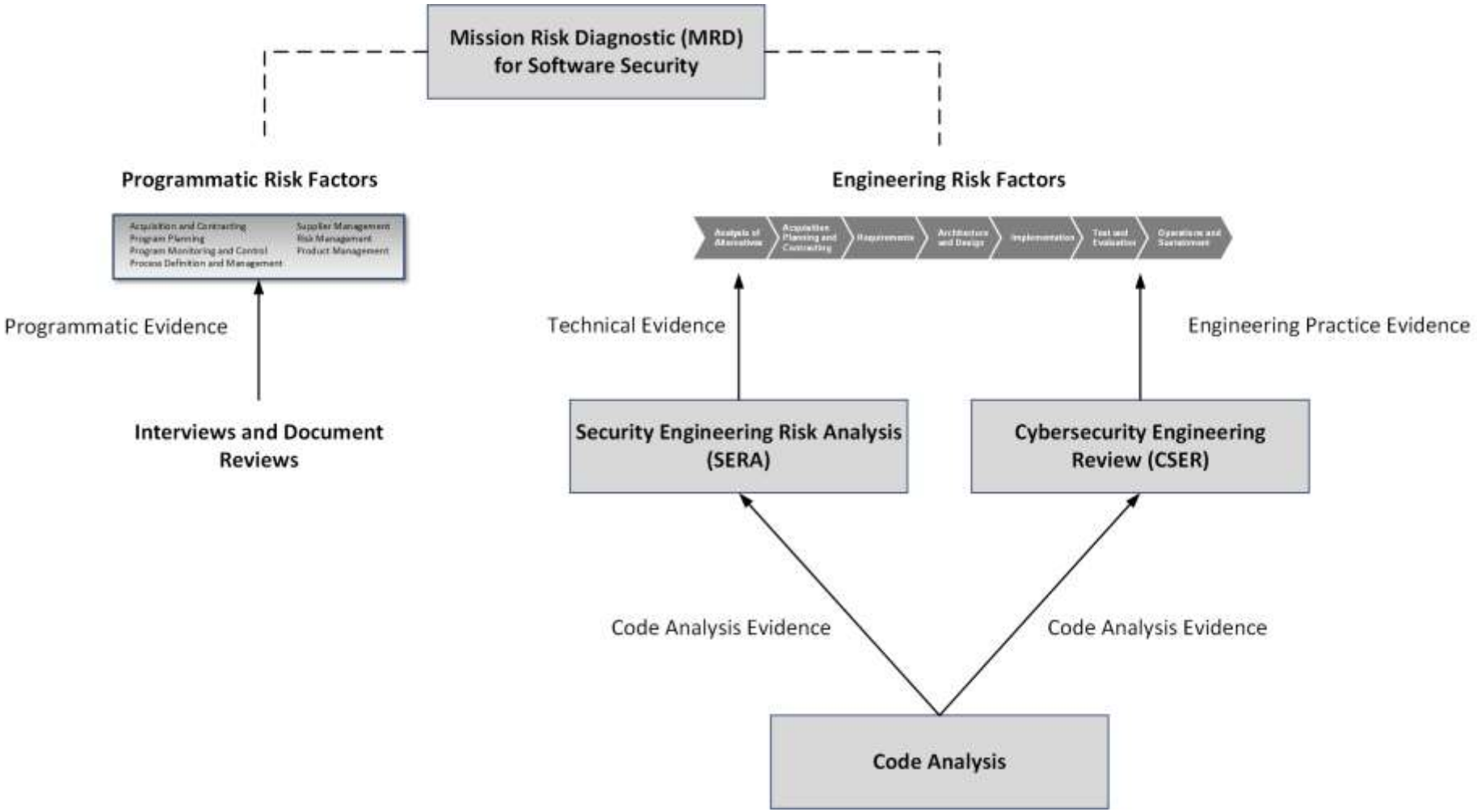
Situational Awareness (SA) CSE Assessments

Assessments are a key component of SEI's CSE strategy.

The CERT SA Team performs the following CSE assessments:

- Mission Risk Diagnostic (MRD)
- Security Engineering Risk Analysis (SERA)
- Cybersecurity Engineering Review (CSER)

SA CSE Assessments: *An Integrated View*



Mission Risk Diagnostic (MRD)

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

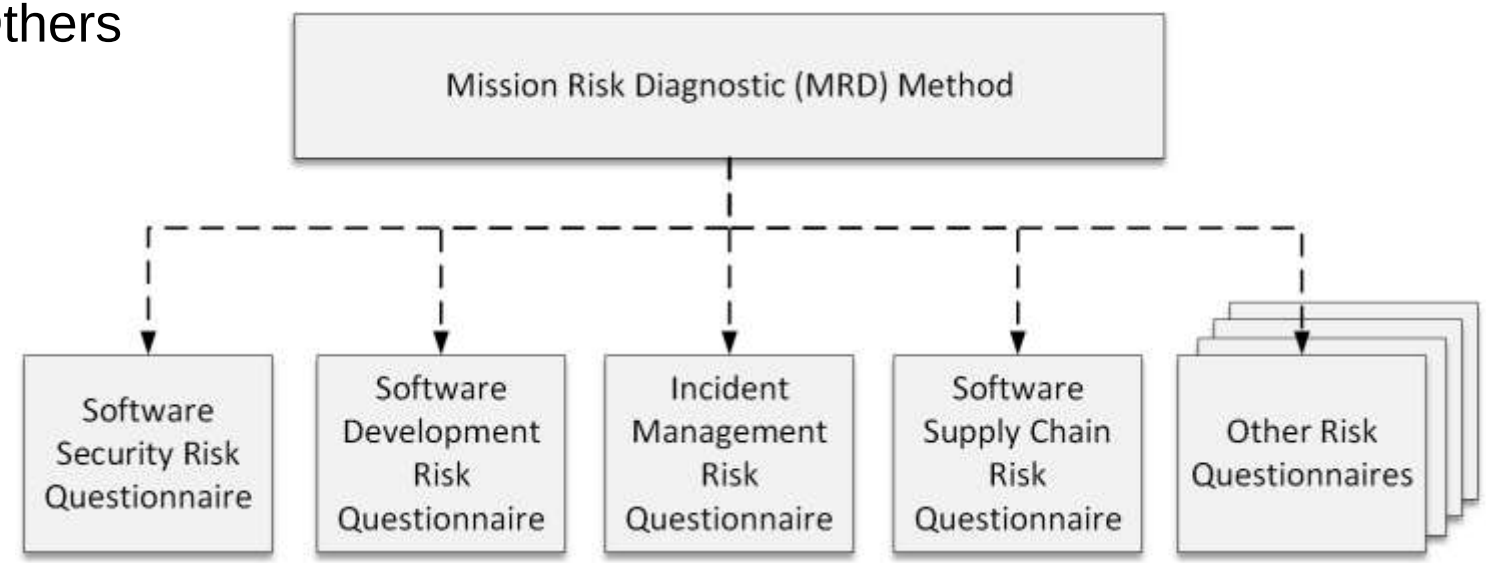
Benefits

- 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

MRD Assessment Platform

The SEI has applied the MRD platform in a variety of contexts, including

- Software acquisition and development
- Software security
- Software supply-chain
- Incident management
- Business portfolio management
- Others



Example: *Risk Factors for Software Development*

Programmatic Risk Factors

1. Program Objectives
2. Plan
3. Process
4. Task Execution
5. Coordination
6. External Interfaces
7. Information Management
8. Technology
9. Facilities and Equipment
10. Organizational Conditions
11. Compliance
12. Event Management

Product Risk Factors

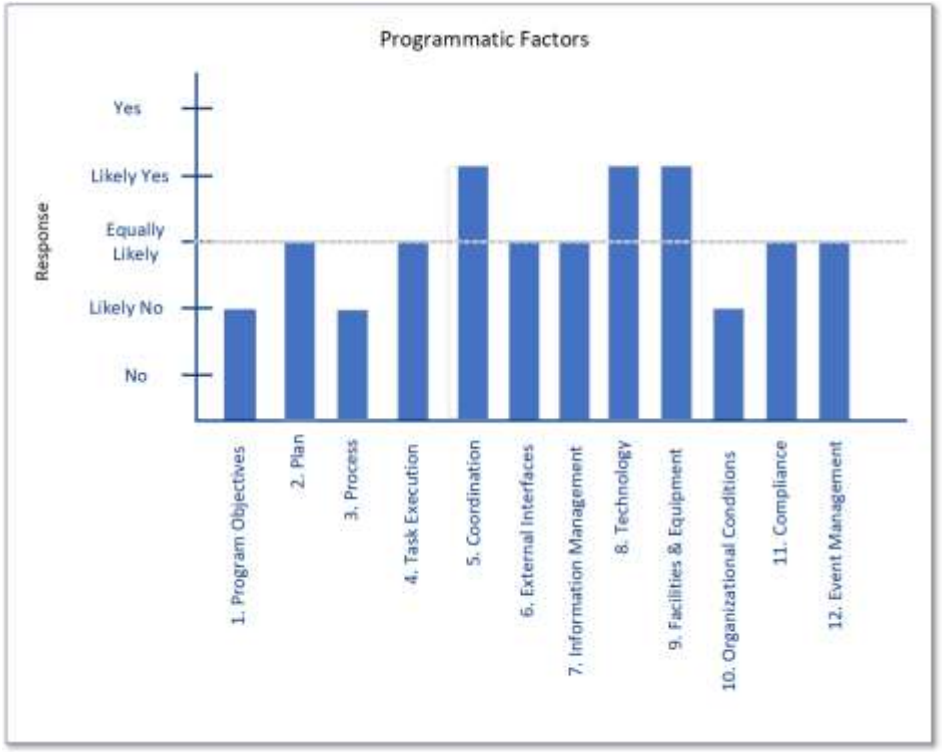
13. Requirements
14. Architecture and Design
15. System Capability
16. System Integration
17. Operational Support
18. Adoption Barriers
19. Operational Preparedness
20. Certification and Accreditation

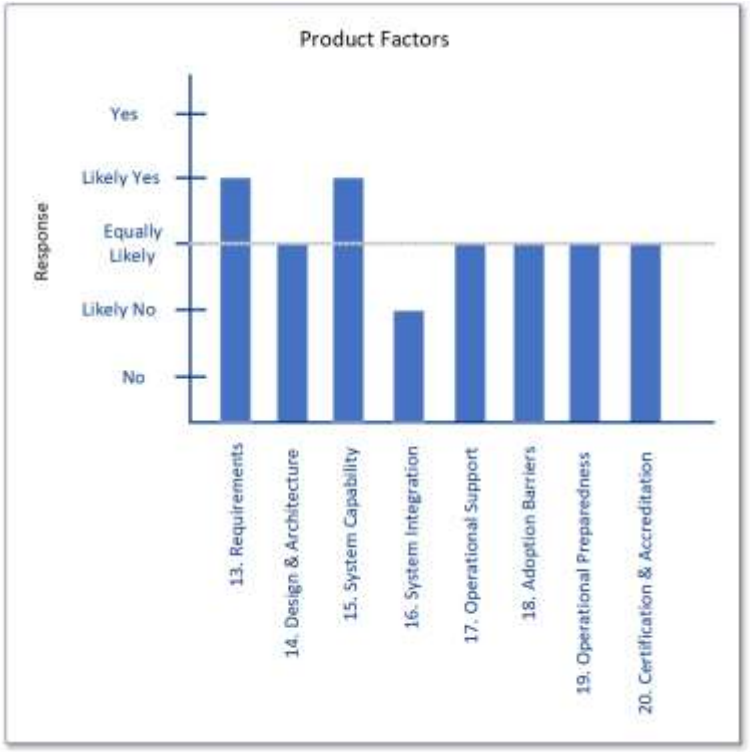
Example: *Evaluating Risk Factors*

Directions: Select the appropriate response to the question.

Question	Response
3. Is the process being used to develop and deploy the system sufficient? *Consider*: Process design; measurements and controls; process efficiency and effectiveness; acquisition and development life cycles; training	☐ Yes ☐ Likely Yes ☐ Equally Likely ☒ Likely No ☐ No ☐ Don't Know

Example: *MRD Mission Assurance Profile*





The mission assurance profile can be used as a dashboard for decision makers.

MRD: *Summary*

Assessment Types:

- DoD and Civil agency acquisition programs
- Cloud technology adoption
- Software development
- Software security
- Software supply chain
- Custom risk assessments

Time to conduct:

- ~1 month (expert-led version with existing questionnaire)
- 3-4 months (expert-led version with questionnaire development)

Security Engineering Risk Analysis (SERA)

Security Engineering Risk Analysis (SERA)

What

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

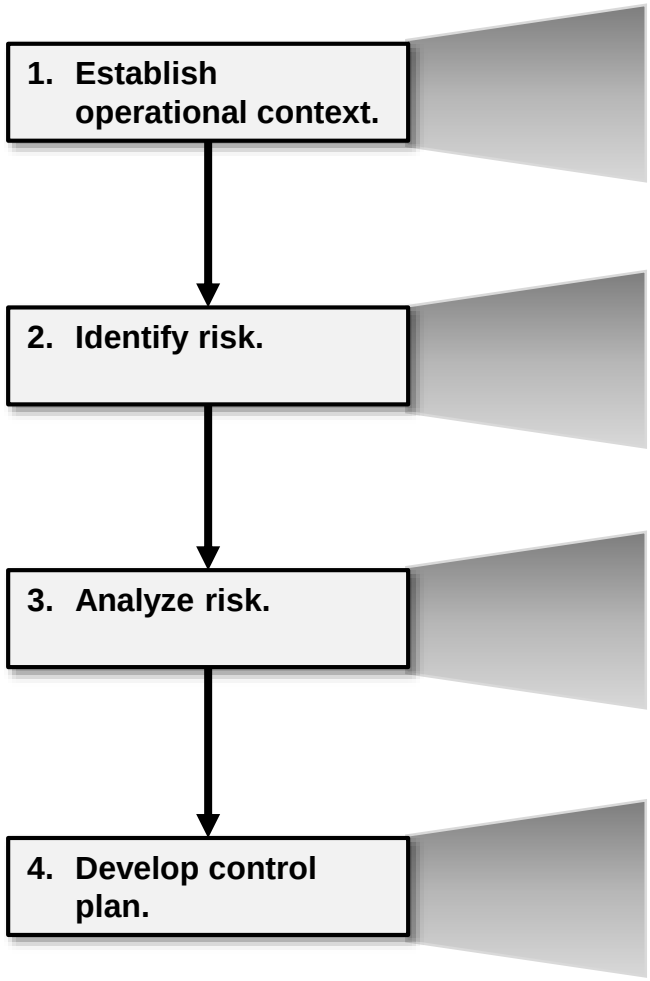
Why

- 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)

SERA Method: *Four Tasks*



Key Output
Compiled data:
- Mission thread
- System architecture
- Software architecture
- Interface diagrams
- Dataflow diagrams
- Use cases
- Network topology

Key Output
- Cyber-risk scenarios

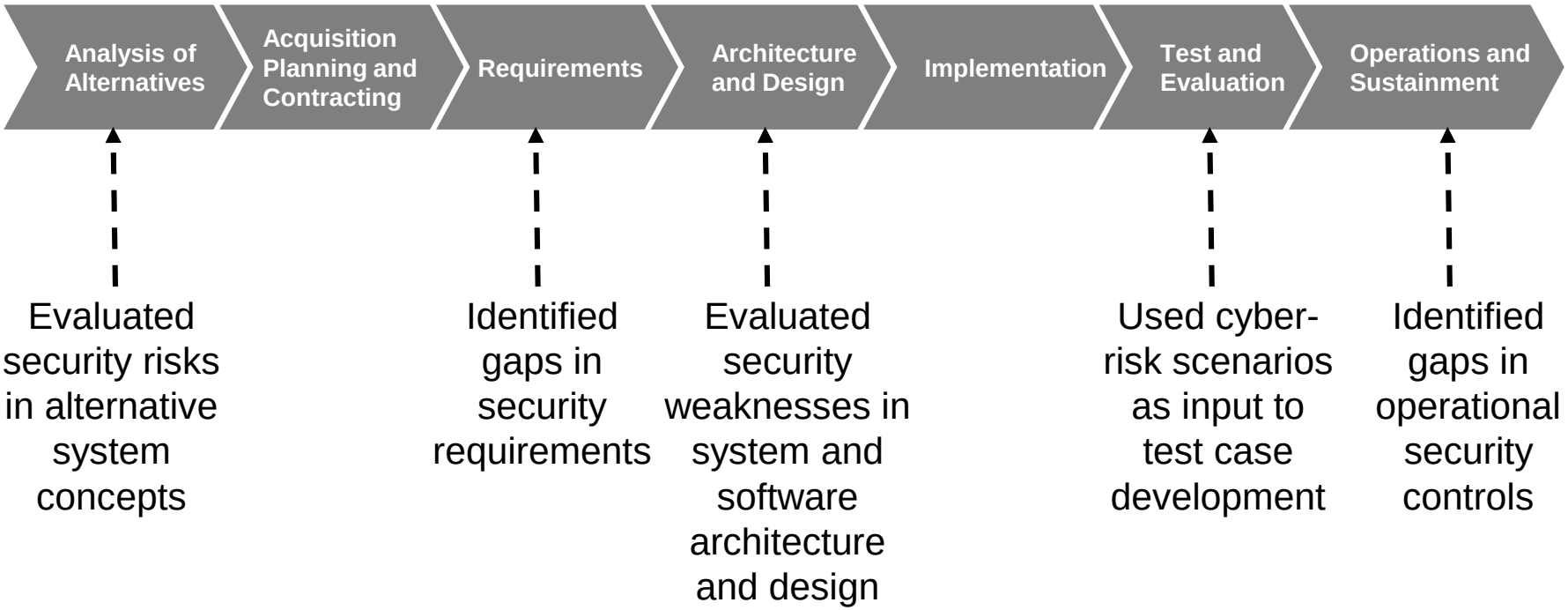
Key Input
- Threat archetypes

Key Output
- Prioritized cyber-risk scenarios

Key Output
- Control plans for high-priority cyber-risk scenarios

SERA Method: *Security Analysis Across the Lifecyle*

The SERA Method has been piloted across the acquisition and engineering lifecycle.

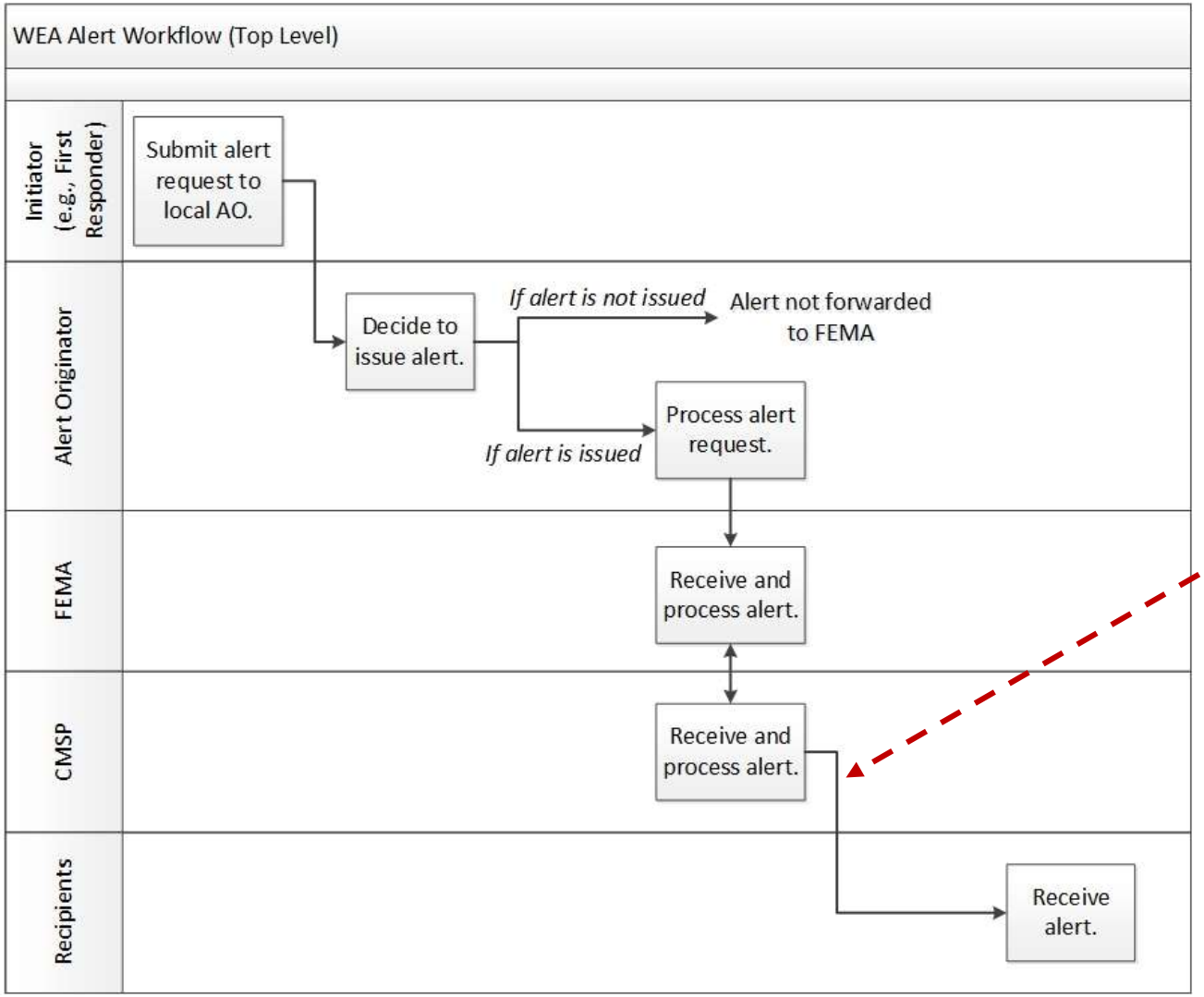


Example: *Wireless Emergency Alerts (WEA) Service*

WEA is a major component of the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS).

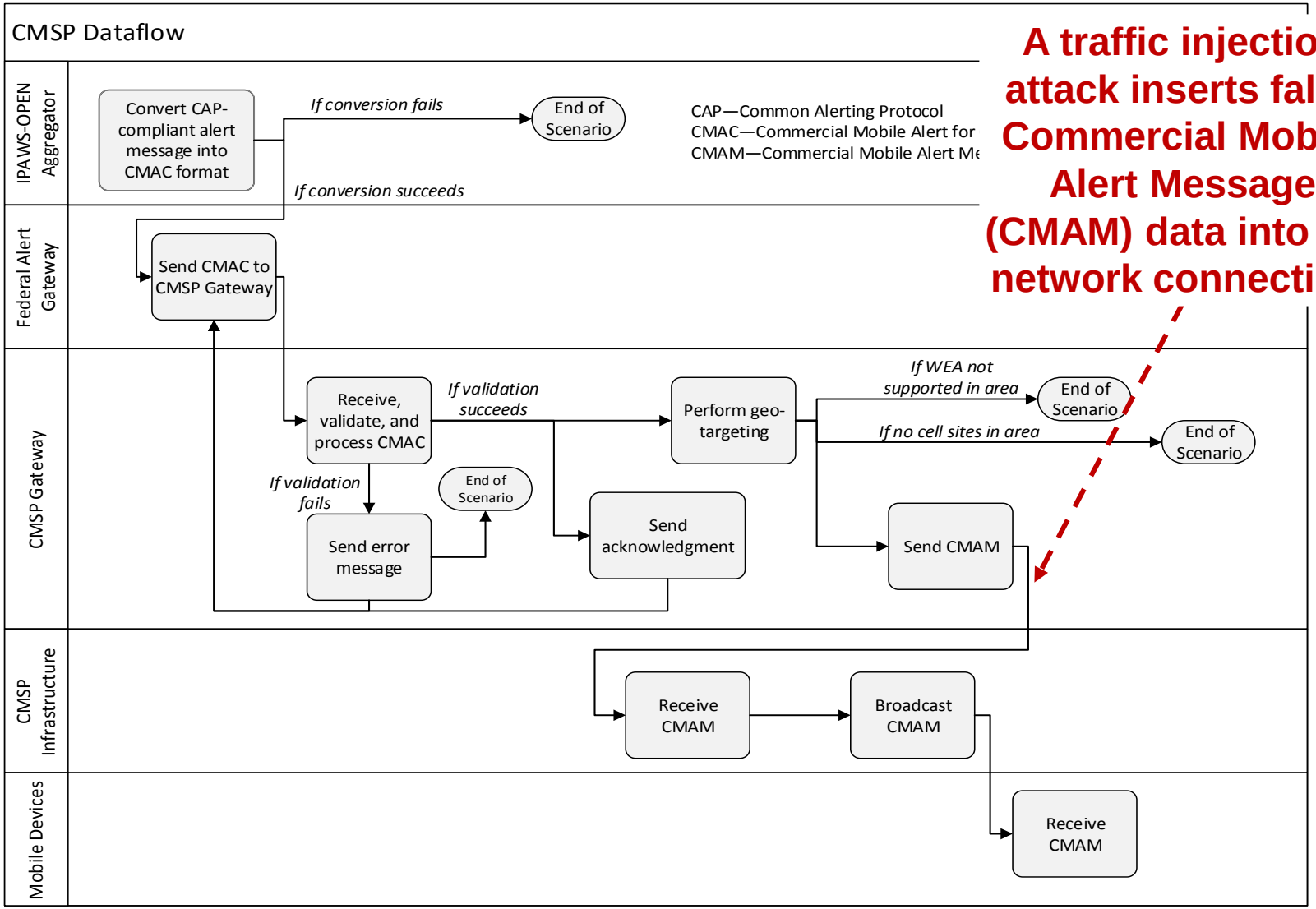
- Enables federal, state, territorial, tribal, and local government officials to send targeted text alerts to the public via **Commercial Mobile Service Providers (CMSPs)**.
- Customers of participating wireless carriers with WEA-capable mobile devices will automatically receive alerts in the event of an emergency if they are located in or travel to the affected geographic area.

Example: *Mission Impact*



CMSP sends a nonsense WEA message repeatedly to customers.

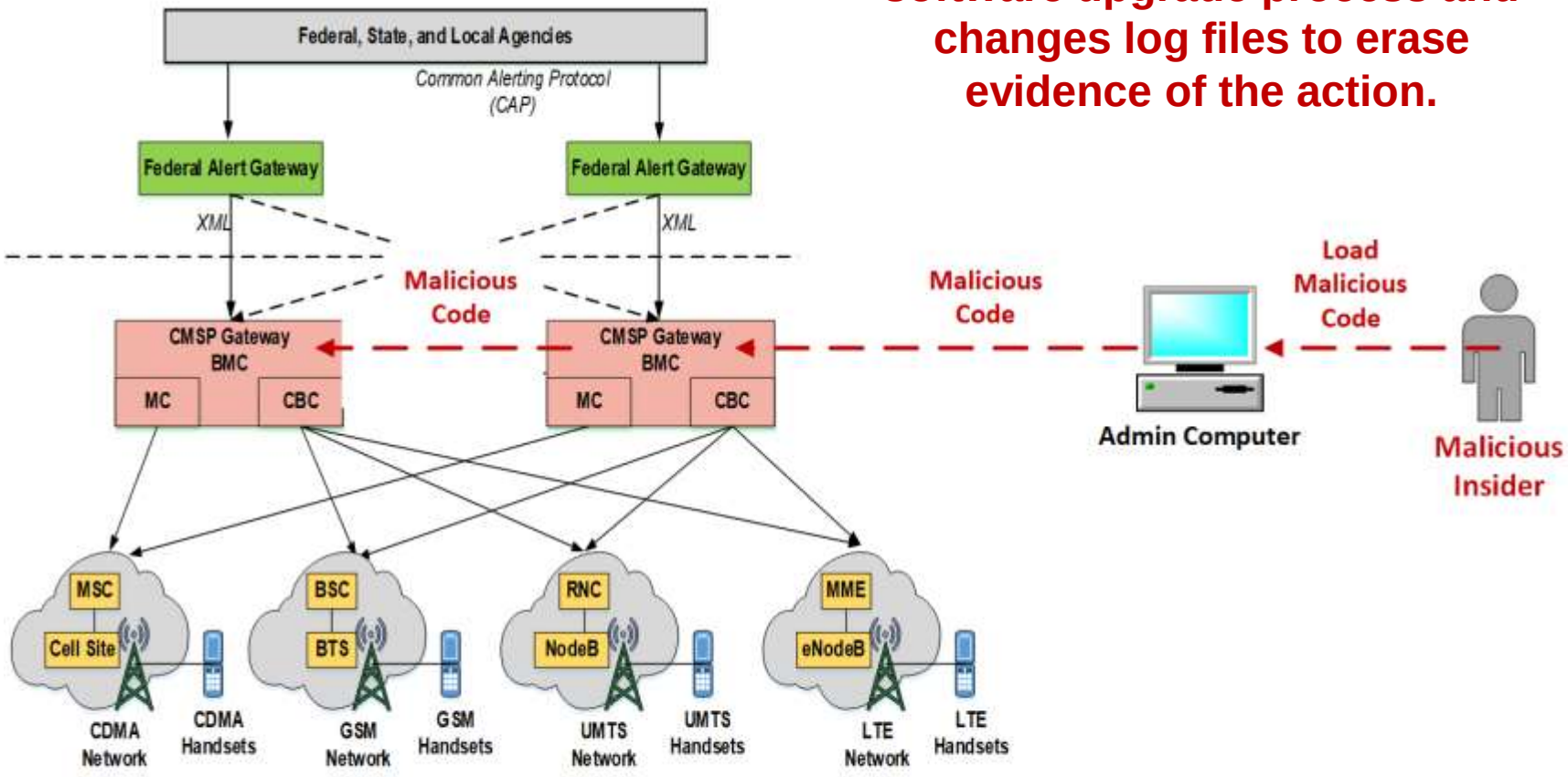
Example: *Cyber Attack*



A traffic injection attack inserts false Commercial Mobile Alert Message (CMAM) data into the network connection.

Example: *SoS Attack Vector*

The insider uploads the malicious code to the CMSP Gateway via the software upgrade process and changes log files to erase evidence of the action.



Note: Acronyms in this figure are defined in the main body of the report.

SERA Method: *Summary*

Customer Types:

- DoD weapon system acquisition (5 pilots)
- Foreign Military Sales (FMS) (2 pilots)
- Civil agency system acquisition (2 pilots)

Lifecycle Phases

- Analysis of alternatives (AoA)
- Requirements specification
- Architecture analysis
- Operational test and evaluation (OT&E)
- Operations and Sustainment (O&S)

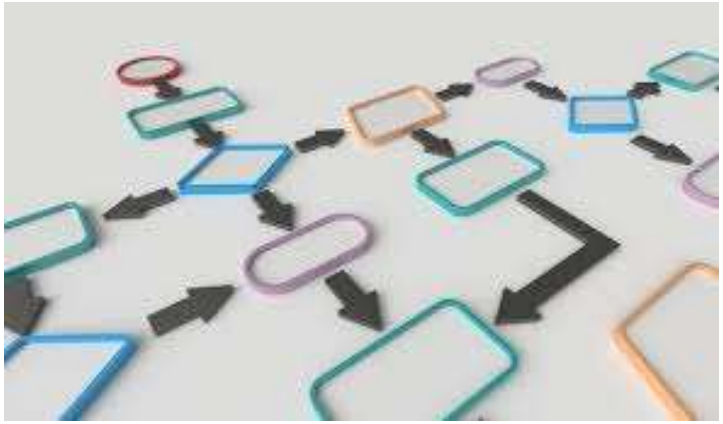
Time to conduct:

- 1-6 months (depending on scope)

CSE: SA Assessments

Cybersecurity Engineering Review (CSER)

Cybersecurity Engineering Review (CSER)



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

Prototype CSE Lifecycle Roadmap

A collection of cybersecurity engineering practices and competencies that can be applied across the lifecycle:

1. Security Risk Assessment
2. Requirements
3. Architecture and Design
4. Implementation
5. Developmental Test and Evaluation (DT&E)
6. Operational Test and Evaluation (OT&E)
7. Operations and Sustainment (O&S)

Each area of the roadmap includes the following:

- Practices
- Evidence (key outputs produced)
- Competencies

CSER: *Assessment Approach*

Collect data on program's security practices.

- Document review
  - Plans and processes
  - Work products (e.g., requirements, architecture analysis)
- Interviews (optional)
- Studies (optional)

Evaluate program's security practices in relation to CSE Lifecycle Roadmap practices.

Document observations about program's security practices.

- Strengths
- Weaknesses

Example: *General Observations*

Compliance Focus

Security is focused on system compliance. [Systems Engineering Management Plan, System Security Plan]

- Lack of a broader context (e.g. system of systems, mission resilience) could lead to unmitigated security risks.

Process Integration

Security is viewed as a specialty engineering activity. [Systems Engineering Management Plan, Critical Design Review]

- This could indicate a lack of process integration.

It is unclear how well cybersecurity engineering practices are integrated with system engineering activities. [Systems Engineering Management Plan, Critical Design Review]

- This could lead to unmitigated security risks.

Example: *Roadmap Observations*

1. Security Risk Assessment

Evaluation: Partially addressed

Rationale:

- Unclear how security assessments are performed
- Unclear if security assessments are comprehensive enough to satisfy the intent of Security Risk Assessment.

Evidence:

- A security assessment is performed on any change created as part of a Systems Engineering (SE) activity. [Systems Engineering Management Plan]
- Security assessments are completed at each relevant SE Lifecyle stage. [Systems Engineering Management Plan]
- For unaccredited systems, a security risk assessment incorporates relevant content from engineering artifacts. [System Security Plan]

CSER: *Summary*

Customer Types:

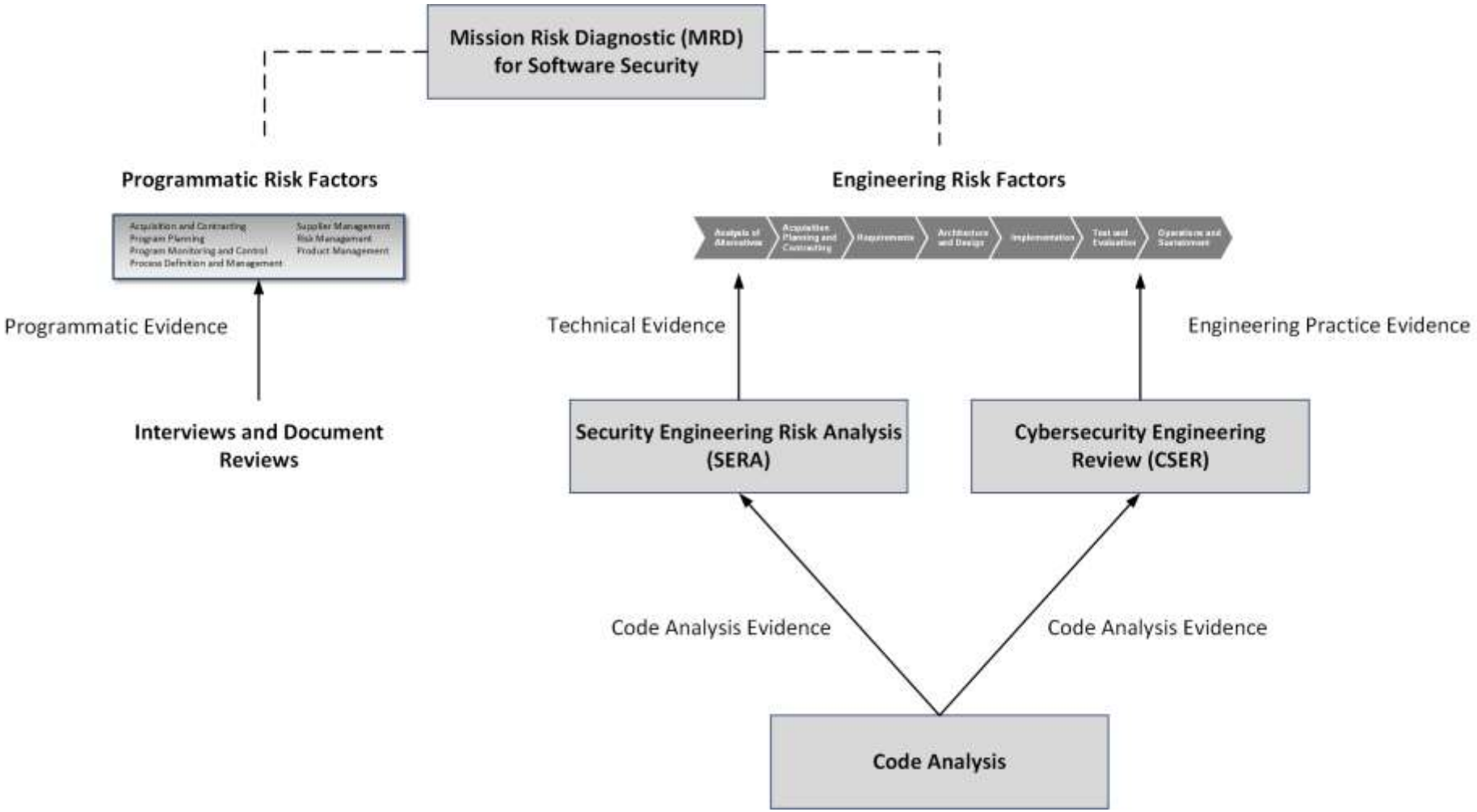
- Foreign Military Sales (FMS) (1 pilot)

Time to conduct:

- 1-3 months (depending on scope)

Summary

Summary: *SA CSE Assessments*



Key Points

SEI CSE research is defining an approach for integrating software security engineering with SSE across the acquisition lifecycle.

Assessments are a key component of the SEI CSE strategy.

- Mission Risk Diagnostic (MRD)
- Security Engineering Risk Analysis (SERA)
- Cybersecurity Engineering Review (CSER)

The CERT Situational Analysis Team is looking to expand its portfolio for its assessments.