SEI's Approach to Mission Engineering and Mission Assurance

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.

DM20-1127

Outline

Introductions

Build security in

- **Cybersecurity Engineering (CSE): Situational Awareness Assessments**
- **Architecture/Acquisition Needs/Support**

Operational resilience

- **Resilience Management Overview**
- **Cyber Resilience Assessment (CRA)**
- **Security Architecture Assessment (SAA)**

Summary

Introductions

SEI participants and backgrounds

- **Frank Redner**
- **Carol Woody**
- **Tim Morrow**
- **Chris Alberts**
- **Brett Tucker**
- **Jason Fricke**

CSE: SA Assessments

Introduction

Mission Assurance

A process to protect or ensure the continued function and resilience of capabilities and assets, including

- personnel,
- equipment,
- facilities,
- networks,
- information and information systems,
- infrastructure, and
- supply chains,

critical to the execution of DoD mission-essential functions in any operating environment or condition[1]

1. Office of the Secretary of Defense for Policy. *Mission Assurance (MA)* (DoD Directive 3020.40). Washington, DC, 2018. https://fas.org/irp/doddir/dod/d3020_40.pdf

Mission Assurance and Acquisition

Mission assurance must be considered during the acquisition of DoD software-intensive systems, such as weapon systems.[1]

- Risk management must be addressed as early as possible in the acquisition of information technology across the lifecycle.
- Acquisition programs must integrate mission assurance goals and activities with acquisition guidance.

Mission assurance must evolve from an after-the-fact, compliance-centric perspective for acceptance to an engineering-based approach that is holistic and risk-informed for all engineering and acceptance activities.[2]

1. Office of the Secretary of Defense for Policy. *Mission Assurance (MA)* (DoD Directive 3020.40). Washington, DC, 2018. https://fas.org/irp/doddir/dod/d3020_40.pdf
2. United States Air Force. *Weapon System Program Protection / Systems Security Engineering Guidebook, Version 2.0*. Wright Patterson Air Force Base, OH, 2020

DoD Mission Assurance Construct

Mission Assurance is a DoD-wide construct that focuses on prioritizing DoD efforts and resources toward addressing the most critical strategic mission execution concerns[1]

Mission Assurance construct comprises four processes:[1]

1. Identification – What is important and why?
2. Assessment – What is the risk?
3. Risk Management – What can we do?
4. Monitoring and Reporting:
   - Monitor: Threat & Hazard, Risk Response Plan, Yearly Review and Validation of DCA status
   - Reporting: Changes in Operational Status and unanticipated risks

1. Office of the Secretary of Defense for Policy. *Mission Assurance (MA) Construct* (DoD Directive 3020.45). Washington, DC, 2018. https://fas.org/irp/doddir/dod/i3020_45.pdf

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

Software Assurance

A level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the lifecycle

- Software must be designed and architected with the knowledge that it must function as intended in an increasingly contested, challenging, and interconnected cyber environment.
- Software assurance is essential for achieving mission assurance.

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

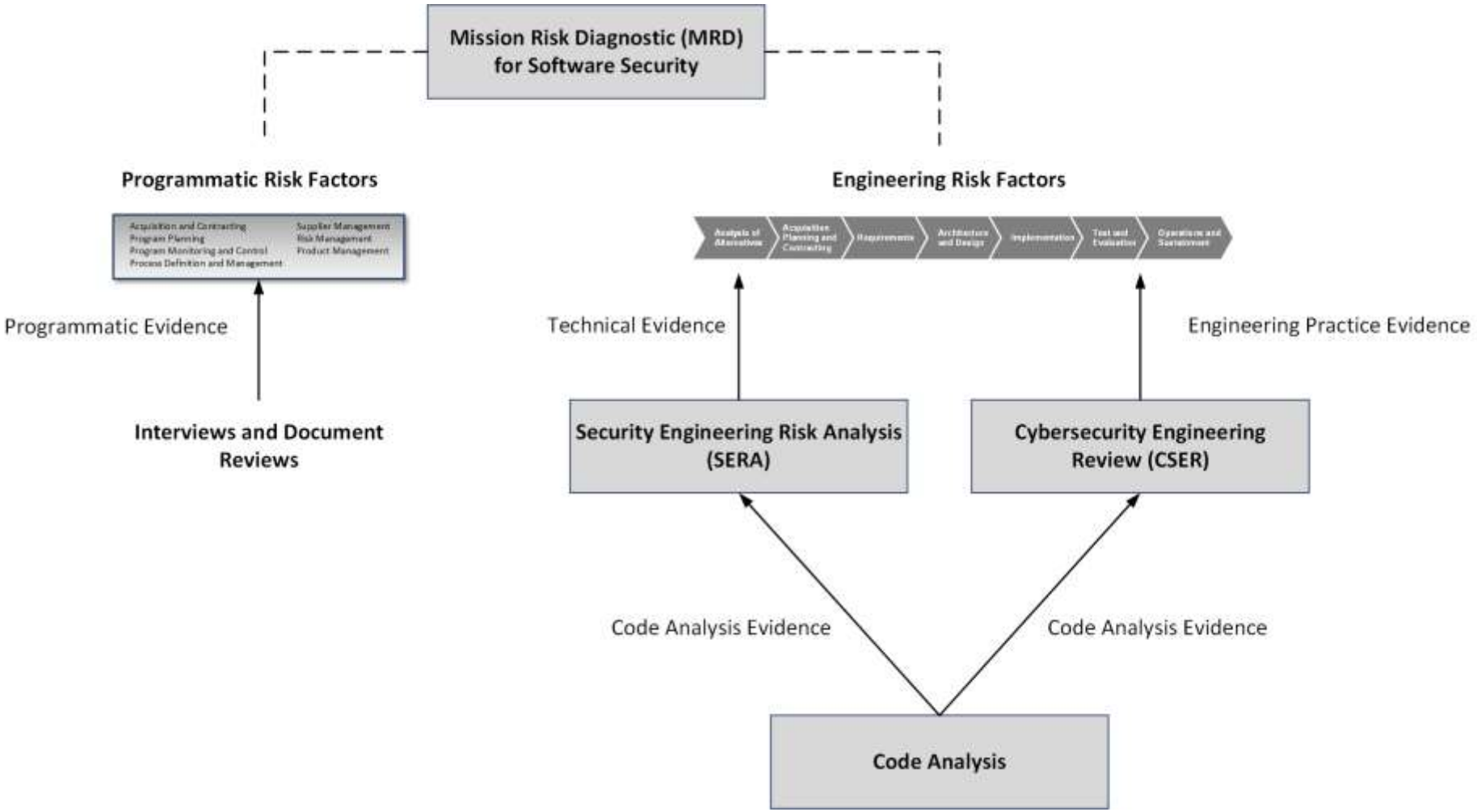
Situational Awareness (SA) CSE Assessments

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

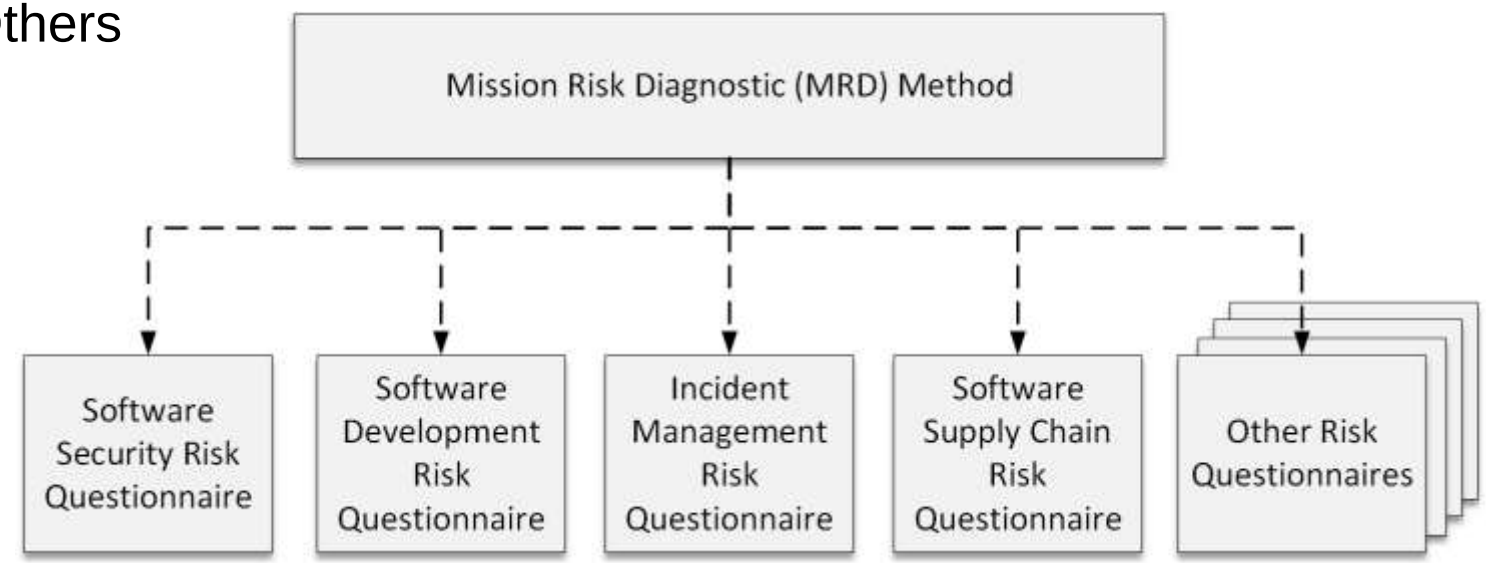
Benefits

- 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 Security*

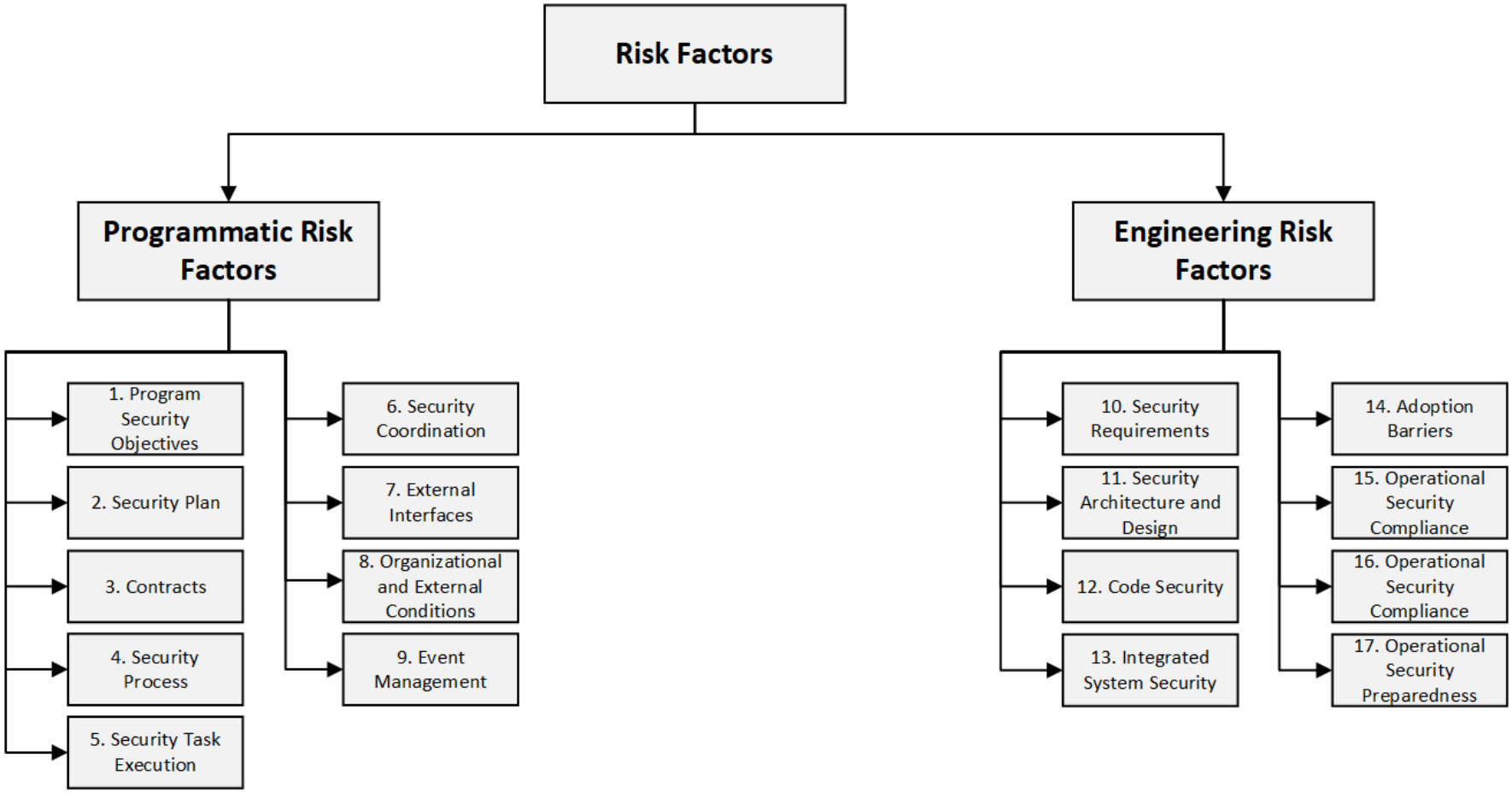
Programmatic Risk Factors

1. Program Security Objectives
2. Security Plan
3. Contracts
4. Security Process
5. Security Task Execution
6. Security Coordination
7. External Interfaces
8. Organizational and External Conditions
9. Event Management

Engineering Risk Factors

10. Security Requirements
11. Security Architecture and Design
12. Code Security
13. Integrated System Security
14. Adoption Barriers
15. Operational Security Compliance
16. Operational Security Preparedness
17. Product Security Risk Management

Example: *Risk Factors for Software Security (Hierarchical View)*



Example: *Evaluating Risk Factors*

Driver 4: Security Process

Driver Question

Does the process being used to develop and deploy the system sufficiently address security?

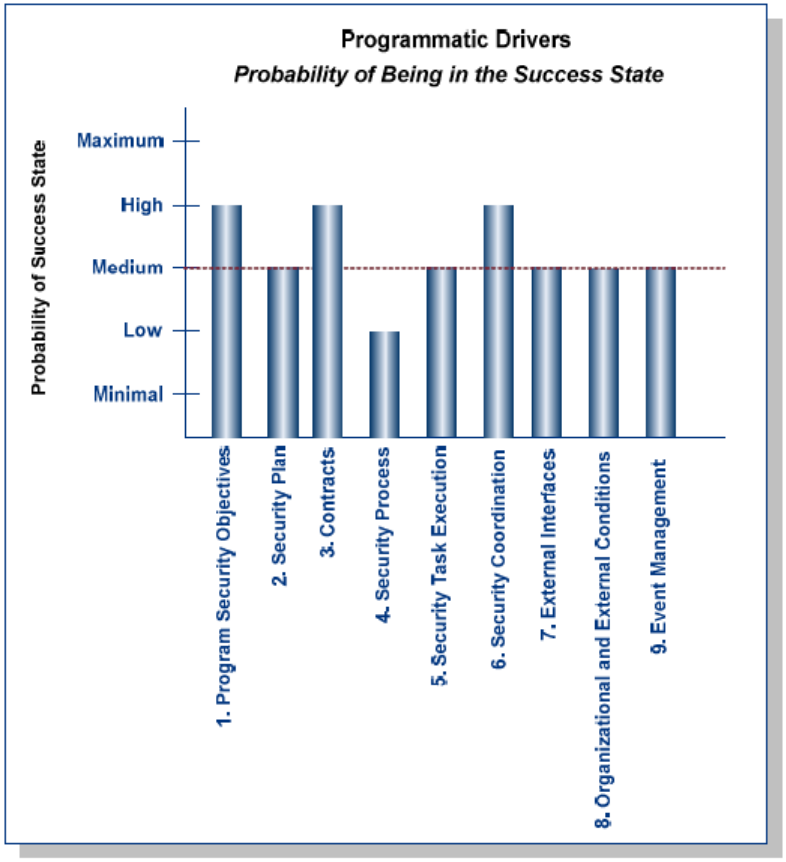
Considerations:

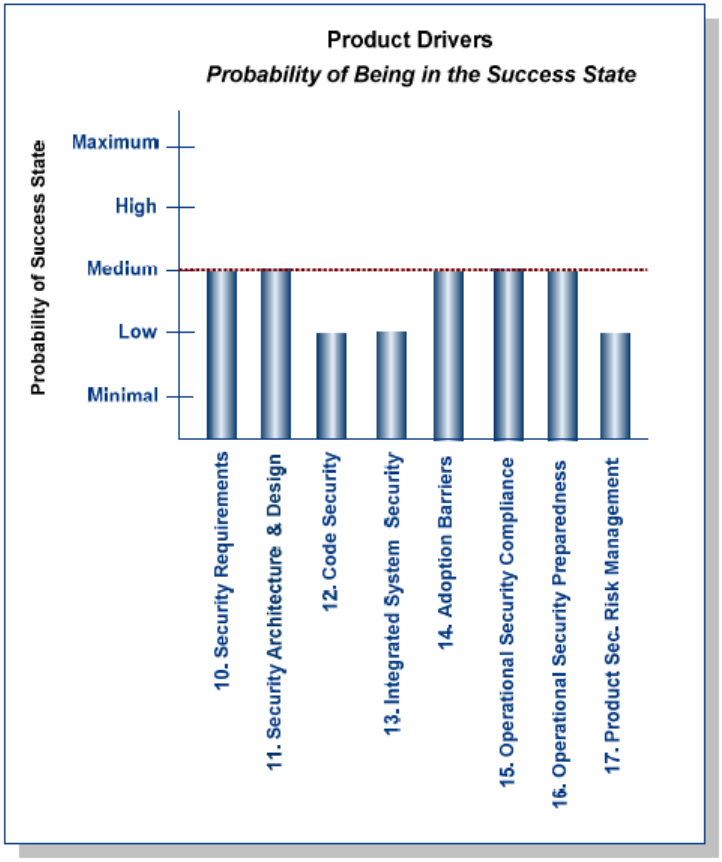
- Security-related tasks and activities in the program workflow
- Conformance to security process models
- Measurements and controls for security-related tasks and activities
- Process efficiency and effectiveness
- Software security development life cycle
- Security-related training
- Compliance with security policies, laws, and regulations
- Security of all product-related information

Response

- ❑ Yes
- ❑ Likely Yes
- ❑ Equally Likely
- ❑ Likely No
- ❑ No
- ❑ Don't Know

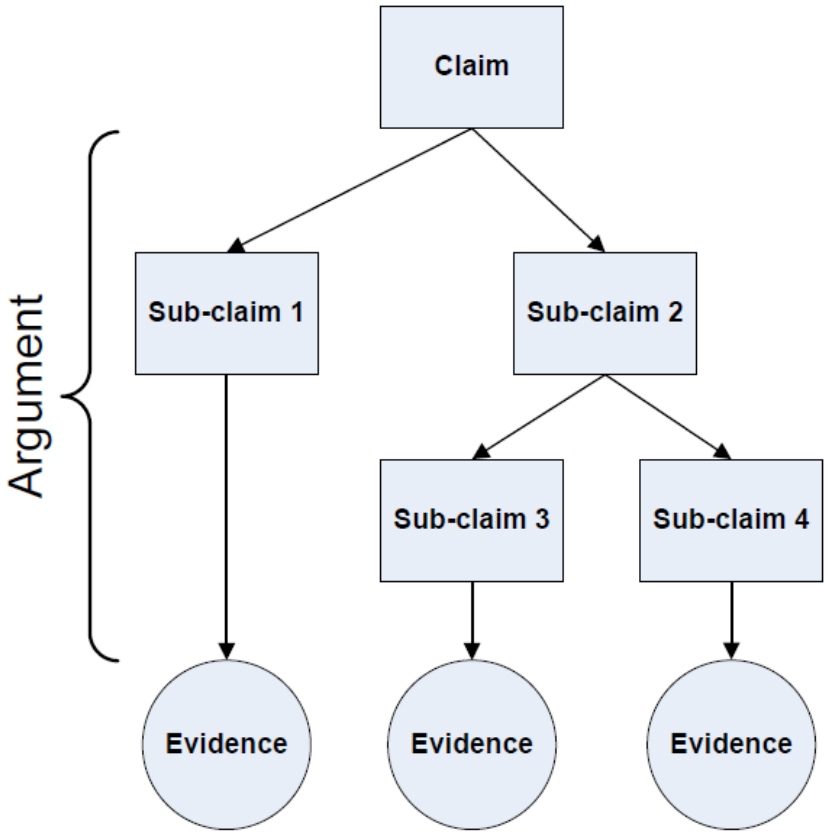
Example: *MRD Mission Assurance Profile*





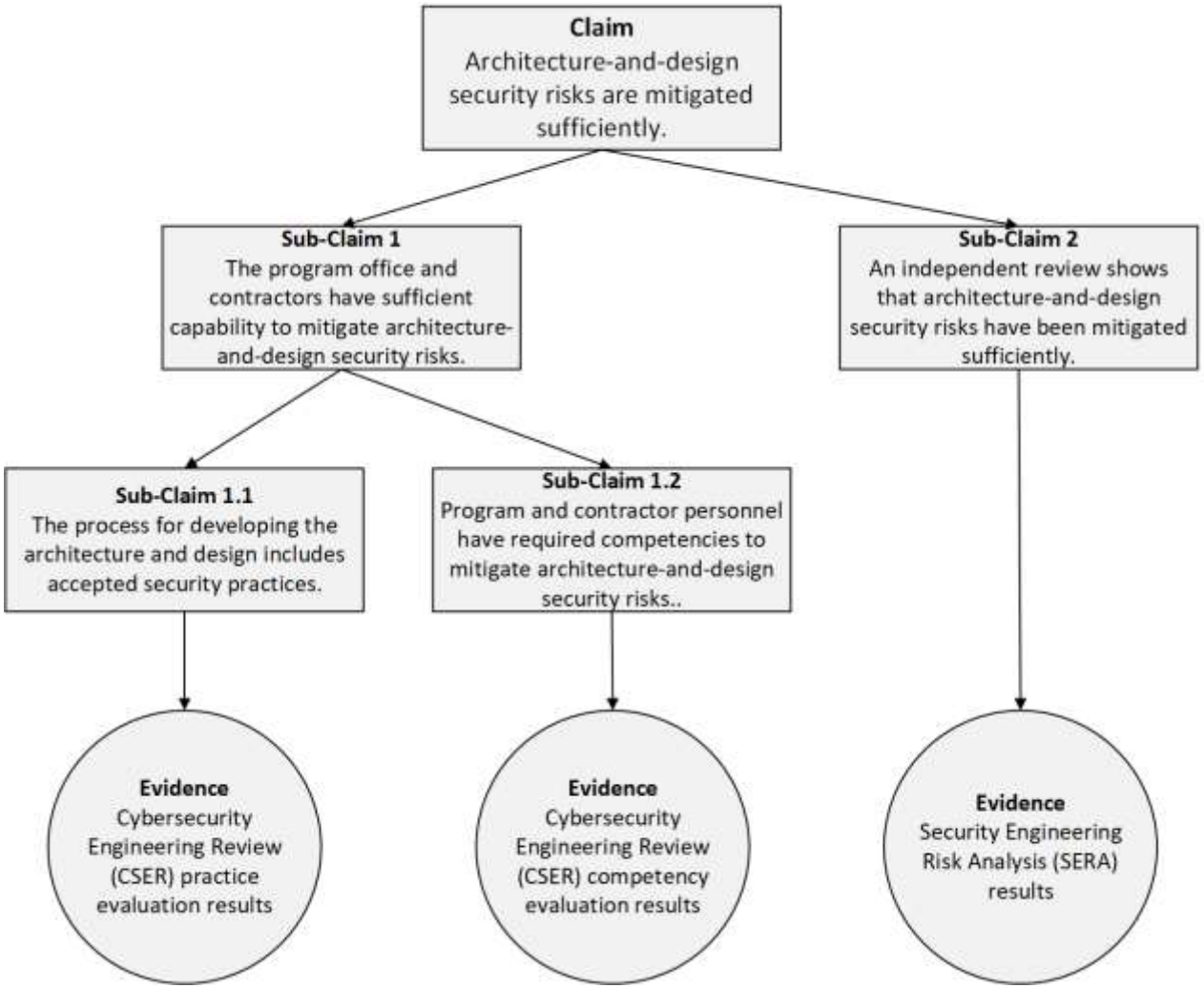
The mission assurance profile can be used as a dashboard for decision makers.

Assurance Case



A security assurance case uses a structured set of arguments and a corresponding body of evidence to demonstrate that a system satisfies specific claims with respect to its security properties

Example: *Assurance Case for Security Architecture and Design (Risk Factor 11)*



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

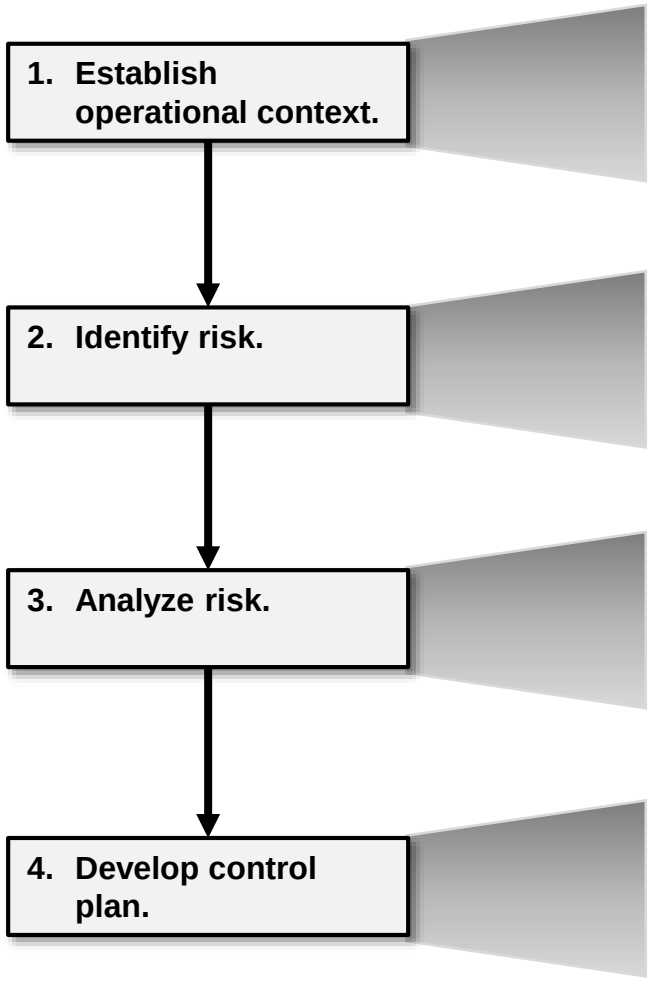
Why

- 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

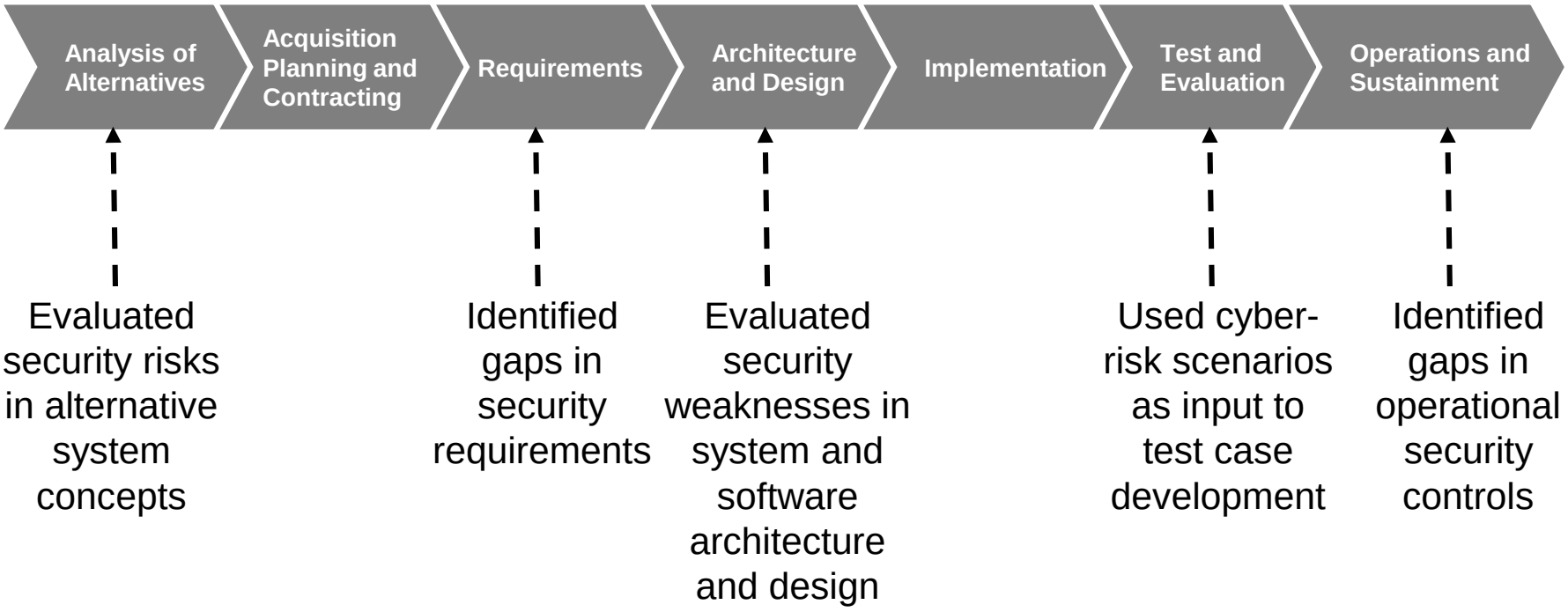
Key Input
- Threat archetypes

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.



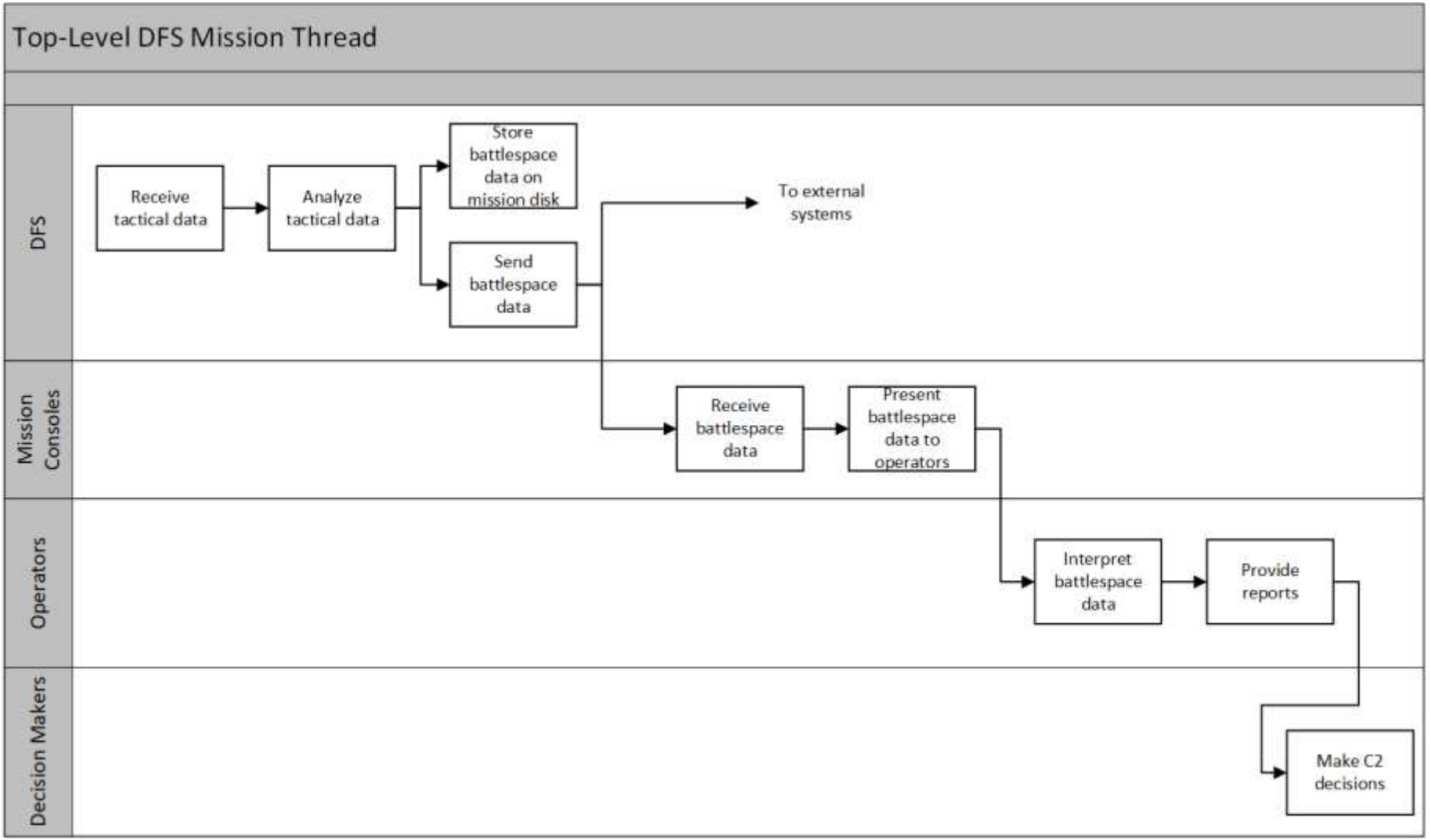
Example: *Mission Context*

A command-and-control group is acquiring a Data Fusion System (DFS) to support strategic and tactical decision making.

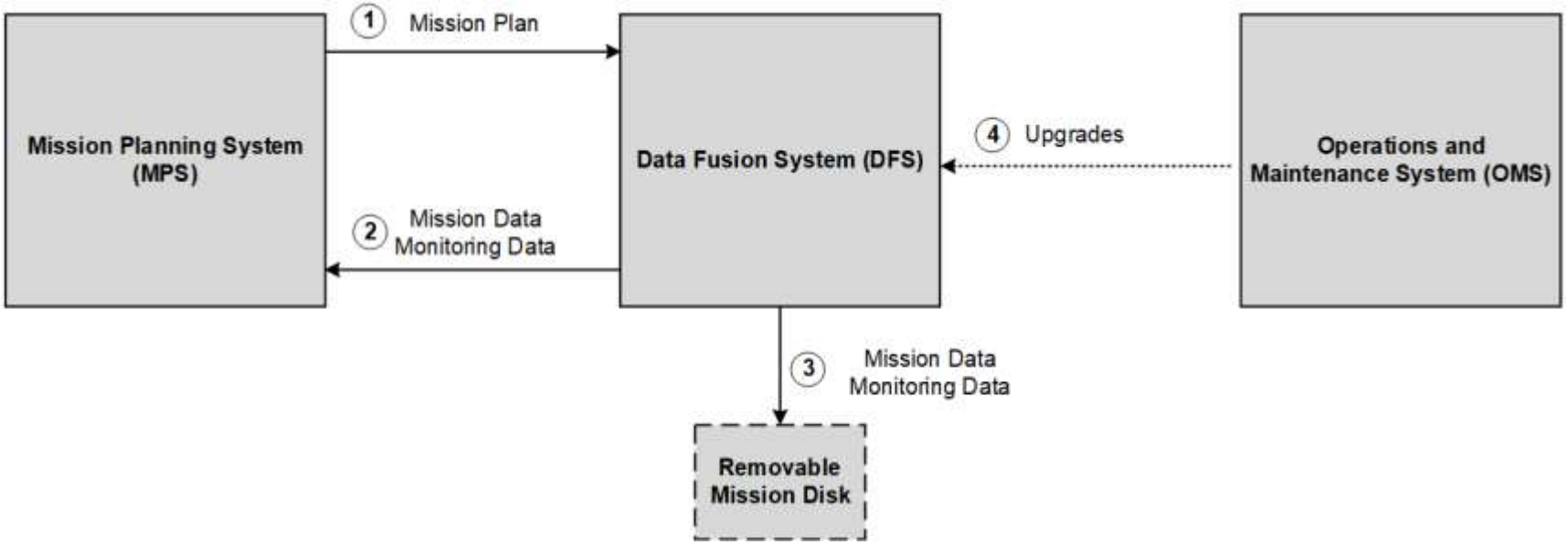
The DFS provides a single graphical representation of the battlespace by integrating tactical data from

- Data link networks
- Ground networks
- Intelligence networks
- Sensor networks

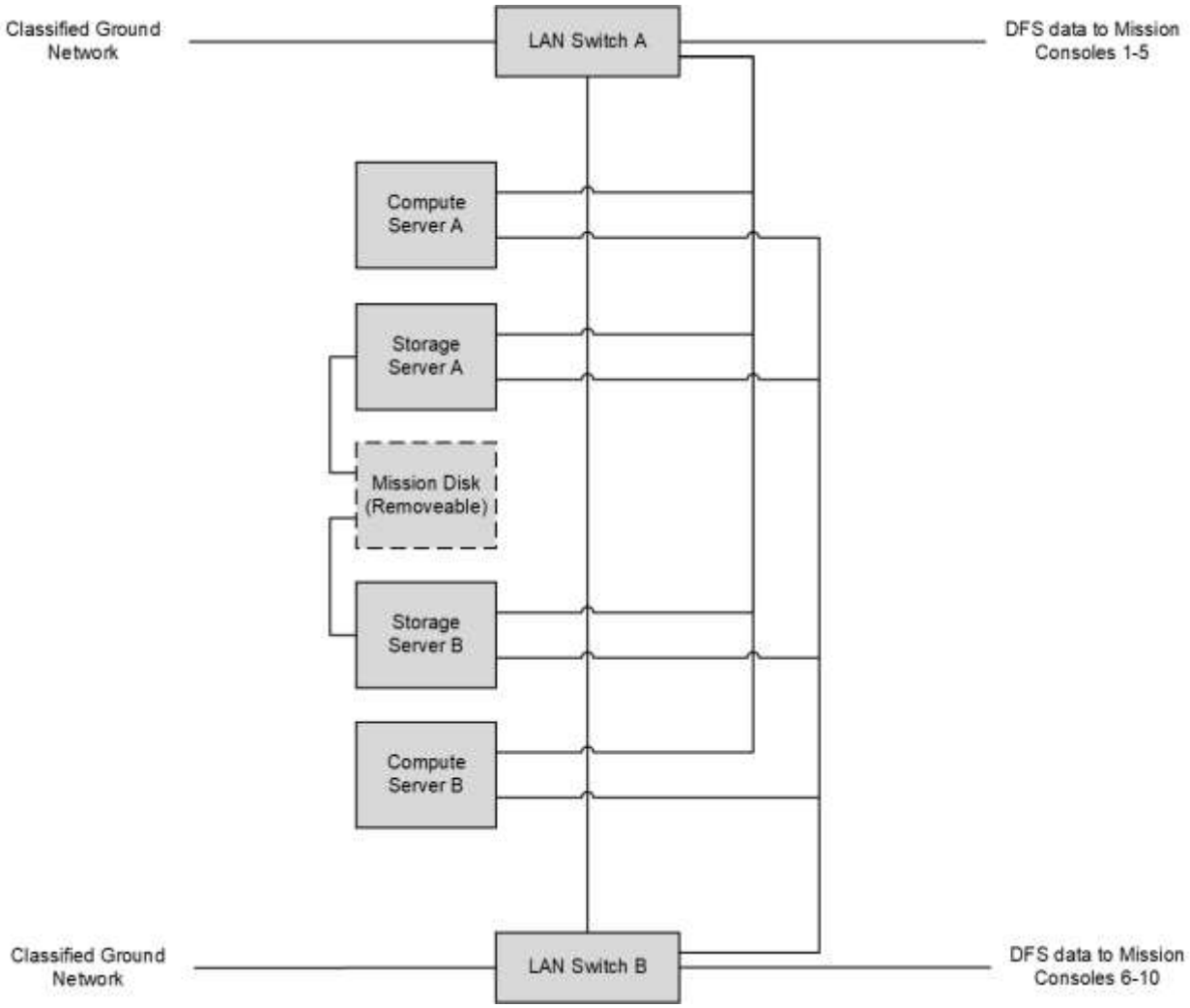
Example: *Mission Thread*



Example: *DFS Interfaces*



Example: *DFS Architecture*



Example: *Threat Archetype 1*

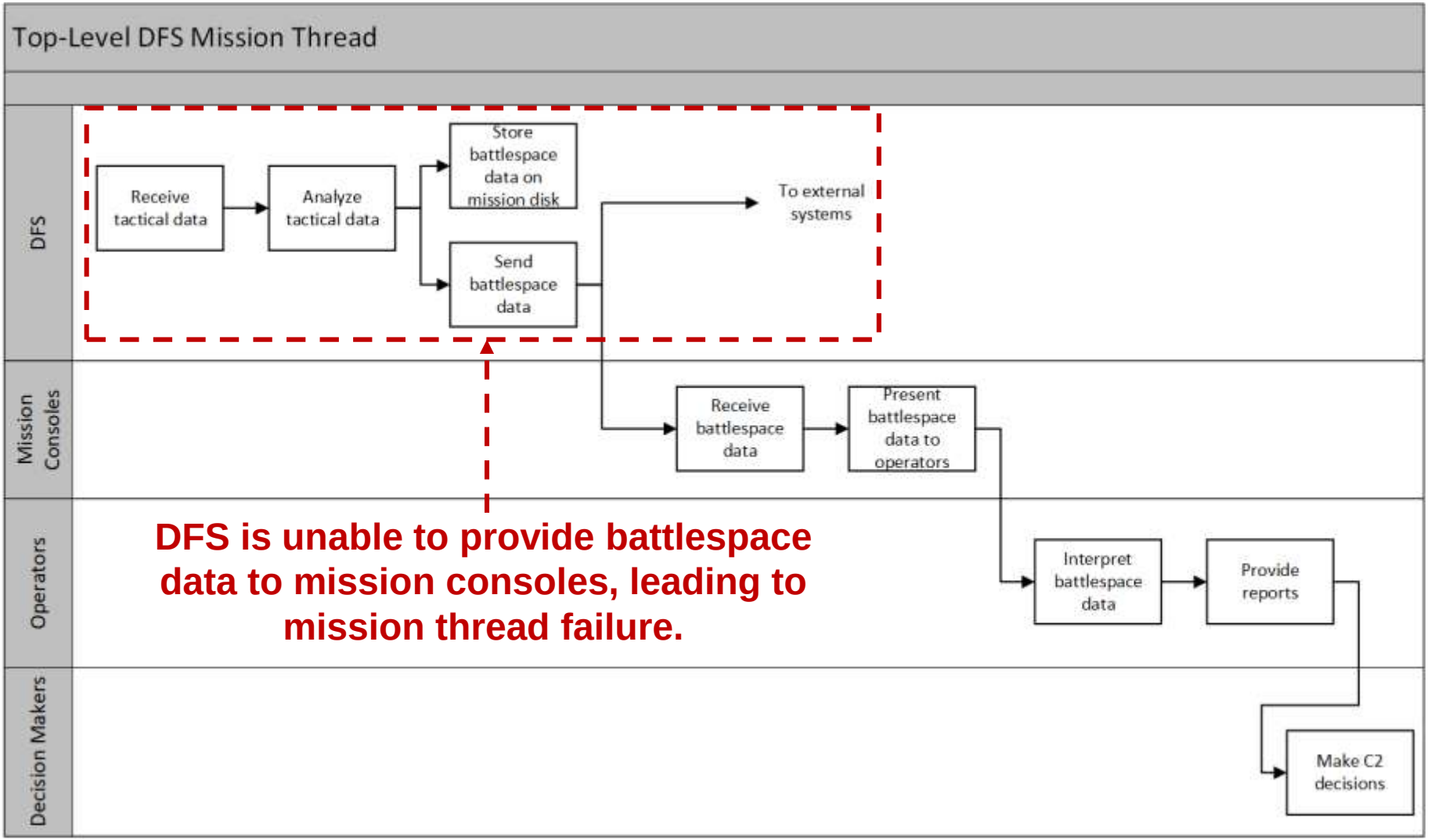
Element	Attribute
Actor	Insider
Threat Type	Targeted
Access Type	Physical
Access Point	Support/maintenance systems
Attack Pattern	Local Execution of Code (CAPEC-549) Flooding (CAPEC-125)
Direct Consequence	Interruption of access to data (availability)

A *threat archetype* is a pattern or model that describes a cyber-based act, occurrence, or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Example: *Threat Archetype 2*

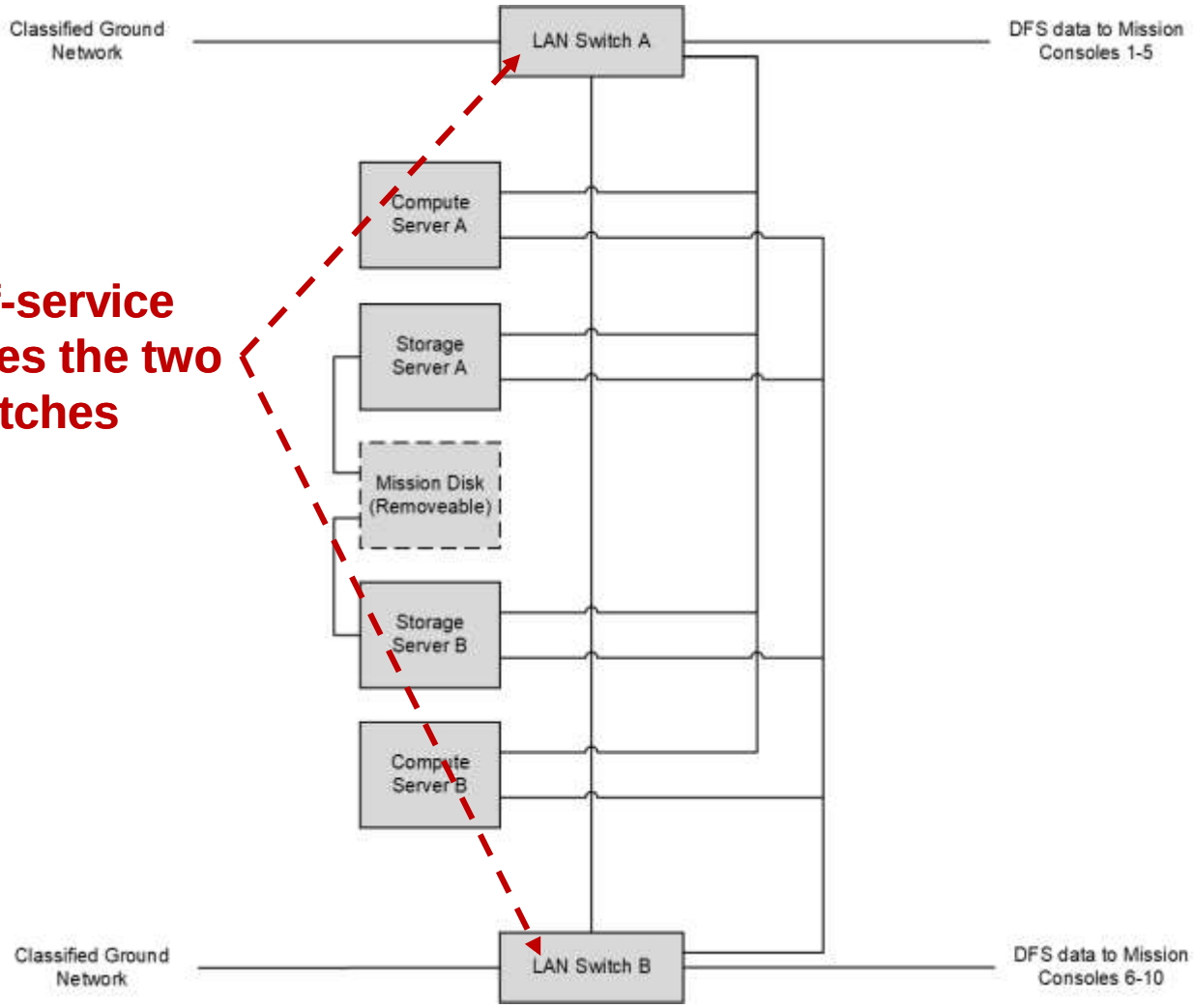
Element	Attribute
Actor	Insider
Threat Type	Targeted
Access Type	Physical and network
Access Point	Enterprise systems/networks
Attack Pattern	Privilege Abuse (CAPEC-122) Bypassing Physical Security (CAPEC-390) Research and Reconnaissance
Direct Consequence	Data disclosure (confidentiality)

Example: *Mission Impact*

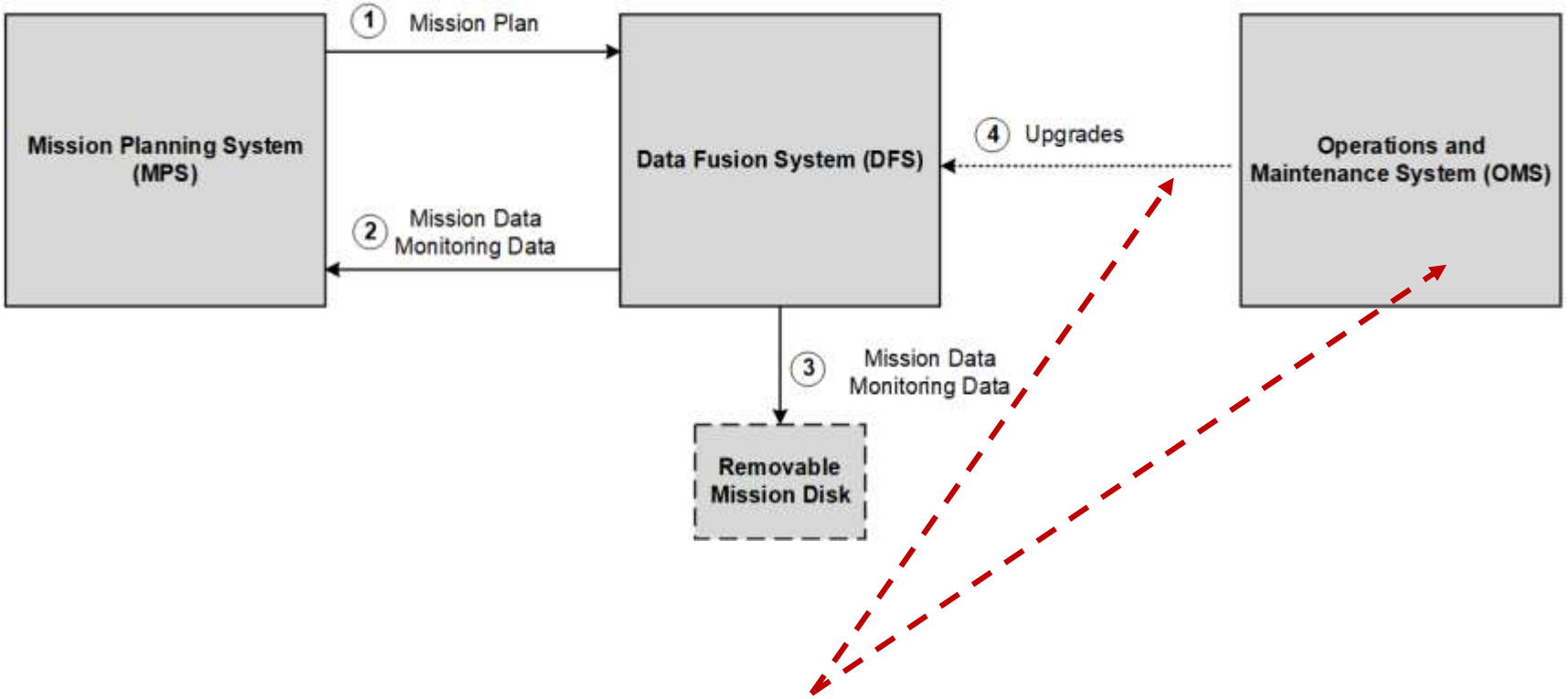


Example: *DFS Denial of Service*

A denial-of-service attack disables the two DFS switches



Example: *SoS Attack Vector*



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

Example: *Threat Sequence*

1. An insider with technical skills and administrative access to the Data Fusion System (DFS) becomes disgruntled after being passed over for a promotion.
2. The insider begins to behave aggressively and abusively toward coworkers.
3. After a while, the insider decides to execute a cyber attack on the DFS. The insider's goal is to execute a denial-of-service (DoS) attack on DFS switches.
4. The insider uses cyber access to the DFS engineering repository (resulting from insufficient access control mechanisms) to view engineering documents. The insider uses physical access to the DFS engineering organization's work space to view unsecured hard copies of DFS engineering documents.
5. The insider develops a plan for the cyber attack based on the available information.
6. The insider uses the organization's resources to develop malicious code designed to flood the DFS network with traffic.
7. The insider uploads the malicious code to the DFS via the software upgrade process and changes log files to erase evidence of the action.
8. After a mission begins, the malicious code monitors DFS network traffic.
9. When the data indicate that the DFS is receiving mission data, the malicious code's attack is triggered. The malicious code floods the DFS network with illegitimate traffic. Processing illegitimate requests consumes the DFS switches' resources, which creates an DFS denial of service.

Example: *Controls Areas for Cyber-Risk Scenario*

Access Control

Change Management

Code Analysis

Disaster Recovery

Human Resources

Incident Response

Monitoring

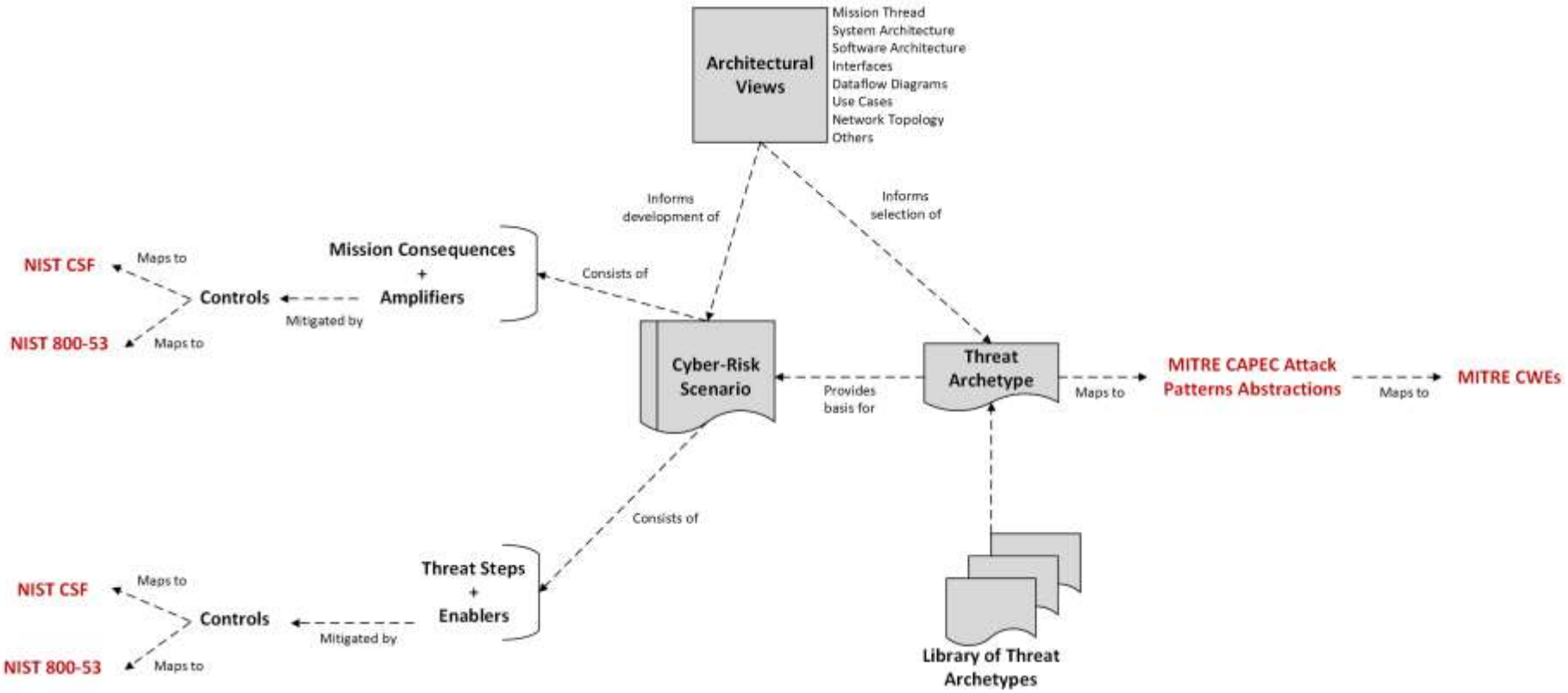
System Architecture

Training

Example: *SERA Threat Sequence Table (Excerpt)*

Step		Enabler	Candidate Control	NIST Mapping
1.	An insider with technical skills and administrative access to the Data Fusion System (DFS) becomes disgruntled after being passed over for a promotion and not receiving a bonus.	Insufficient feedback about employee performance	The organization's managers are trained to provide constructive feedback on performance issues.	NIST CSF: PR.IP-11 NIST 800-53: PS-1. PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
2.	The insider begins to behave aggressively and abusively toward coworkers.	Tolerance for inappropriate employee behavior	The organization's managers recognize inappropriate behavior when it occurs and respond appropriately.	NIST CSF: PR.IP-11 NIST 800-53: PS-1. PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
3.	After a while, the insider decides to execute a cyber attack on the DFS. The insider's goal is to execute a denial-of-service (DoS) attack on DFS switches.	No resolution to underlying employee issue	The organization's managers recognize an employee's escalating frustration and proactively work to diffuse the situation.	NIST CSF: PR.IP-11 NIST 800-53: PS-1. PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
4.	The insider uses cyber access to the DFS engineering repository (resulting from insufficient access control mechanisms) to view engineering documents. The insider uses physical access to the DFS engineering organization's work space to view unsecured hard copies of DFS engineering documents.	Insufficient access control for information and resources (physical and cyber)	Physical access to information and resources is managed and protected.	NIST CSF: PR.AC-2 NIST 800-53: PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
			Access permissions and authorizations for computing resources are managed.	NIST CSF: PR-AC-4 NIST 800-53: AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		Insufficient monitoring of the organizational environment for abnormal activity (physical and cyber)	The organization monitors the physical environment for abnormal activity.	NIST CSF: DE.CM-2 NIST 800-53: CA-7, PE-3, PE-6, PE-20
			The organization monitors systems and networks for abnormal activity.	NIST CSF: DE.CM-1 NIST 800-53: AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
			The organization performs targeted monitoring of individuals with suspected behavioral issues.	NIST CSF: DE.CM-3 NIST 800-53: AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
			The organization responds appropriately when abnormal activity is detected.	NIST CSF: RS.MI-1, RS-MI-2 NIST 800-53: IR-4

SERA Data Mapping



SERA cyber-risk data can be mapped to security standards, such as

- NIST Cybersecurity Framework (CSF) and NIST 800-53
- MITRE CAPEC attack patterns and MITRE CWEs

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)

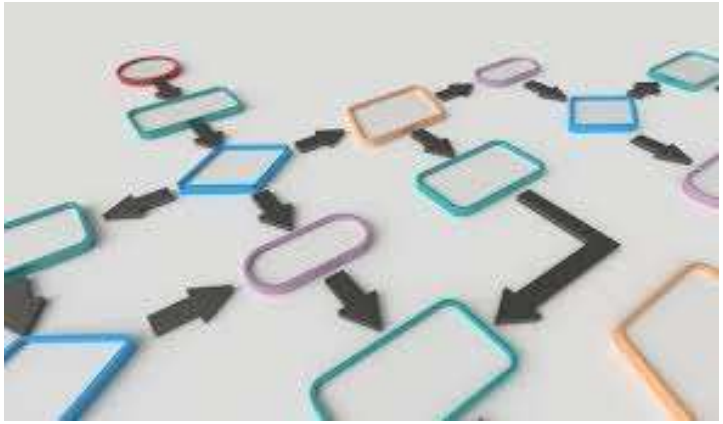
Time to conduct:

- 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:

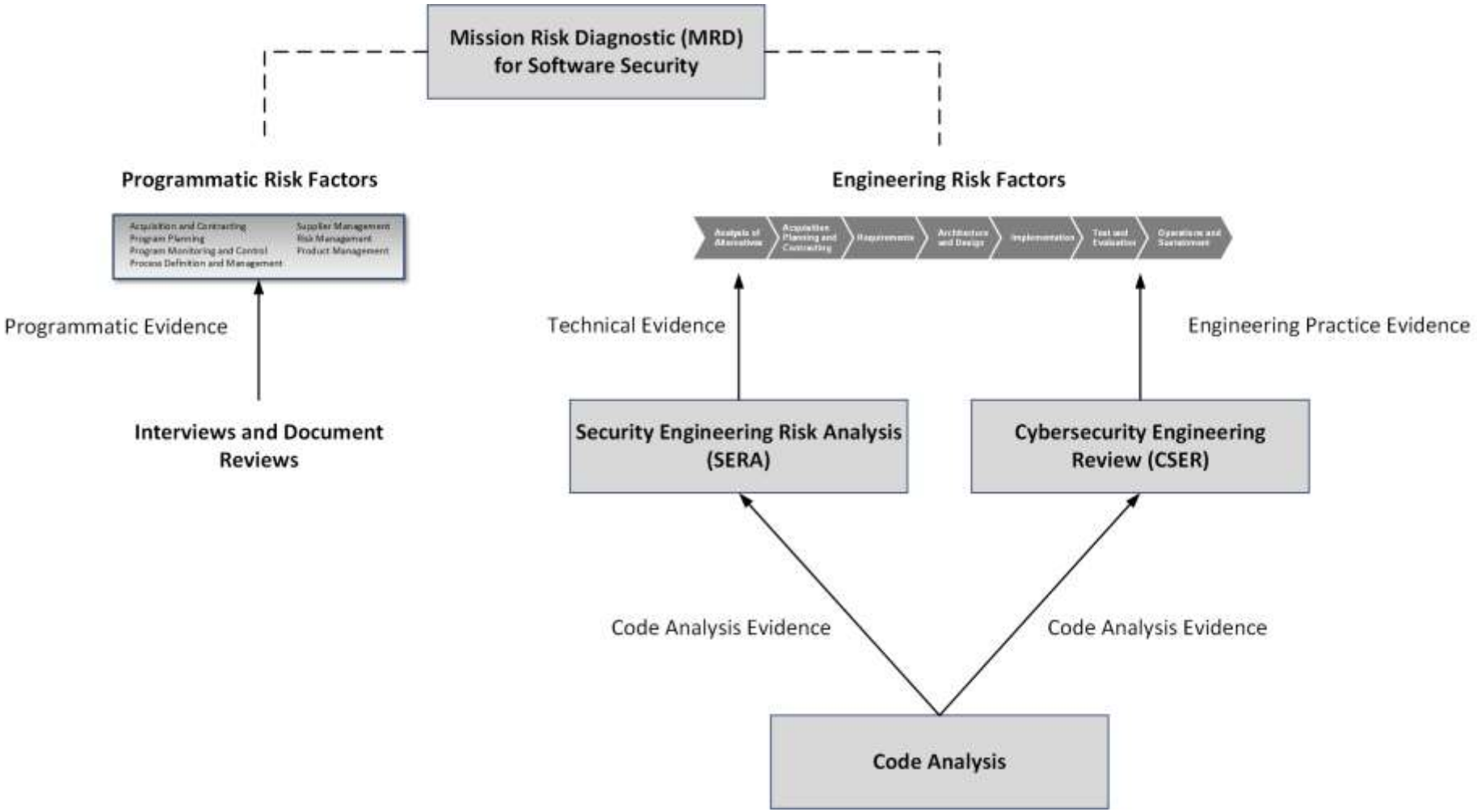
- Foreign Military Sales (FMS) (1 pilot)

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.

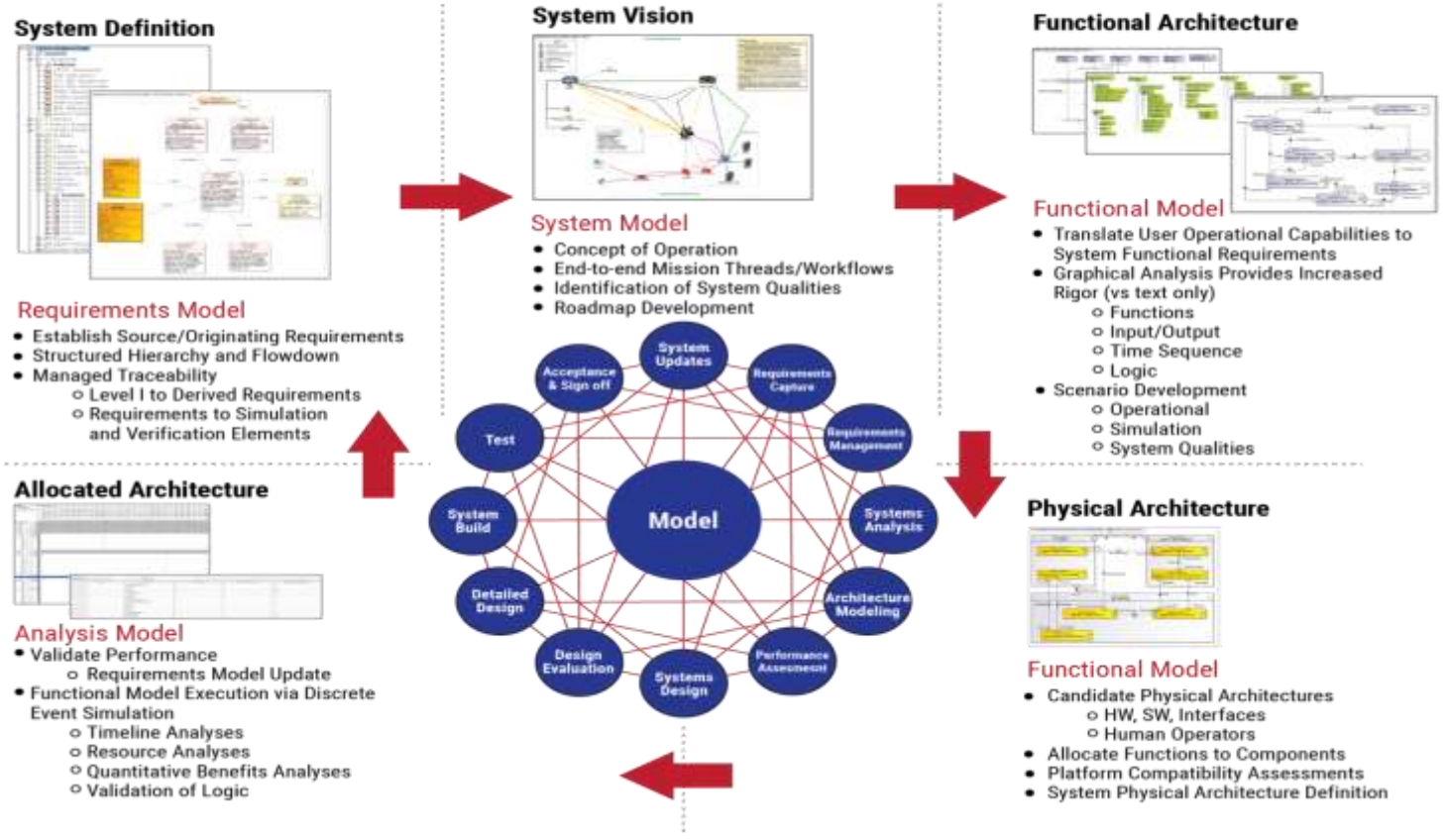
- Mission Risk Diagnostic (MRD)
- Security Engineering Risk Analysis (SERA)
- Cybersecurity Engineering Review (CSER)

We have worked with UPMC, VA, DHS, MDA, CROWS, GBSD, NC3, HBI, NASA, ATEC, Dept. of Commerce, Telemedicine and Advanced Technology Research Center (TATRC) to name a few.

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

Architecture/Acquisition Needs/Support

Model Based Systems Engineering



System-of-Systems (SoS), System, and Software Architecture

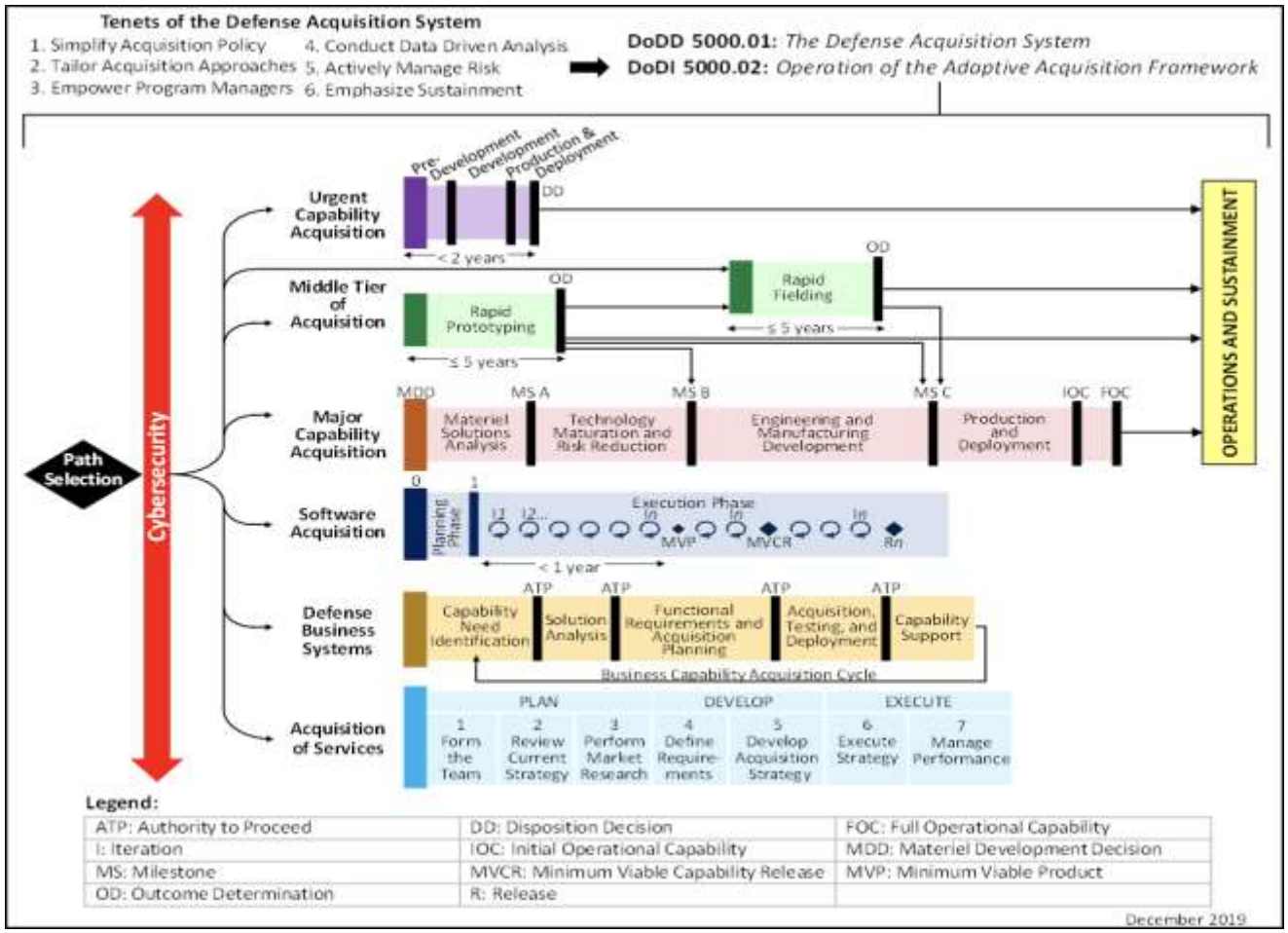
Need to develop documentation to support architecture analysis of the implementation, operation, and security of autonomous ground-based systems which operate in hybrid, multi-cloud, multiple security enclaves development, production, and test environments where Artificial Intelligence and Machine Learning (AI/ML) approaches/solutions can be applied to support autonomous operations. in a digital engineering environment.

What that will entail

- Development of conceptual, capability, operational, systems/services, and stakeholder architecture views that will provide a vision for the system which include the conceptual, logical, and physical designs. (system security engineering)
  - As-Is and To-Be architectures.
  - operational, developmental, and lifecycle support mission threads and scenarios to help provide a vision for the systems to enhance concept of operations (CONOPs) development.
  - Mission-specific reference architectures for the vehicle systems.
- Requirements development, consolidation, and refinement which includes gathering objectives and identifying mission, stakeholders, users, non-functional, and performance requirements.
  - Workflow integration.
  - Support for retrospective, streaming, and predictive analytics.
- Data security plan and methods to address storage and retrieval of data of various sensitivities, both for datasets and analytical output.
- Business case and comparative analysis of capabilities and operational activities in support of transitioning to cloud services, AI/ML, and zero trust architecture.
- Expertise and training is needed to support digital engineering environment and above mentioned technologies.

Adaptive Acquisition Framework: *Multiple Acquisition Pathways*

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



SEI's Approach to Mission Engineering and Mission Assurance

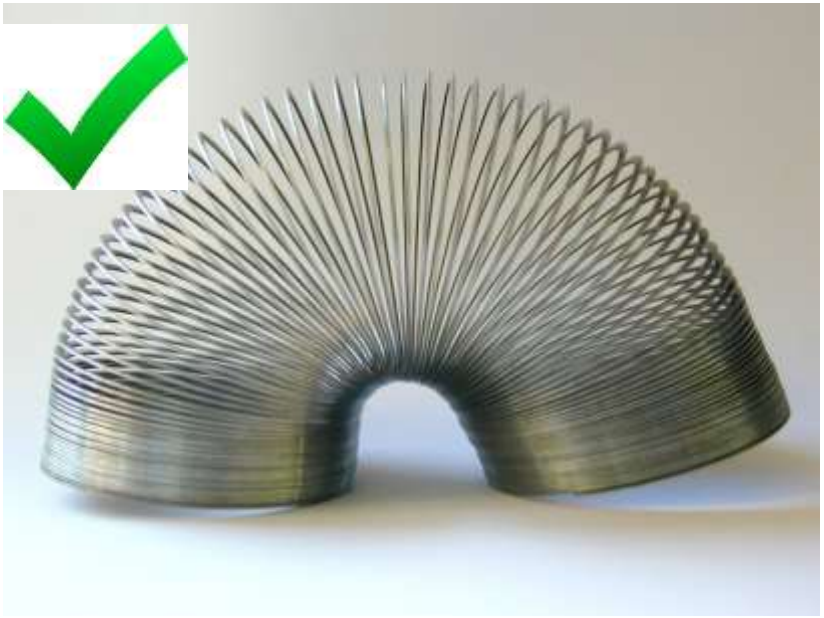
Resilience Management Overview

Operational Resilience Defined

Resilience: The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit [wordnet.princeton.edu]

Operational resilience: The ***emergent*** property of an ***organization*** that can ***continue to carry out its mission*** after ***disruption*** that ***does not exceed*** its ***operational*** limit[CERT-RMM]

Like a Slinky….



https://www.youtube.com/watch?v=EZL6RGkPjws

ERM and ORM

Operational risk management (ORM) is a significant subset of ERM.

ORM addresses day-to-day risks that can affect the organization's ability to carry out its mission.

Failure to manage operational risk can have significant impact on the organization's ERM process.

Scope of Operational Stress

Natural or Manmade

Accidental or Intentional

Small or Large

Information Technology or Operational Technology

Affecting

Technology

Information

People

Facilities

Challenges to the Operational Mission

The operational **mission** of organizations is regularly **under stress.**

The stress comes from **disruptive events** affecting business operations.

Disruptive Events…

Natural or Manmade

Accidental or Intentional

Small or Large

Information Technology or Operational Technology

- Fire
- Flooding
- IT failures
- Earthquakes
- Cyber attacks
- Severe weather
- Network failures
- Technology failures
- Organizational changes
- Loss of service provider
- Strikes or other labor actions
- Loss of customer or trading partner
- Chemical, biological, nuclear hazards
- Unavailability of workforce
- Failed internal processes
- Supply chain disruption
- Employee kidnappings
- Workplace violence
- Data corruption
- Product failure
- Power outages
- Civil unrest
- Terrorism
- Fraud
- Etc.

Result in

Interruption of Business Processes

…through which **risks are realized**

Asset Types Essential to Operational Resilience

Technology

Information

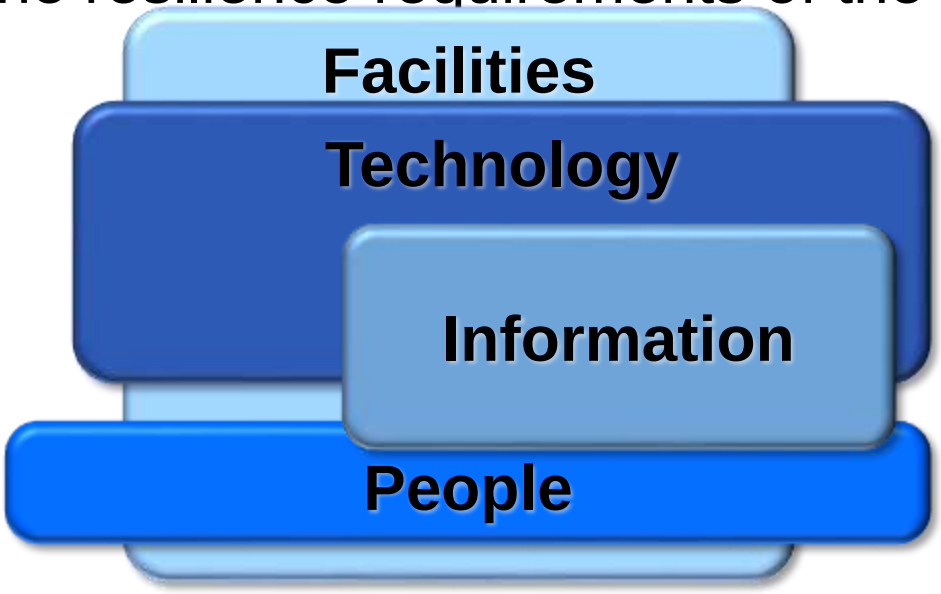
People

Facilities

Assets as “Containers”

Often, assets are containers of other assets. Facility assets may contain technology assets that, in turn, contain information assets to be stored, transported, or processed.

This concept is important because controls may be applied at the container level to meet the resilience requirements of the assets they contain.

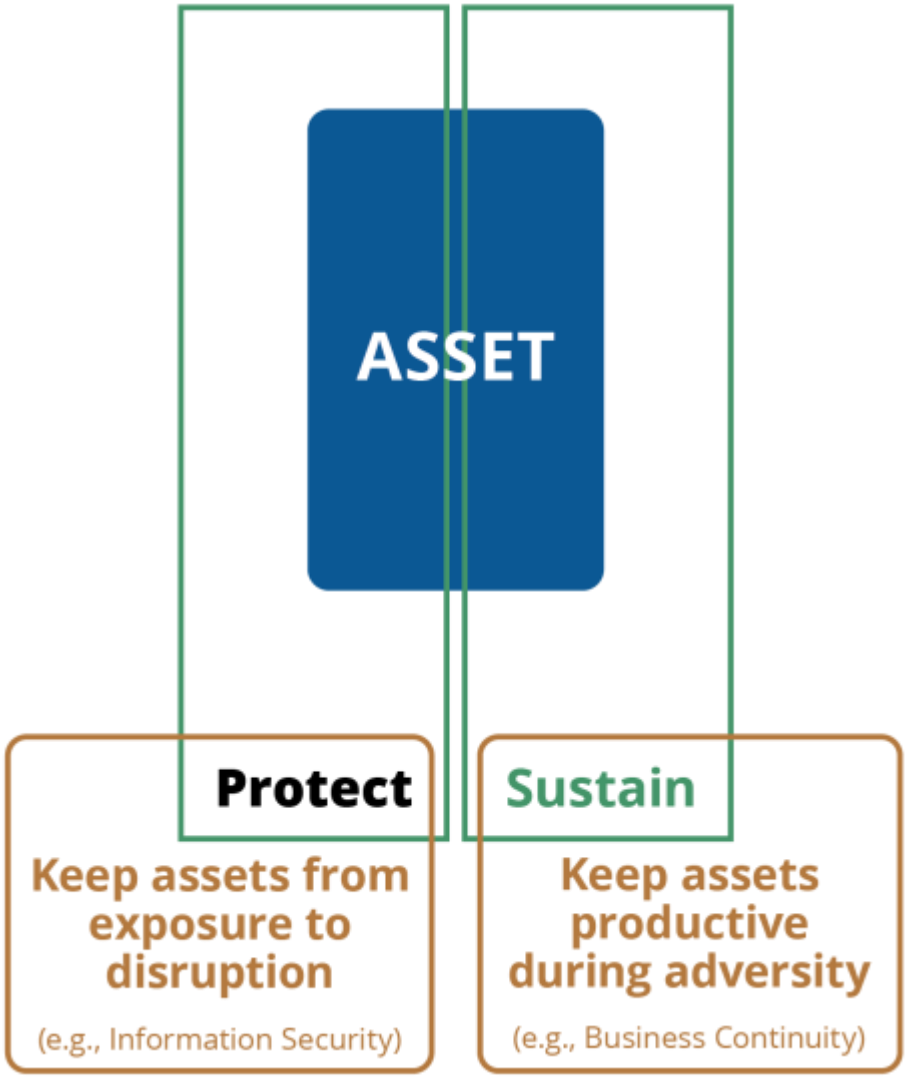


Putting Assets in Context

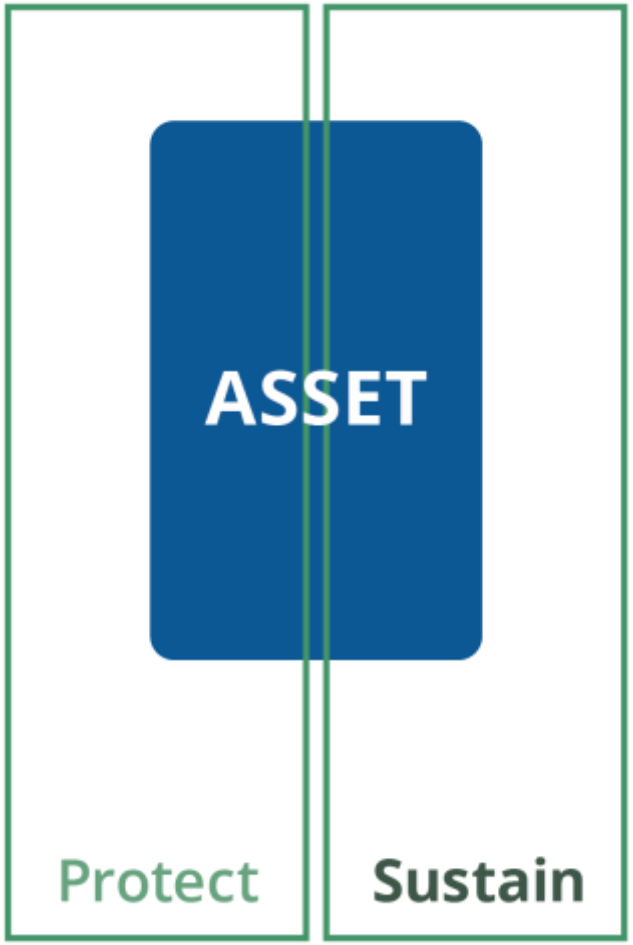
Relationships among assets have implications for resilience. Some assets are containers for others.

Information is the most embedded type of asset (i.e., resilience linked to technology, facilities, and people).

Operational Resilience Starts at the Asset Level



Protection Strategies

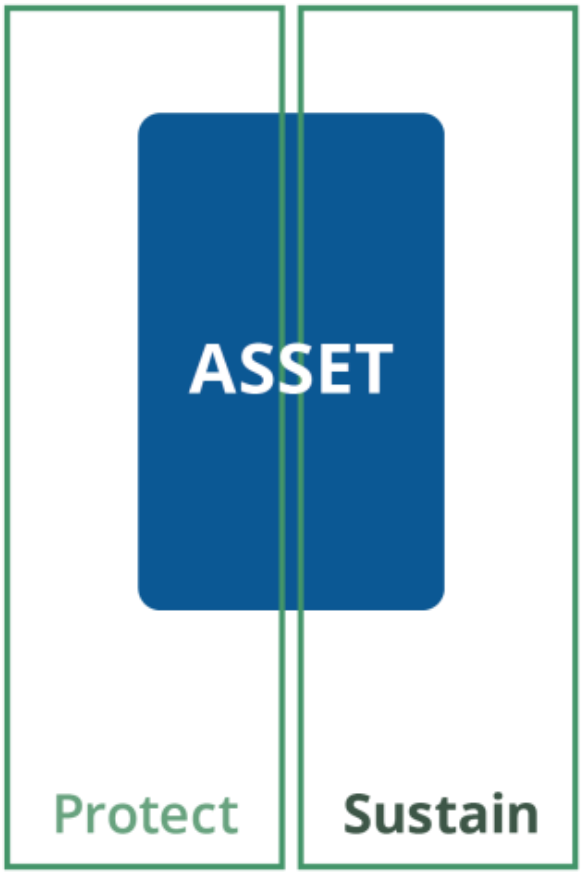


Translate into activities designed to keep assets from exposure to disruption

Typically **security** activities, but may also be embedded in IT operations activities

Instantiated through processes, procedures, policies, and controls

Sustainment Strategies



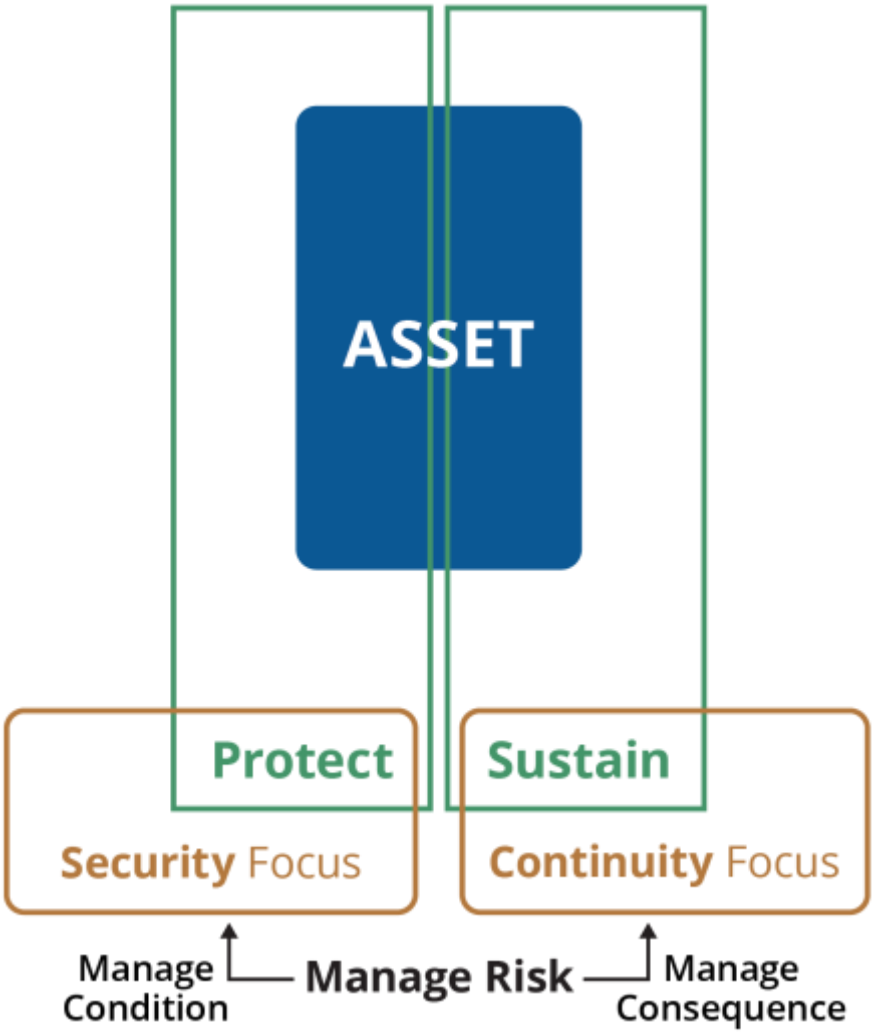
Translate into activities designed to keep assets productive during adversity

Keep an associated business process or service operable without the asset's contributions

Typically **business continuity** activities, but may also be embedded in IT operations activities

Instantiated through processes, procedures, policies, and controls

Efficiency

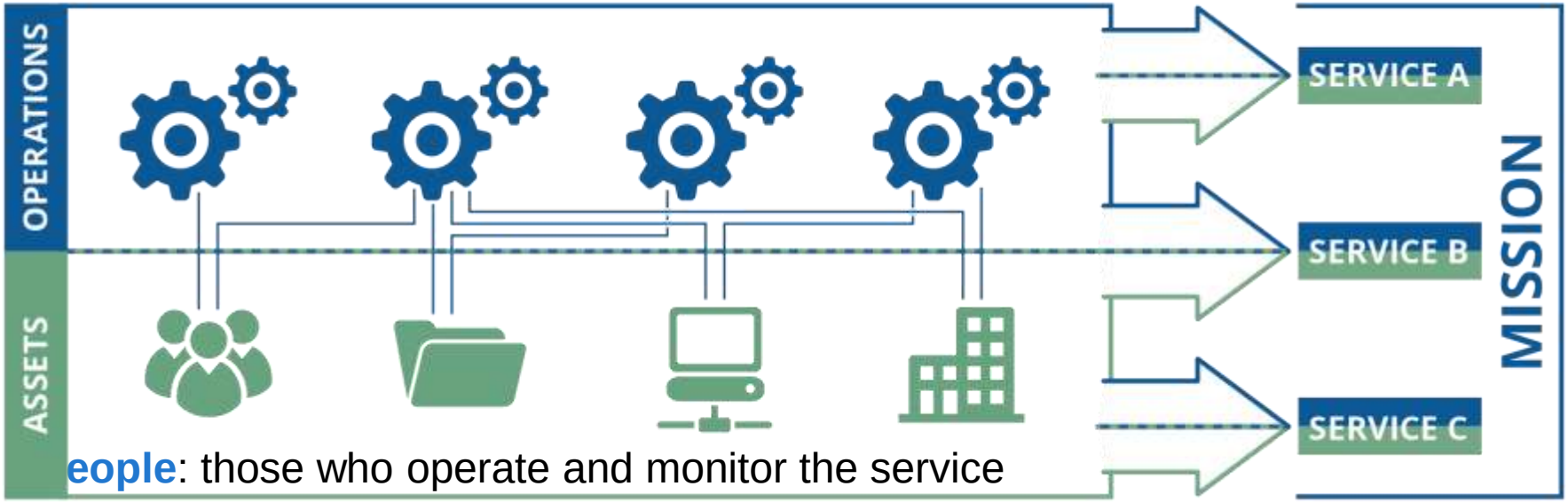


The optimal mix of protection and sustainment strategies

Depends on the **value** of the asset to the service and the **cost** of deploying and maintaining the strategy

The management challenge of operational resilience

Asset Support Services



eople: those who operate and monitor the service

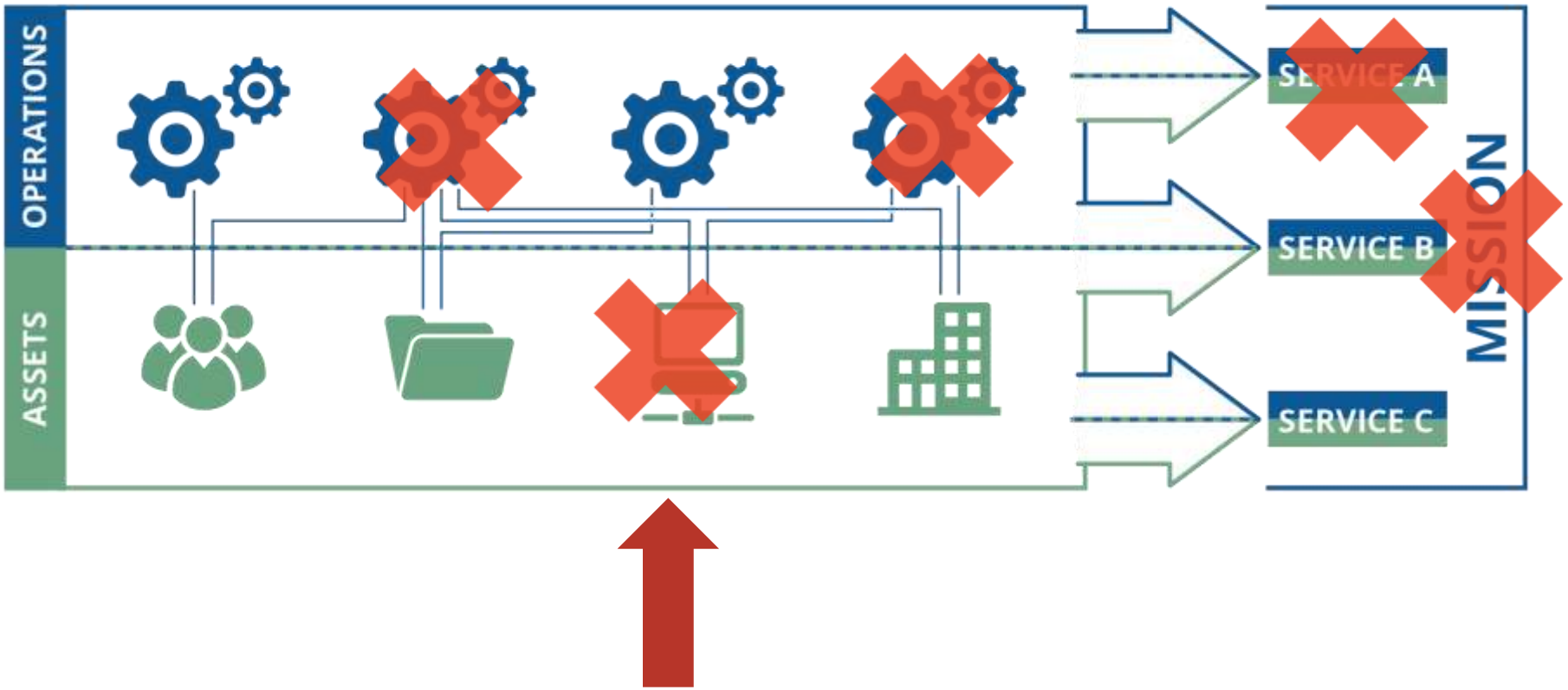
Information: data associated with the service

Technology: tools and equipment that automate and support the service

Facilities: where the service is performed

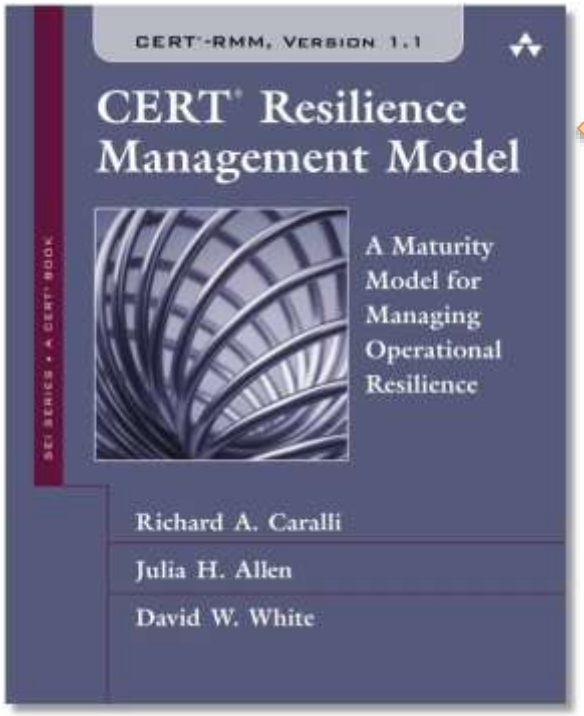
Assets derive their value from their importance in meeting the service mission.

Disruption of Assets Can Lead to Mission Failure



Realized operational risk resulting in asset disruption

CERT Resilience Management Model (CERT-RMM)



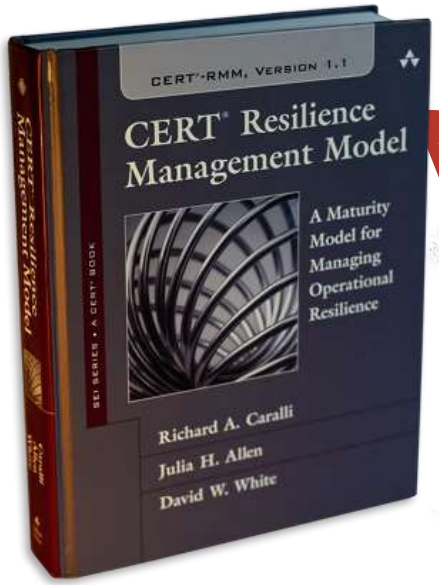
Framework for managing and improving operational resilience

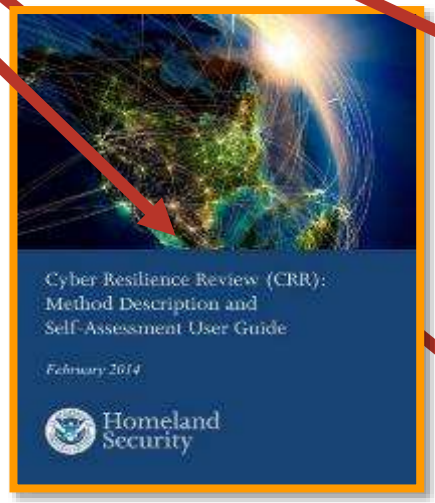
http://www.cert.org/resilience/

"…an extensive super-set of the things an organization could do to be more resilient."

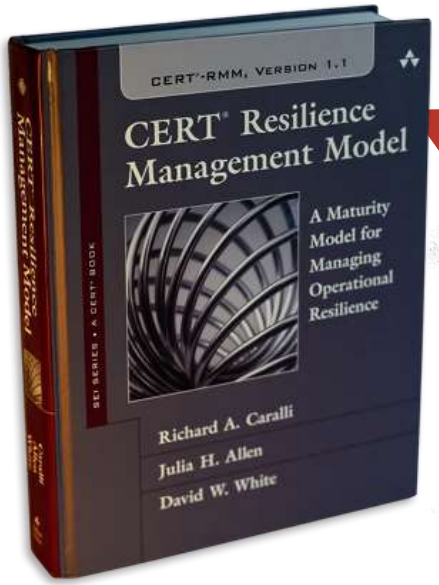
- CERT-RMM adopter

A Sampling of CERT-RMM Applications and Derivatives





Additional Success Stories for Department of Defense



Core Principle and Focus of CERT-RMM

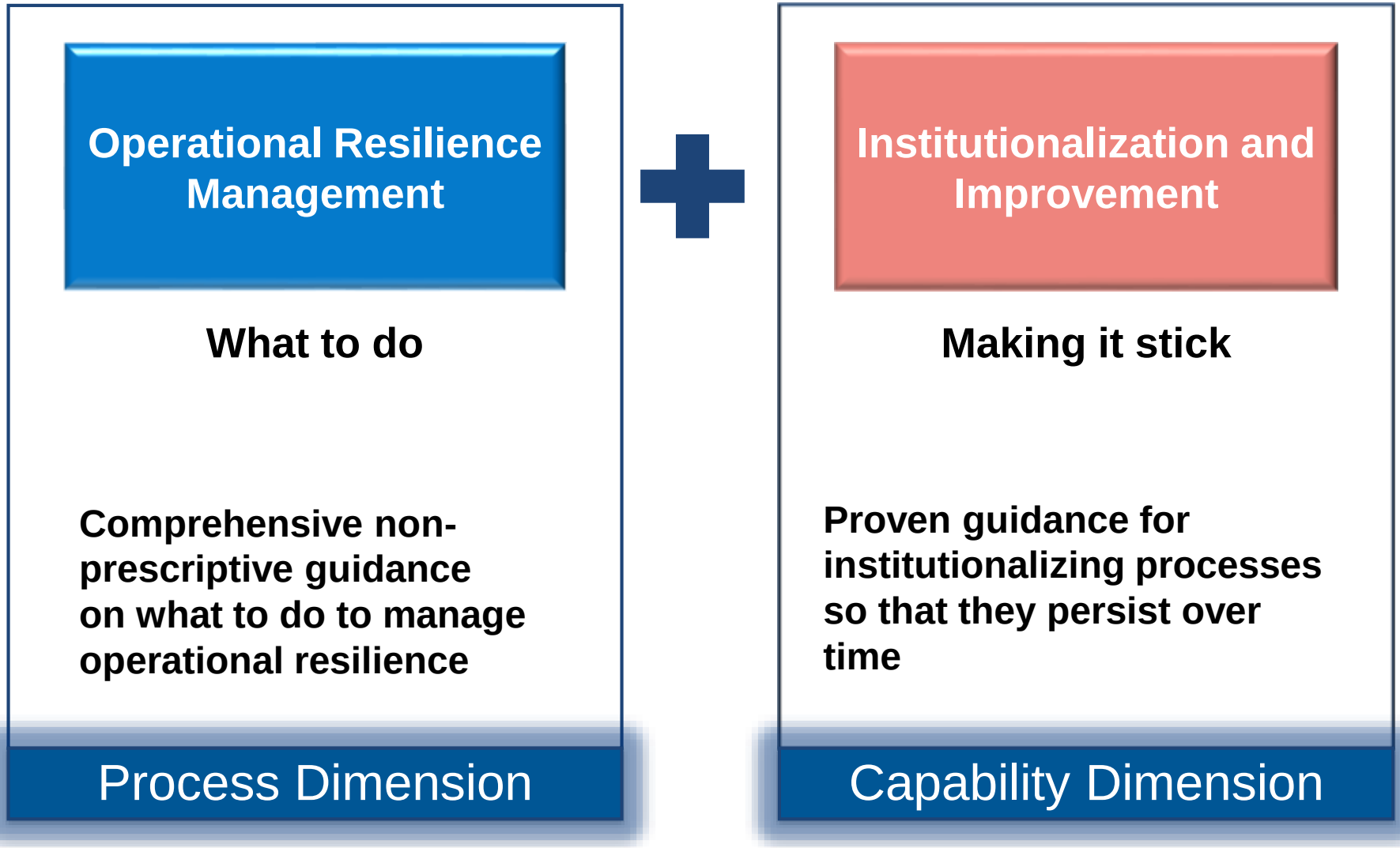
Premise at the core of CERT-RMM

The ability of the organization to sustain operations in the face of operational risk is highly influenced by the quality of the process used to ensure assets remain protected and sustained.

Focus of CERT-RMM

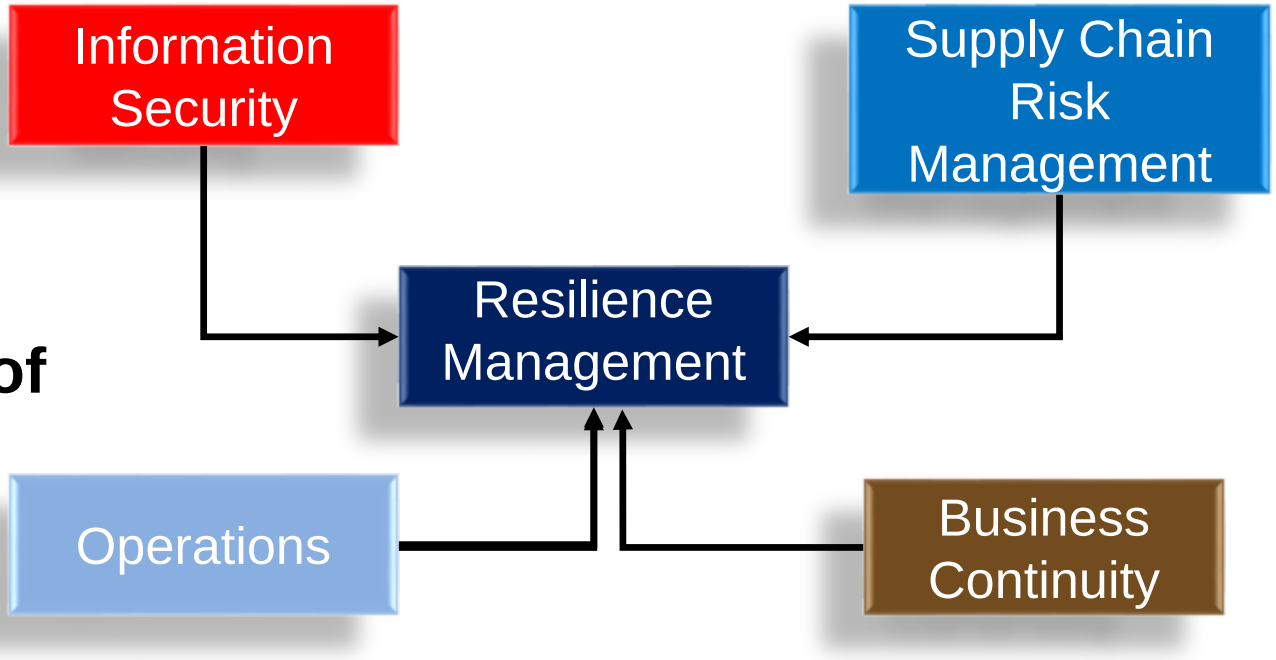
Transforming some (emergent) quality of the organization, called operational resilience, focuses on the processes or activities that support operational resilience management system.

CERT-RMM Approach

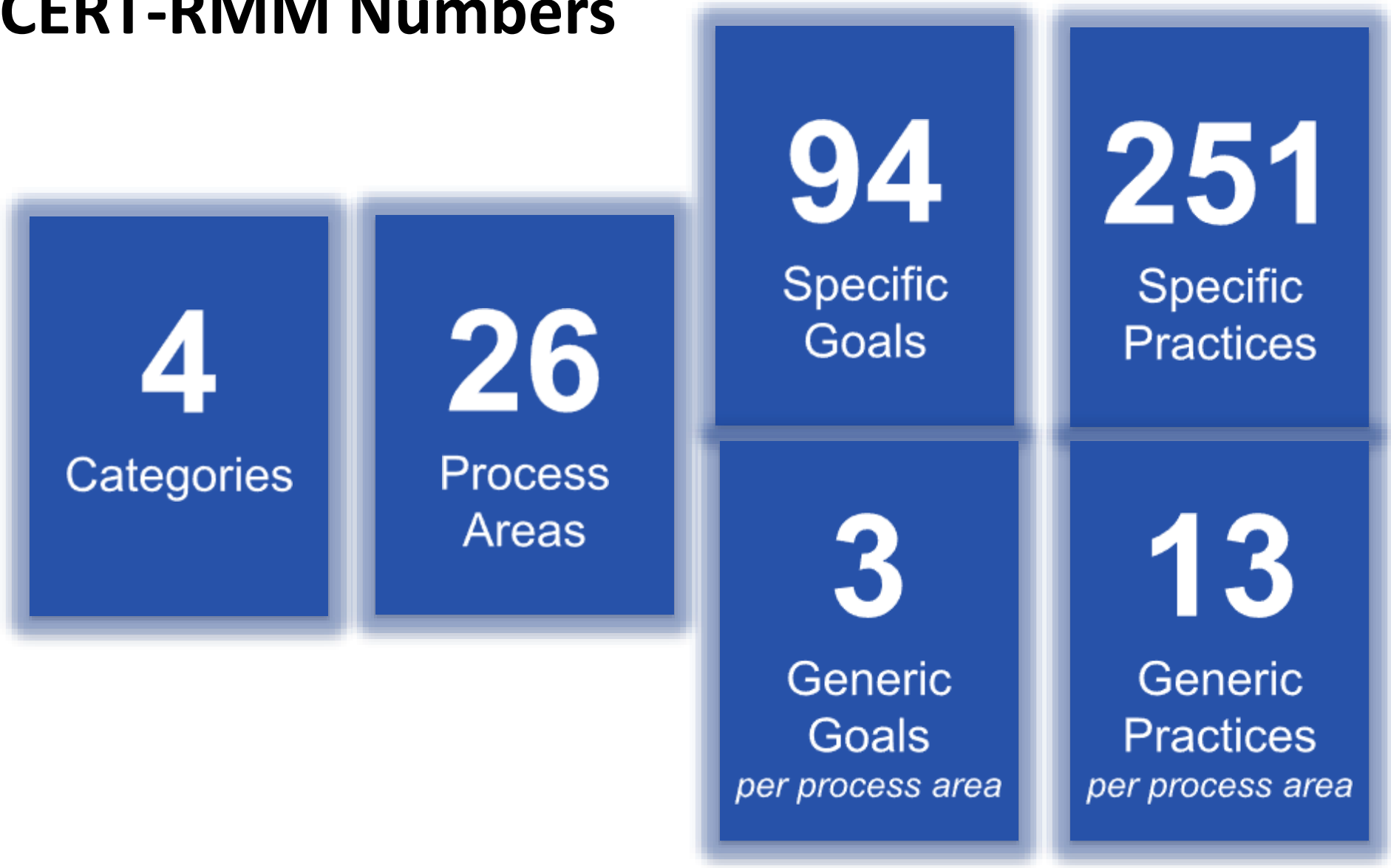


Convergence of Process

CERT-RMM facilitates and measures the convergence of disparate critical processes



CERT-RMM Numbers



26 Process Areas in 4 Categories

Engineering	
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management	
COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training and Awareness
RISK	Risk Management

Operations	
AM	Access Management
EC	Environmental Control
EXD	External Dependencies Management
ID	Identity Management
IMC	Incident Management and Control
KIM	Knowledge and Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis and Resolution

Process Management	
MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus

Example: Managing Cloud Computing

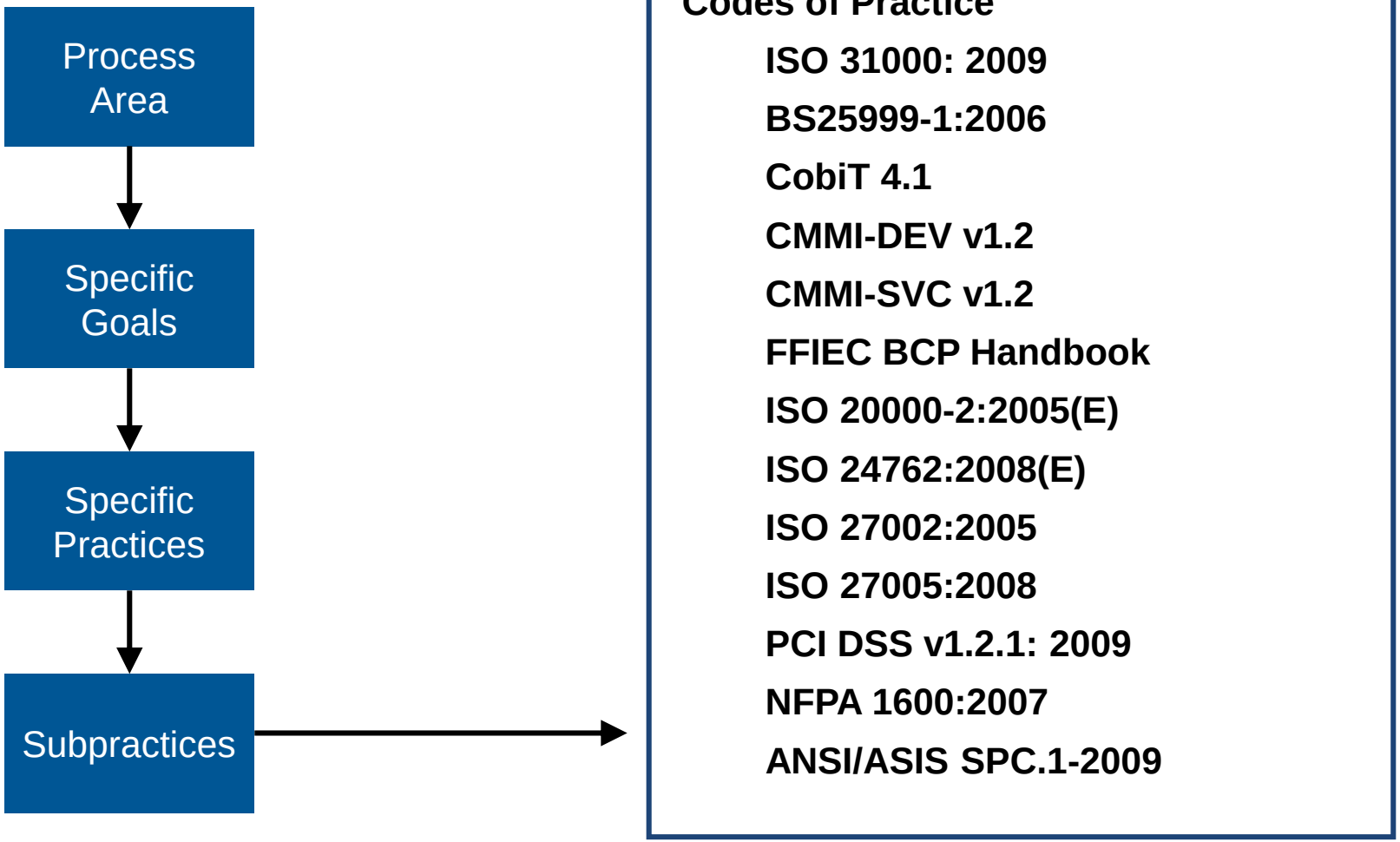
Engineering	
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management	
COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training and Awareness
RISK	Risk Management

Operations	
AM	Access Management
EC	Environmental Control
EXD	External Dependencies Management
ID	Identity Management
IMC	Incident Management and Control
KIM	Knowledge and Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis and Resolution

Process Management	
MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus

CERT-RMM Links to Codes of Practice



Resilience Management Overview

The Role of Risk Management

Risk Management Is a Lynchpin Activity

Enterprise (Governance)

- **Governance addresses risk from an enterprise perspective by developing a comprehensive governance structure and organization-wide risk management strategy.**

Service (Business Process)

- **A business process addresses risk from a service and business process perspective and is guided by the risk decisions at the enterprise level.**

Asset (Environment of Operations)

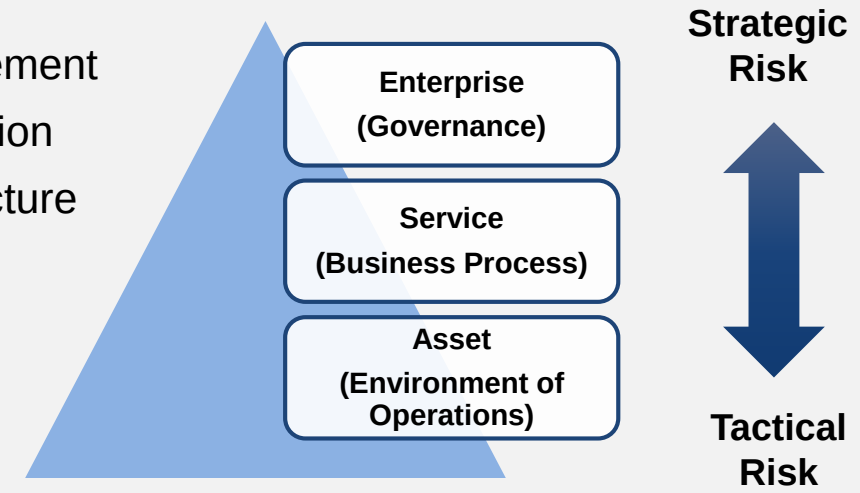
- **Risk decisions at the enterprise and service levels impact the ultimate selection and deployment of needed safeguards and countermeasures at the asset level.**

Risk Management Is a Team Sport

Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization:

- enterprise level
- service and business process level
- asset level

- multi-tier organization-wide risk management
- implemented by the risk executive function
- tightly coupled to the enterprise architecture and information security architecture
- system development life-cycle focus
- disciplined and structured process
- flexible and agile implementation



Outcomes of Risk Management

An understanding of

- the organization's threat, vulnerability, and risk profile
- risk exposure
- potential consequences of compromise
  - awareness of risk management priorities based on potential consequences

A risk mitigation strategy sufficient to achieve an acceptable level of residual risk

Organizational acceptance/transference based on an understanding of potential consequences of residual risk

Integration as "business as usual"

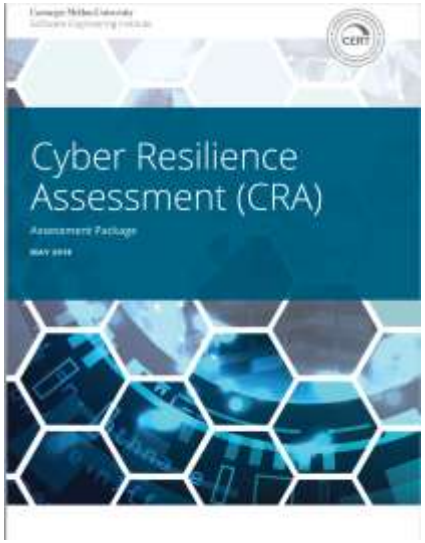
Compliance as a by-product

SEI's Approach to Mission Engineering and Mission Assurance

Cyber Resilience Assessment

Architecture Assessment

Cyber Resilience Assessment (CRA)



Purpose: Help organizations assess their operational resilience and cybersecurity practices:

- as it relates to a specific critical service
- across ten foundational cybersecurity domains
- based on the organization's unique risk profile

Delivery: The CRA is *facilitated* by SEI cybersecurity professionals

Output: The CRA provides an organization with a report detailing its capability and maturity in security management. The CRA also allows an organization to compare its capabilities to the criteria of the NIST Cybersecurity Framework (CSF)

Overview of the CRA

The CRA is a structured assessment conducted during a **one-day facilitated session**.

The CRA session is facilitated by multiple SEI Navigators who solicit answers to **297 questions**.

The CRA results are made available in a **summary report** that provides the organization with suggested **options for consideration**.

Cyber Resilience Assessment - Domains

Asset Management
Controls Management
Configuration and Change Management
Incident Management
Vulnerability Management
Risk Management
Service Continuity Management
External Dependency Management
Training and Awareness
Situational Awareness

Cyber Resilience Assessment (CRA)

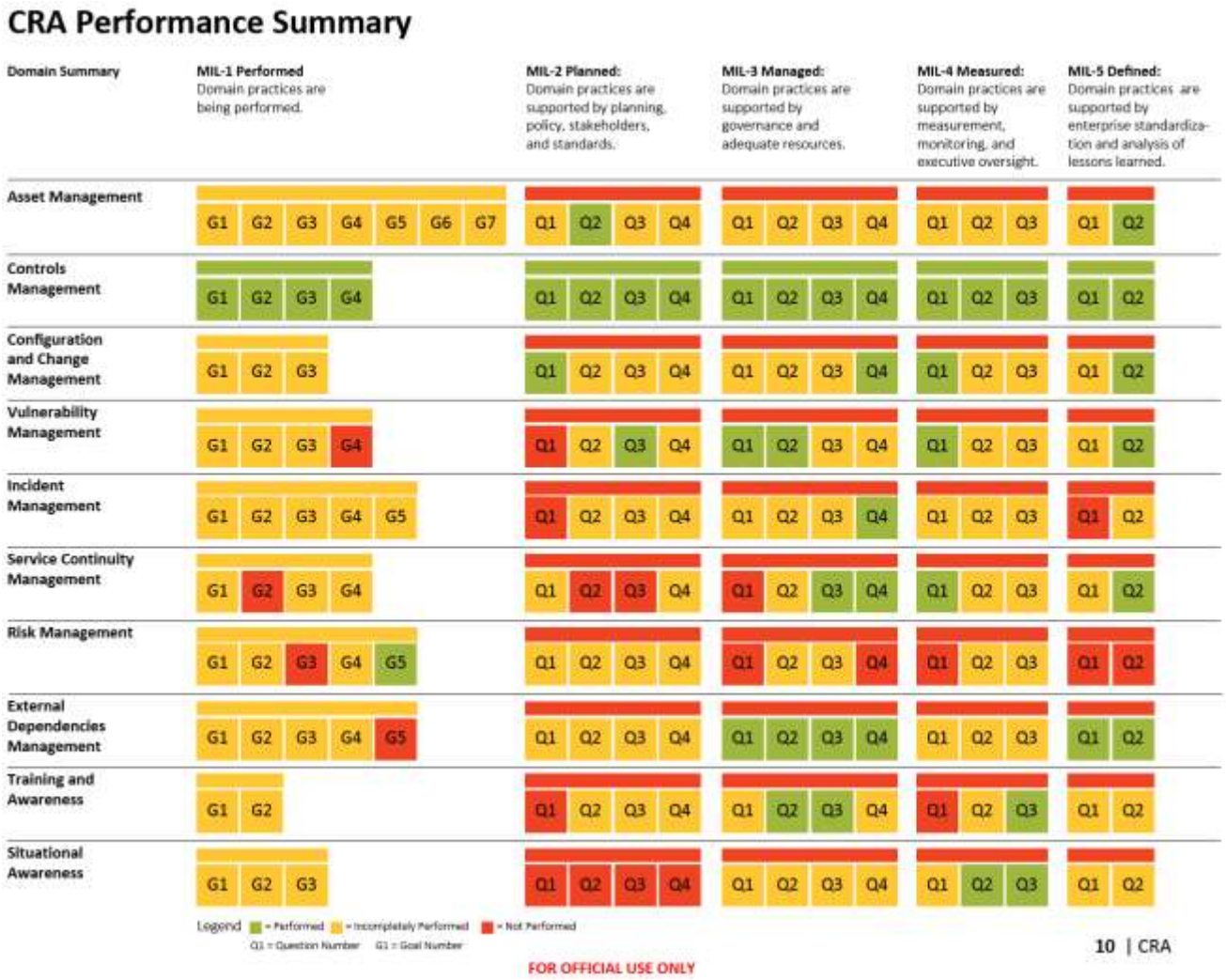
1 Asset Management

The purpose of Asset Management is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services.

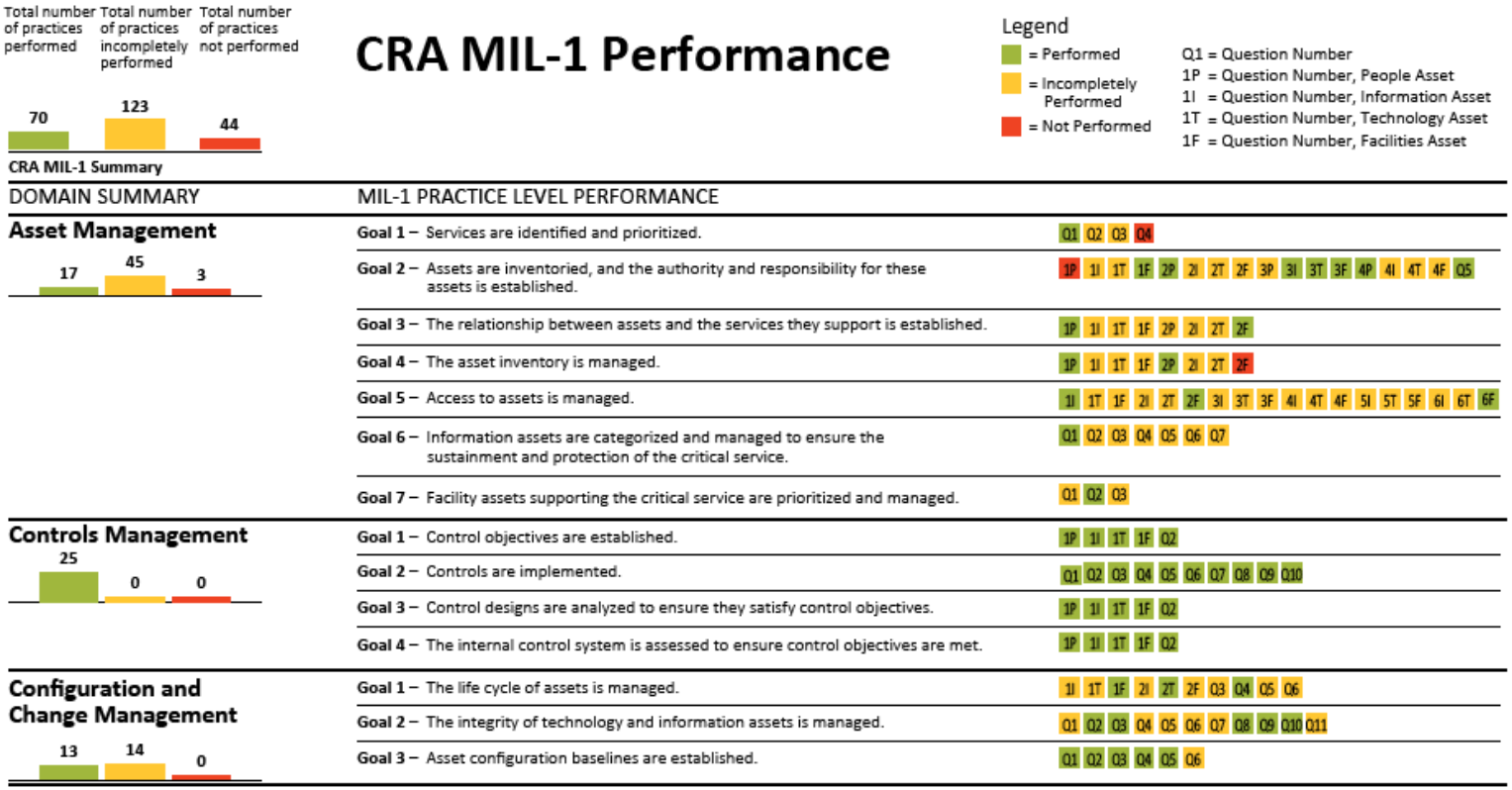
Goal 1 - Services are identified and prioritized.	Yes	Incomplete	No
1. Are services identified? [SC:SG2.SP1]	☐	☐	☐
2. Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	☐	☐	☐
3. Is the organization's mission, vision, values and purpose, including the organization's place in critical infrastructure, identified, and communicated? [EF:SG1.SP1]	☐	☐	☐
4. Are the organization's mission, objectives, and activities prioritized? [EF:SG1.SP3]	☐	☐	☐

Goal 2 - Assets are inventoried, and the authority and responsibility for these assets is established.	Yes	Incomplete	No
1. Are the assets that directly support the critical service inventoried (technology includes hardware, software, and external information systems)? [ADM:SG1.SP1]			
People	☐	☐	☐
Information	☐	☐	☐
Technology	☐	☐	☐
Facilities	☐	☐	☐
2. Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2]			
People	☐	☐	☐
Information	☐	☐	☐
Technology	☐	☐	☐
Facilities	☐	☐	☐

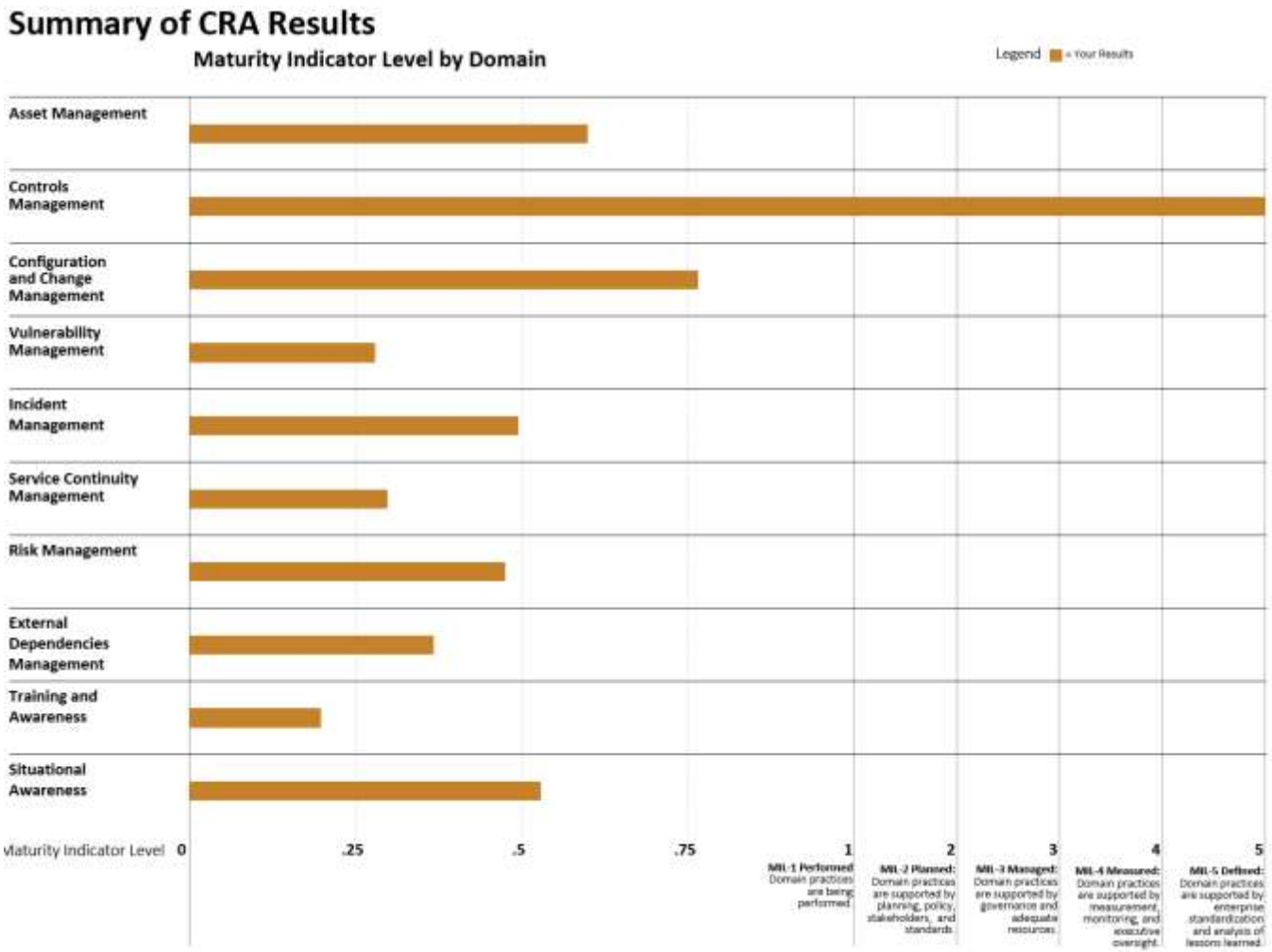
Cyber Resilience Assessment (CRA)



Cyber Resilience Assessment (CRA)



Cyber Resilience Assessment (CRA)



SEI's Approach to Mission Engineering and Mission Assurance

Security Architecture Assessment

Summary

- In collaboration with the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA), SEI developed a methodology to assess the cybersecurity architecture of Federal Civilian Enterprise (FCE) High Value Assets (HVAs)

- SEI personnel performed as Technical Leads for more than 120 Security Architecture Reviews and High Value Asset Assessments in support of the Office of Management and Budget (OMB) / DHS HVA Program

Assessment Methodology

Overview

- Holistic view of the security of a sensitive or mission-critical system
- Conducted utilizing the methods defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A:
  - Examine: The examine method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects. (Document or Configuration Review)
  - Interview: The interview method is the process of holding discussions with individuals or groups of individuals within an organization (Technical Exchange Meetings)
  - Test: The test method is the process of exercising one or more assessment objects under specified conditions to verify and validate conformity or nonconformity with a requirement. (Penetration Tests)
- Security Controls assessment utilizing the High Value Asset (HVA) Overlay
  - NIST SP 800-53r5 Security Controls
  - Specific requirements/parameters required for HVAs

Assessment Methodology
Domains

- Network-Based Protections
- Identity and Access Management
- Application Security
- System-Based Protections
- Service Continuity
- Risk Management
- Incident Management
- Continuous Monitoring
- Data Security
- Enterprise Processes and Capabilities
- Penetration Tests

Assessment Methodology
Enhancements

- Incident Response Evaluations
- Specific Threat Scenarios
- Threat Modeling
- Reference Architectures

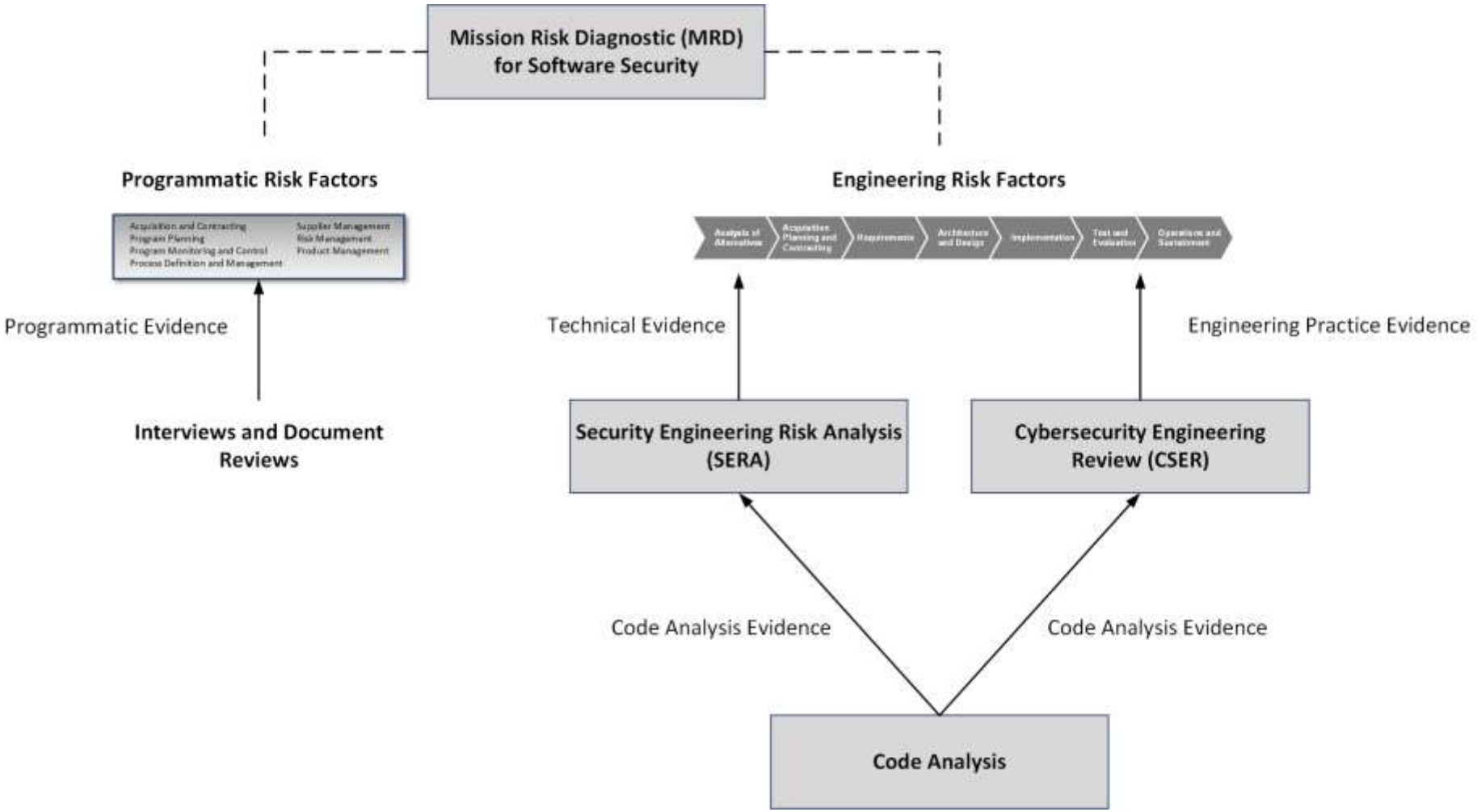
Assessment Results

- Business Impact Analysis
- Key Observations
- Risks
- Recommendations
- High Value Asset (HVA) Overlay Analysis
- Penetration Test Findings

SEI's Approach to Mission Engineering and Mission Assurance

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.

Operational Resilience Key Points

Operational Resilience is a critical element that minimizes disruption in times of peril.

- CERT RMM is predictive of future behaviors despite disruptive events based upon its measures of maturity
- CERT RMM has proven itself with a diverse set of derivatives in a broad customer set
- CERT RMM can be leveraged by any organization, regardless of its current degree of maturity

The Cyber Resilience Assessment (CRA) and Security Architecture Assessment (SAA) gages overall resilience measures across a variety of high value assets.

Questions Concerning Build Security In?

Chris Alberts

Principle Cyber Security Analyst

Telephone: +1 412.268.3045

Email: cja@cert.org

Carol Woody

Principal Researcher

Telephone: +1 412.770.5133

Email: cwoody@sei.cmu.edu

Tim Morrow

Technical Manager, Situational Awareness

Telephone: +1 412.268.4792

Email: tbm@sei.cmu.edu

Questions Concerning Operational Resilience?

Jason Fricke

Senior Cybersecurity Engineer

Telephone: +1 571.423.9600

Email: jfricke@cert.org

Brett Tucker, PMP, CSSBB, CISSP

Technical Manager, Cyber Risk Management

Telephone: +1 412.268.6682

Email: batucker@sei.cmu.edu

Questions Concerning Business Development?

Frank Redner

Program Development Manager

Telephone: +1 703.247.1347

Email: fredner@sei.cmu.edu