Security Engineering Risk Analysis (SERA) Tutorial

Cybersecurity Engineering (CSE) Team

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.

DM19-0110

SERA Tutorial: *Topics*

Cybersecurity Engineering

Risk Management Concepts

SERA Method Overview

Establish Operational Context (Task 1)

Identify Risk (Task 2)

Analyze Risk (Task 3)

Develop Control Plan (Task 4)

Summary

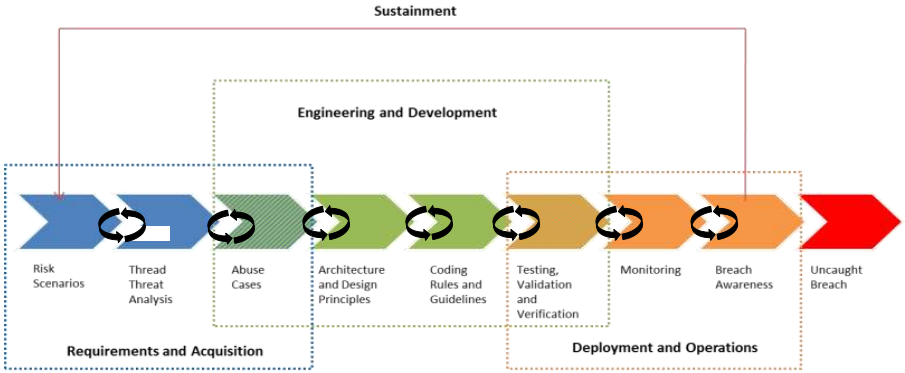
Security Engineering Risk Analysis (SERA) Tutorial

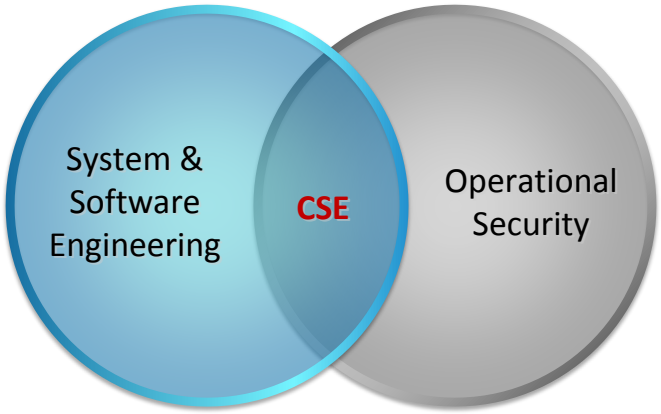
Cybersecurity Engineering

Cybersecurity Engineering

Mission: Build Security In

Address security, software assurance, and survivability throughout the development and acquisition lifecycle by creating methods, solutions, and training that can be integrated into existing practices.

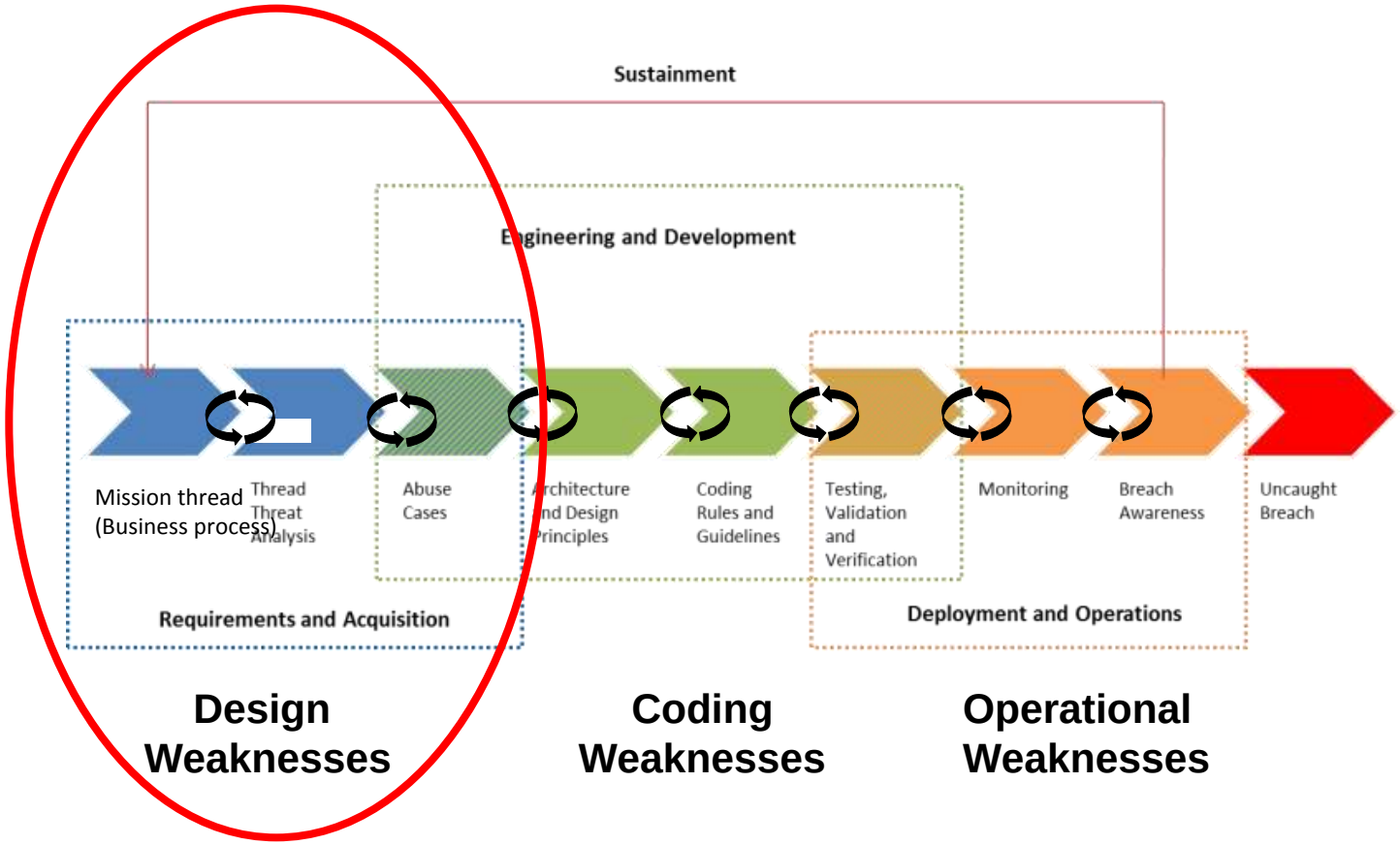




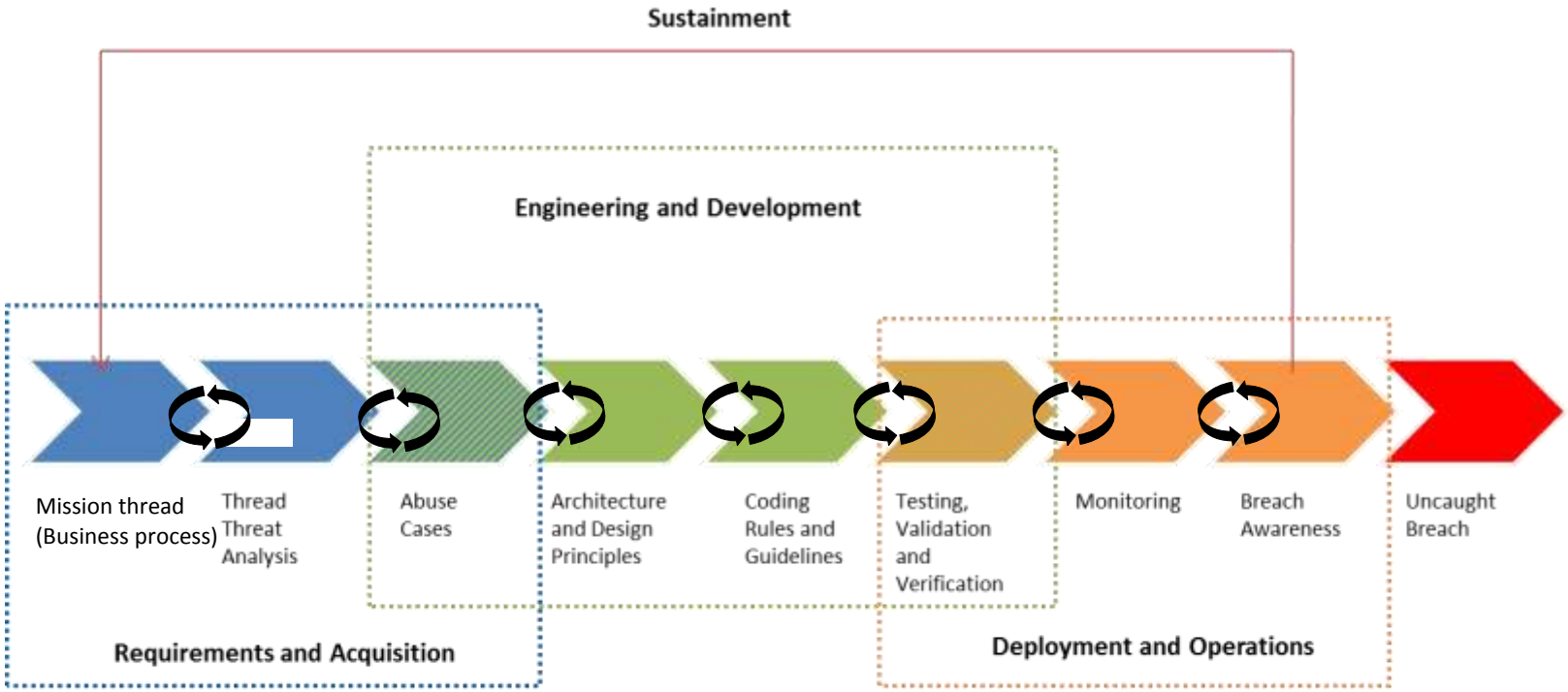
Current Focus Areas

- Software Assurance Education and Competencies
- Software Assurance Management and Measurement
- Cybersecurity and Software Assurance Lifecycle Integration

Emphasizing Cybersecurity Early in the Lifecycle



Cybersecurity Is a Lifecycle Challenge



Design and Coding Weaknesses

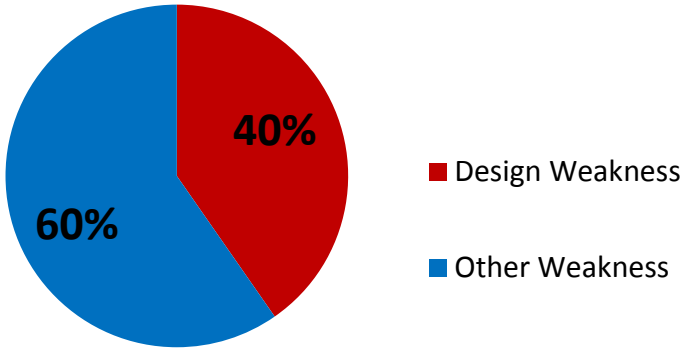
940 Common Weakness Enumerations (CWEs)

Operational Weaknesses

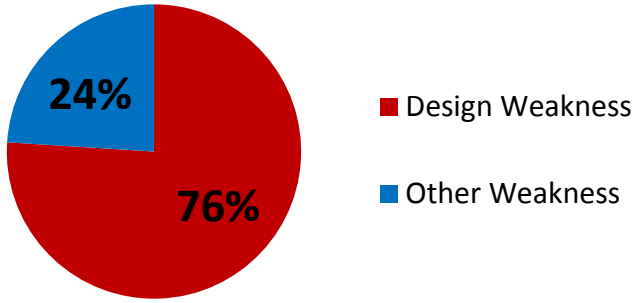
72,576 Common Vulnerability and Exposures (CVEs)

Criticality of Early Lifecycle Cybersecurity Practices

940 Total CWEs*



Top 25 CWEs
(Most Dangerous)

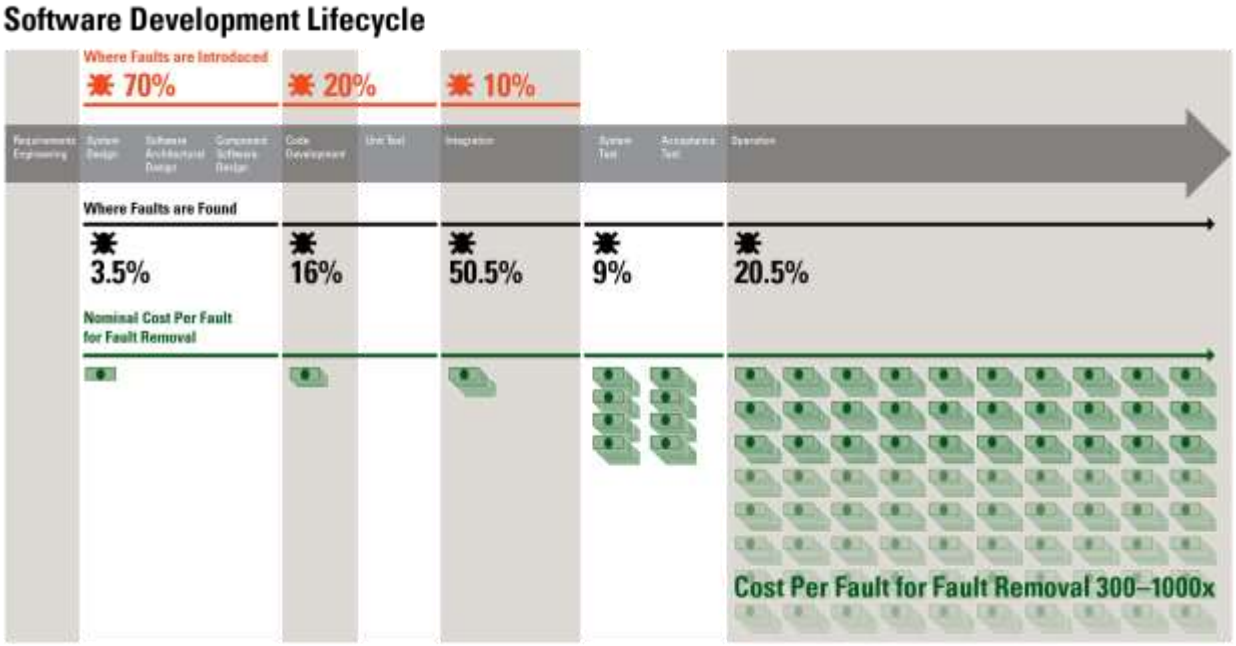


Source: MITRE CWE web pages as of Feb 9, 2014

Causes for software design weaknesses:

- Poor software security requirements
- Limited understanding of the impact of software security risk on mission success

Catching Software Faults Early Saves Money



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

Faults account for 30–50% percent of total software project costs.

Systems Engineering View

Each system is assumed to be self-sufficient.

A focus on reliability and quality is assumed to be sufficient for systems engineering and development.

Security requirements are

- Selected based on system concerns for confidentiality, integrity, and availability (CIA) or mandated compliance
- Assigned to components through system engineering decomposition

System components are assumed to be independent with well-controlled interfaces.

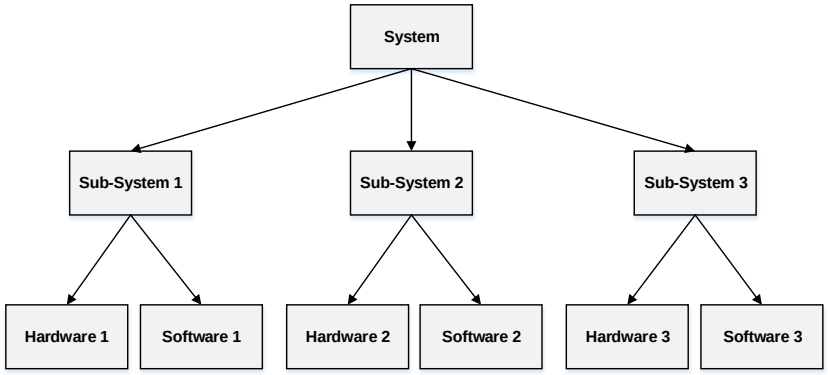
Software is viewed as just being part of each system component.

INCOSE. 2015. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, version 4.0. Hoboken, NJ, USA: John Wiley and Sons, Inc, ISBN: 978-1-118-99940-0

System Engineering versus Software Engineering

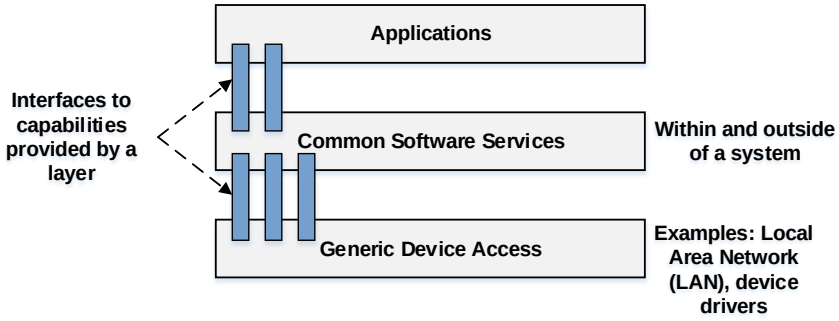
Systems Engineering Assumptions

- Systems can be decomposed into discrete, independent, and hierarchically related components (or subsystems)
- **Is part of:** Components can be constructed and integrated with minimal effort based on the original decomposition
- **Quality properties can be allocated to specific components**



Software Engineering Realities

- Software components are often related sets of layered functionality (one layer is *not* contained inside another layer)
- **Is used by:** Interactions of the components (*not* the decomposition) must be managed
- **Security properties relate to composite interactions (*not* to individual components)**



Source: INCOSE System Engineering Handbook

Role of Software has Changed

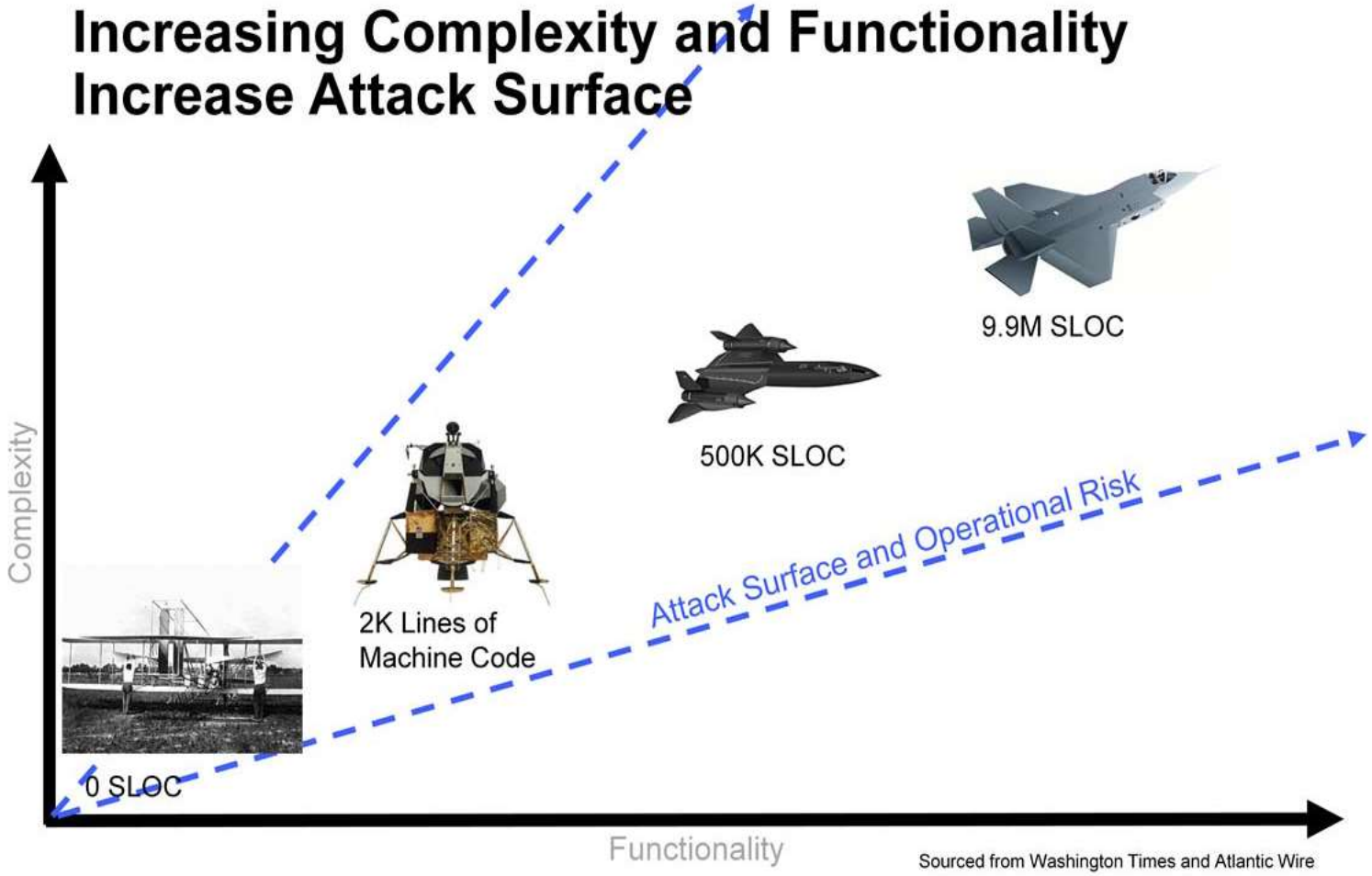
From the National Research Council (NRC) Critical Code Report[1]

"Software has become essential to all aspects of military system capabilities and operations" p.19

- 1960 – 8% of the F-4 aircraft functionality
- 1982 – 45% of the F16 aircraft functionality
- 2000 – 80% of the F-22 aircraft functionality

1. Committee for Advancing Software-Intensive Systems Producibility; National Research Council (NRC). *Critical Code: Software Producibility for Defense,* 2010.

Increasing Complexity and Functionality Increase Attack Surface



Security Principles

Principles of security were defined by Saltzer and Schroeder in their paper titled “The Protection of Information in Computer Systems” published in Communications of the ACM, 1974

Security is defined as

> “techniques that control who may use or modify the computer or the information contained in it”

Three main categories of concern:

> confidentiality, integrity, and availability (CIA)

Technology Environment has Changed

In 1974:

- S360 in use from 1964-1978; S370 came on market in 1972
- COBOL & BAL programming languages
- MVS operating system released in March 1974
- Patches were carefully tested to minimize operational disruption

Changes since 1974:

- Internet; Morris worm – November 2, 1988
- 50,000+ software vulnerabilities and exposures (CVE)
- Java, C++, C#
- Mobile and Cloud computing
- Patches are applied ASAP to minimize zero-day attacks

Standards Require New Approaches

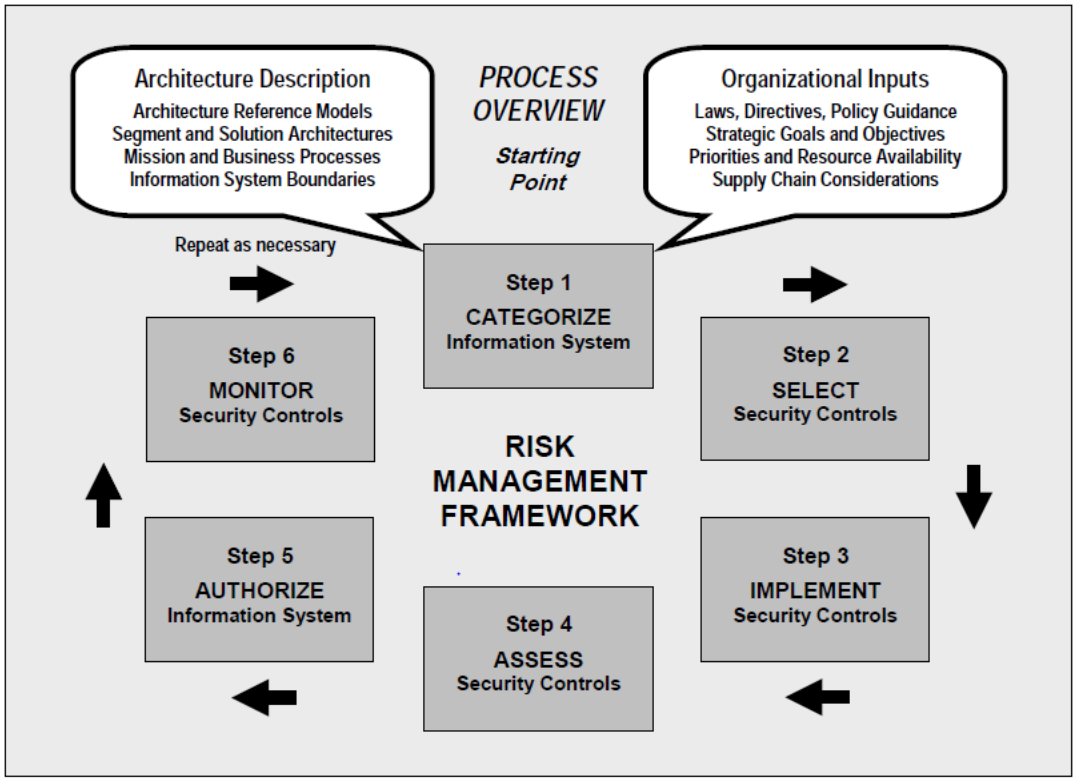
Recent Department of Defense (DoD) policy changes expand cybersecurity responsibility for engineering in the acquisition lifecycle.[1]

Replacing DIACAP[2] with the NIST Risk Management Framework (RMF) for Authority to Operate (ATO)[3] has pushed traditional evaluation approaches beyond their limits.

1. Department of Defense (DoD). *Operation of the Defense Acquisition System*. DoD Instruction 5000.02. February 2, 2017
2. Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP)
3. Department of Defense (DoD). *Cybersecurity*. DoD Instruction 8500.01. March 14, 2014

NIST Risk Management Framework (RMF)[1]

A DoD program's cybersecurity risk management practices must be consistent with the NIST RMF.

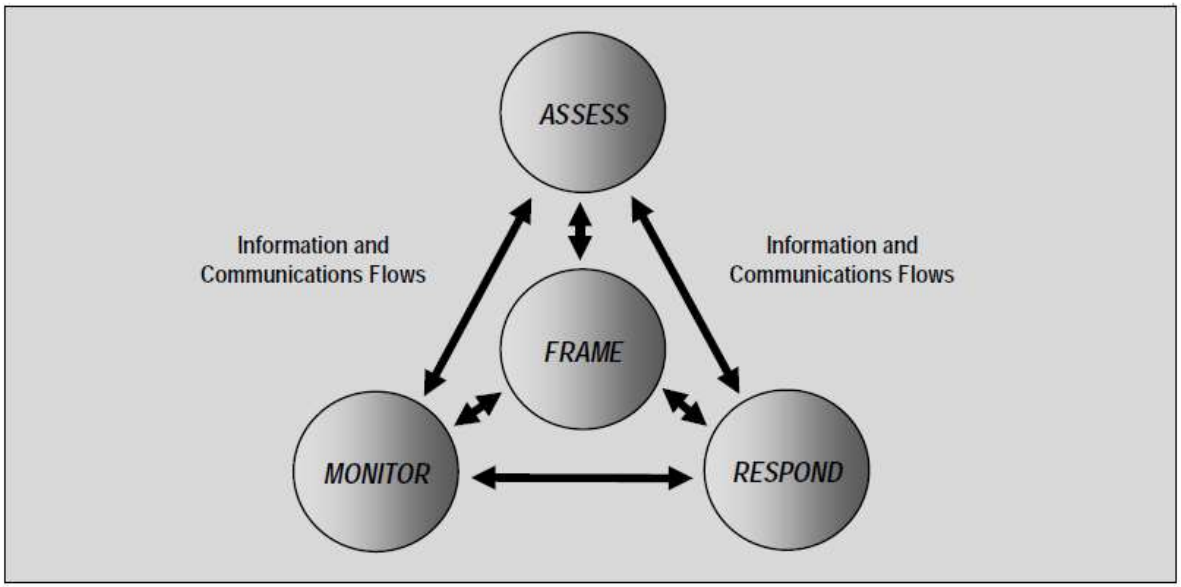


1. National Institute of Standards and Technology. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (NIST Special Publication 800-37 Revision 1). Gaithersburg, MD, National Institute of Standards and Technology, 2014.

NIST Risk Assessment Process[1]

NIST defines a general process for conducting risk assessments.

The NIST risk assessment process support a wide variety of program activities, including cybersecurity engineering.



1. National Institute of Standards and Technology. *Guide for Conducting Risk Assessments* (NIST Special Publication 800-30 Revision 1). Gaithersburg, MD, National Institute of Standards and Technology, 2012.

Security Engineering Risk Analysis (SERA) Tutorial

Risk Management Concepts

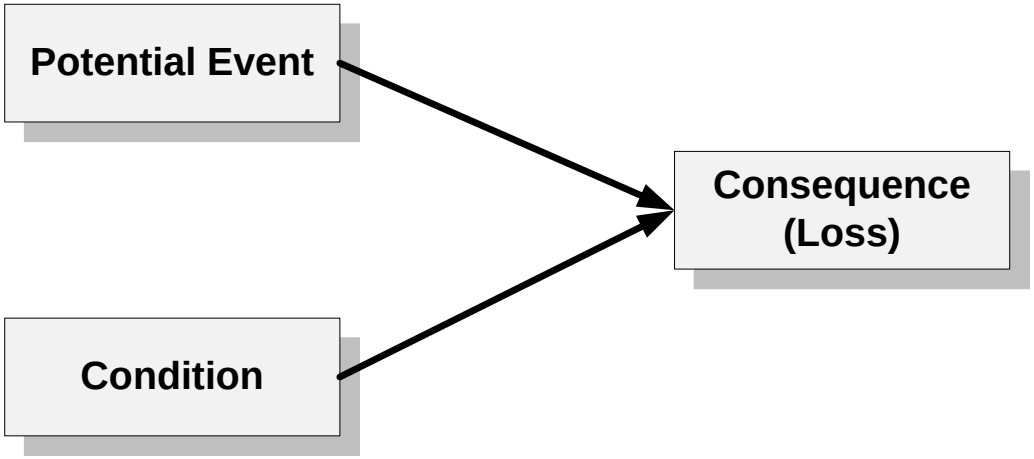
What Is Risk?

The probability of suffering harm or loss

A measure of the likelihood that an event will lead to a loss coupled with the magnitude of the loss

Risk requires the following conditions:[1]

- A potential loss
- Likelihood
- Choice



1. Charette, Robert N. *Application Strategies for Risk Analysis*. New York, NY: McGraw-Hill Book Company, 1990.

Risk Measures

Probability

- The likelihood that the event will occur

Impact

- The loss experienced when the event occurs

Risk exposure

- The magnitude of a risk based on current values of probability and impact

Timeframe (optional)

- The length of time before a risk is realized or the length of time in which action can be taken to prevent a risk

Risk Management

A systematic approach for minimizing exposure to potential losses.

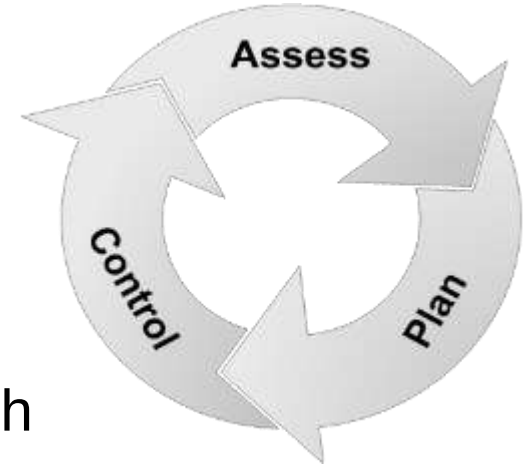
Risk management provides a disciplined environment for

- Continuously assessing what could go wrong (i.e., assessing risks)
- Determining which risks to address (i.e., setting mitigation priorities)
- Implementing actions to address high-priority risks and bring those risks within tolerance

Risk Management Activities

Assess risk

- Transform the concerns people have into distinct, tangible risks that are explicitly documented and analyzed.



Plan for controlling risk

- Determine an approach for addressing each risk; produce a plan for implementing the approach.

Control risk

- Deal with each risk by implementing its defined control plan and tracking the plan to completion.

Approaches for Controlling Risks

Accept—If a risk occurs, its consequences will be tolerated; no proactive action to address the risk will be taken. When a risk is accepted, the rationale for doing so is documented.

Control—Action is taken to handle a risk. Types of control actions include:

- *Transfer—*A risk is shifted to another party (e.g., through insurance or outsourcing).
- *Avoid—*Activities are restructured to eliminate the possibility of a risk occurring.
- *Mitigate—*Actions are implemented in an attempt to reduce or contain a risk.

Types of Risk Control Actions

Recognize and respond

- Monitor the event and take action when it is detected.

Resist

- Implement protection measures to reduce exposure to the event or minimize any consequences that might occur.

Recover

- Return to an acceptable state if the consequences or losses are realized.

Security Risk

Security risk is a measure of the

- Likelihood that a threat will exploit a vulnerability to produce an adverse consequence, or loss
- Magnitude of the loss

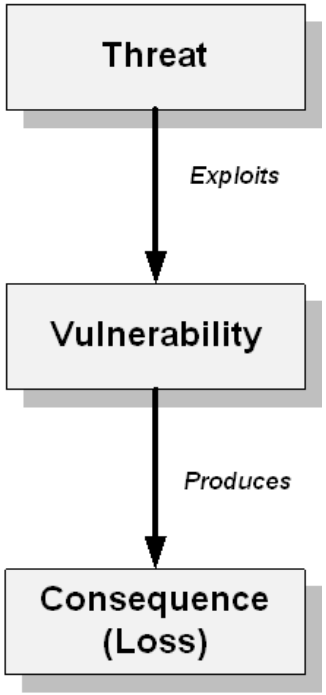
Three Components of Security Risk

Threat

- A cyber-based act, occurrence, or event that exploits one or more vulnerabilities and leads to an adverse consequence or loss

Vulnerability

- A weakness in an information system, system security procedures, internal controls or implementation that a threat could exploit to produce an adverse consequence or loss; a current condition that leads to or enables security risk



Consequence

- The loss that results when a threat exploits one or more vulnerabilities; the loss is measured in relation to the status quo (i.e., current state)

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.

WEA Service: *Participants*

Initiator

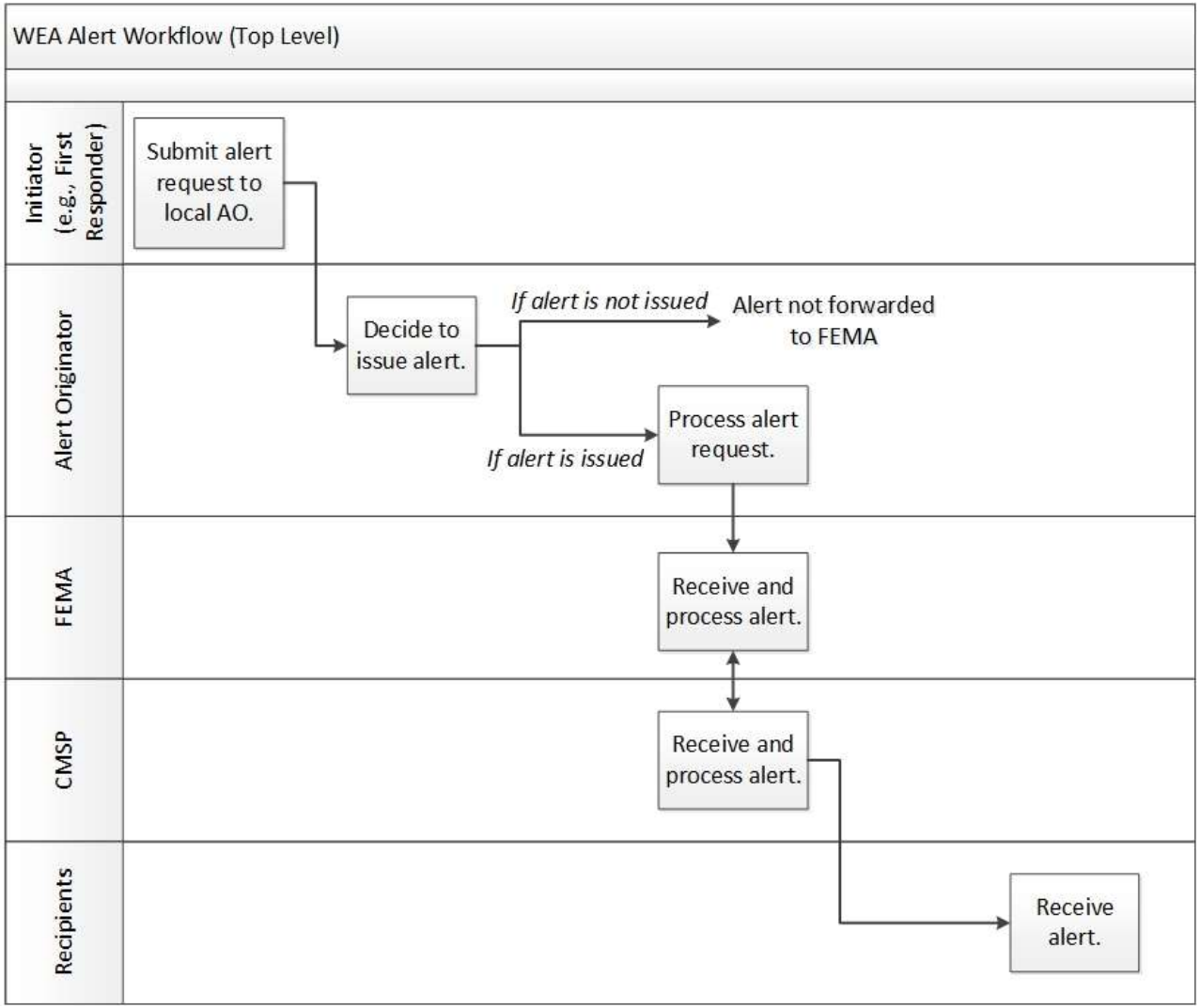
Alert Originator

Federal Emergency Management Agency (FEMA)

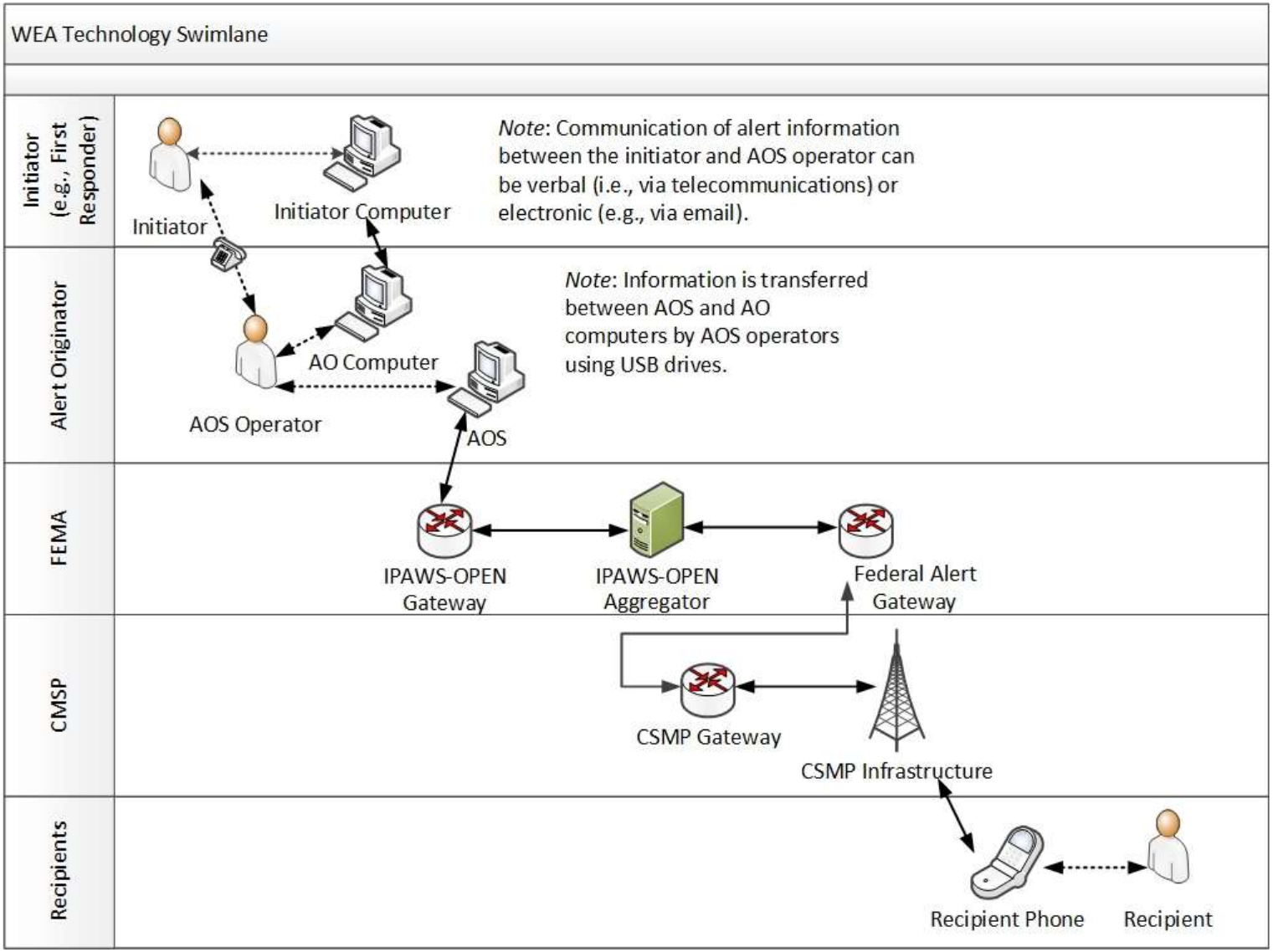
Commercial Mobile Service Provider (CMSP)

Recipients

WEA Workflow



WEA System of Systems



Tutorial Examples and Exercises

All examples and exercises presented in this tutorial are based on the WEA service.

- Examples focus on commercial mobile service providers (CMSPs).
- Exercises focus on Alert Originators (AOs)

Exercise 1: *Program Security Risks*

Turn to Exercise 1 in the tutorial workbook.

Read the overviews provided for

- Wireless Emergency Alerts (WEA) Service
- Pleasant Suburbs Scenario

Answer the following questions:

- What are the security risks in this scenario? Why?

Security Engineering Risk Analysis (SERA) Tutorial

SERA Method Overview

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)

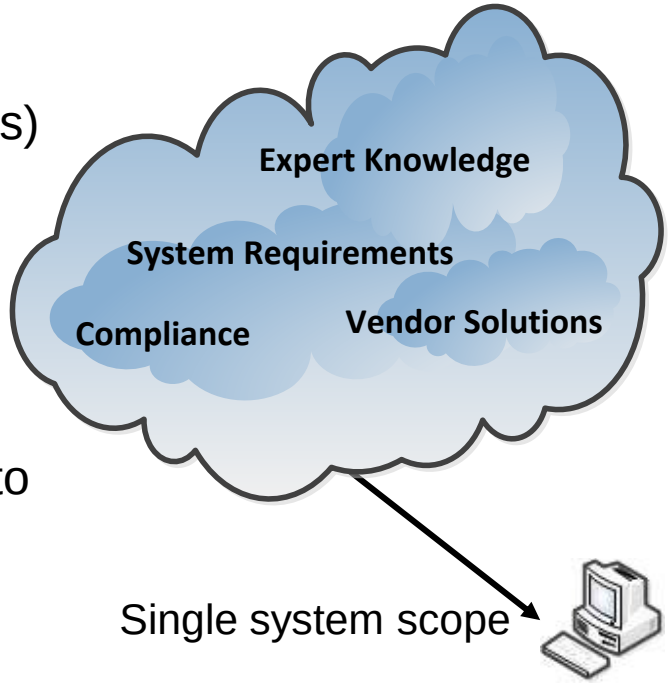
Limitations of Traditional Software Security Risk Analysis

Simplistic risk analysis

- Single actor, single system, single vulnerability
- Simple expression of risk (i.e., cause-effect pairs)
- Management focused, not engineering focused

Ad hoc risk analysis

- Based on tacit understanding of operational context
- Lack of results traceability (e.g., linking threats to vulnerabilities to controls)



- **System and software engineers and acquisition experts need to include software security expertise in early lifecycle activities (e.g., requirements development)**
- **Attacks frequently come from other trusted systems**
- **Complex attacks need to be included in a software-security risk evaluation**

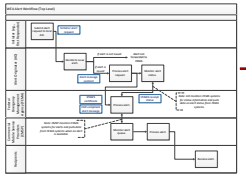
SERA Method: *Security Risk Scenarios*

Outcomes

- **Data disclosure (Confidentiality)**
- **Data modification (Integrity)**
- **Insertion of false data (Integrity)**
- **Destruction of data (Availability)**
- **Interruption of access to data (Availability)**

Affects

Workflow / Mission Thread

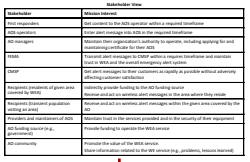


Produces

Adverse Mission Consequences / Losses

Affects

Stakeholder Interests

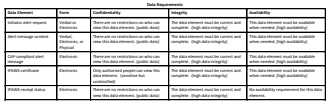


Produces

Adverse Stakeholder Consequences / Losses

Produces

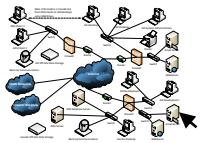
Mission Data



Targets

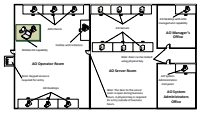
Technology Environment

Technology Infrastructure



Use Cases

Facilities



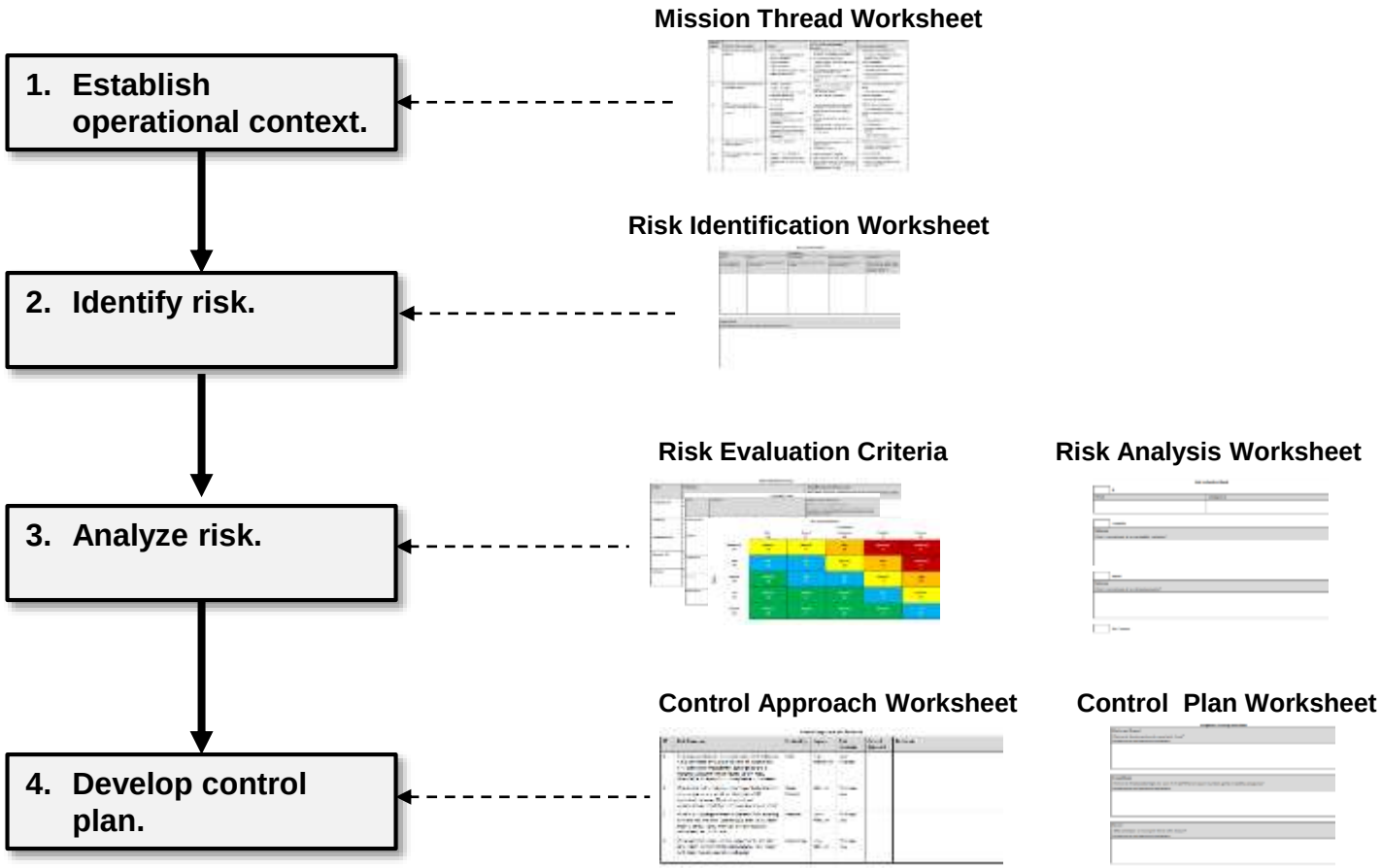
Entity of Interest

Exploits weaknesses and vulnerabilities

Threat Actor

SERA requires the development of security risk scenarios to analyze the mission impact of data security breaches.

SERA Method: *Four Tasks*



SERA Method: *Analysis Team*

An analysis team is

- A small team of approximately three to five people responsible for applying the SERA Method and reporting findings to stakeholders
- An interdisciplinary team that requires team members with diverse skill sets, such as
  - Cybersecurity risk analysis
  - Systems engineering
  - Software engineering
  - Operational cybersecurity
  - Physical/facility security

The exact composition of an Analysis Team depends on the

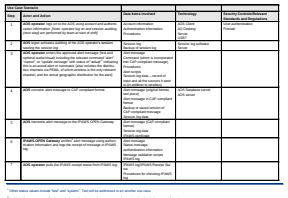
- Point in the lifecycle where the SERA Method is being applied
- Nature of the engineering activity being pursued

SERA Method: *Developing Security Risk Scenarios*

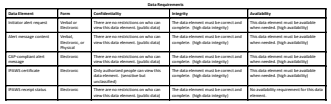
Threat Identification Models

Consequence Analysis Models

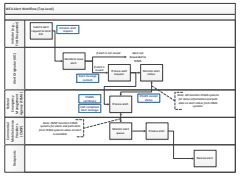
Use-Case View



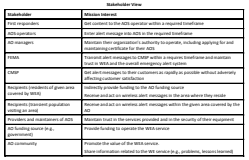
Data View



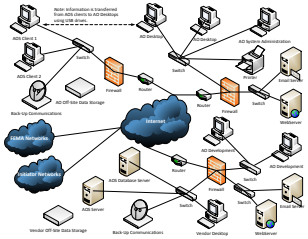
Workflow View



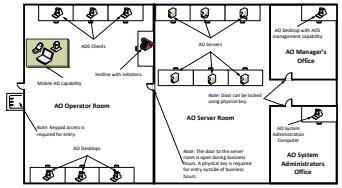
Stakeholder View

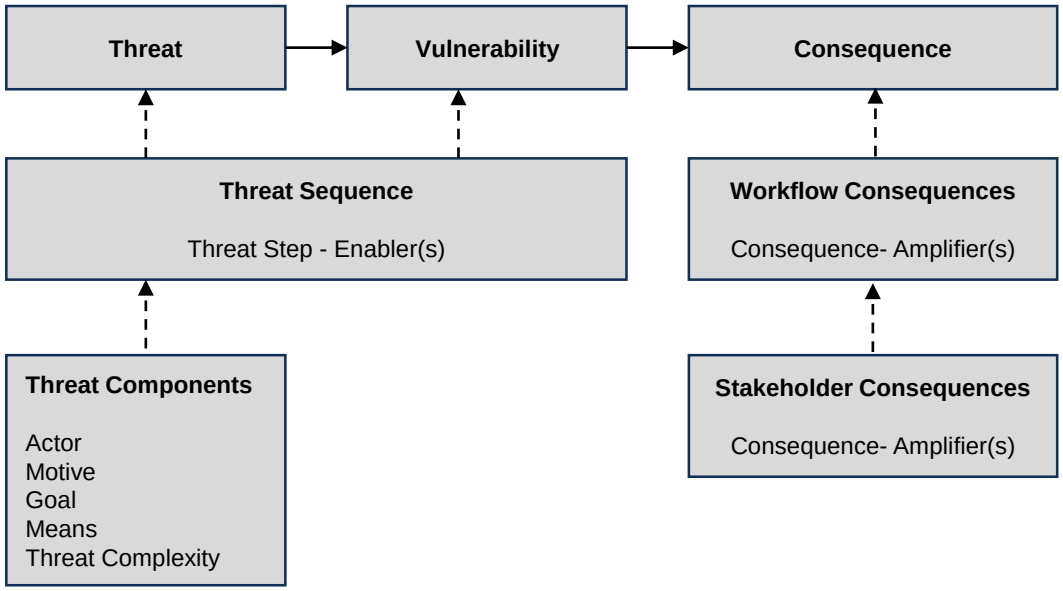


Technology View



Physical View





SERA Differentiators

Operational modeling (Task 1)

- Establishes a baseline of operational performance to inform risk identification (i.e., models that support threat modeling and consequence analysis)

Scenario-based structure for documenting cybersecurity risks (Task 2)

- Describes how multiple threat actors can exploit vulnerabilities in multiple systems to cause adverse consequences

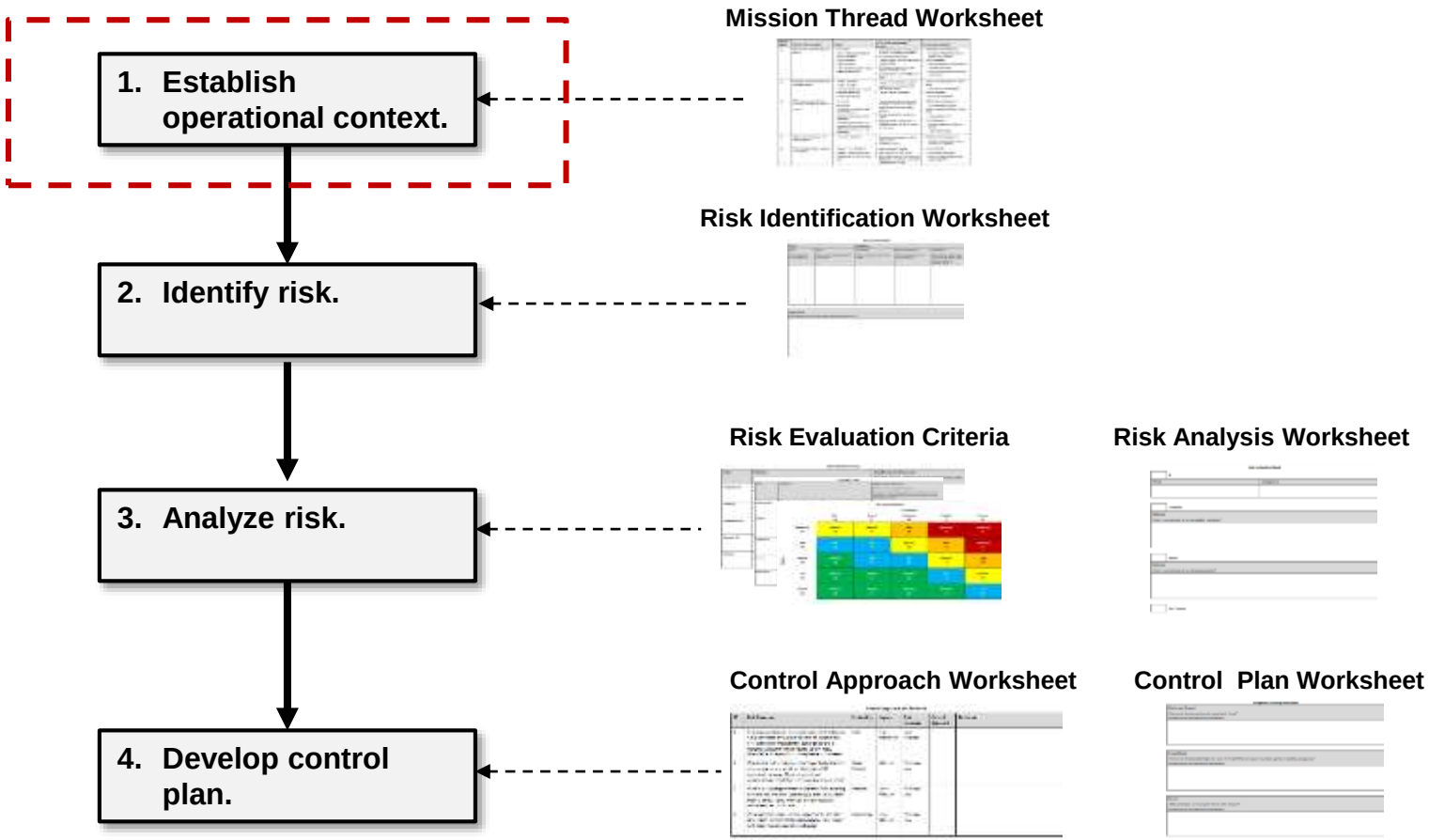
Shared cybersecurity view

- Presents a view that is understood by multiple stakeholders
  - System and software engineers
  - Security experts
  - Program managers
- Enables evaluation and management of complex security risks based on impact to the operational mission (Tasks 3-4)

Security Engineering Risk Analysis (SERA) Tutorial

Establish Operational Context (Task 1)

Establish Operational Context (SERA Task 1)



Establish Operational Context (Task 1)

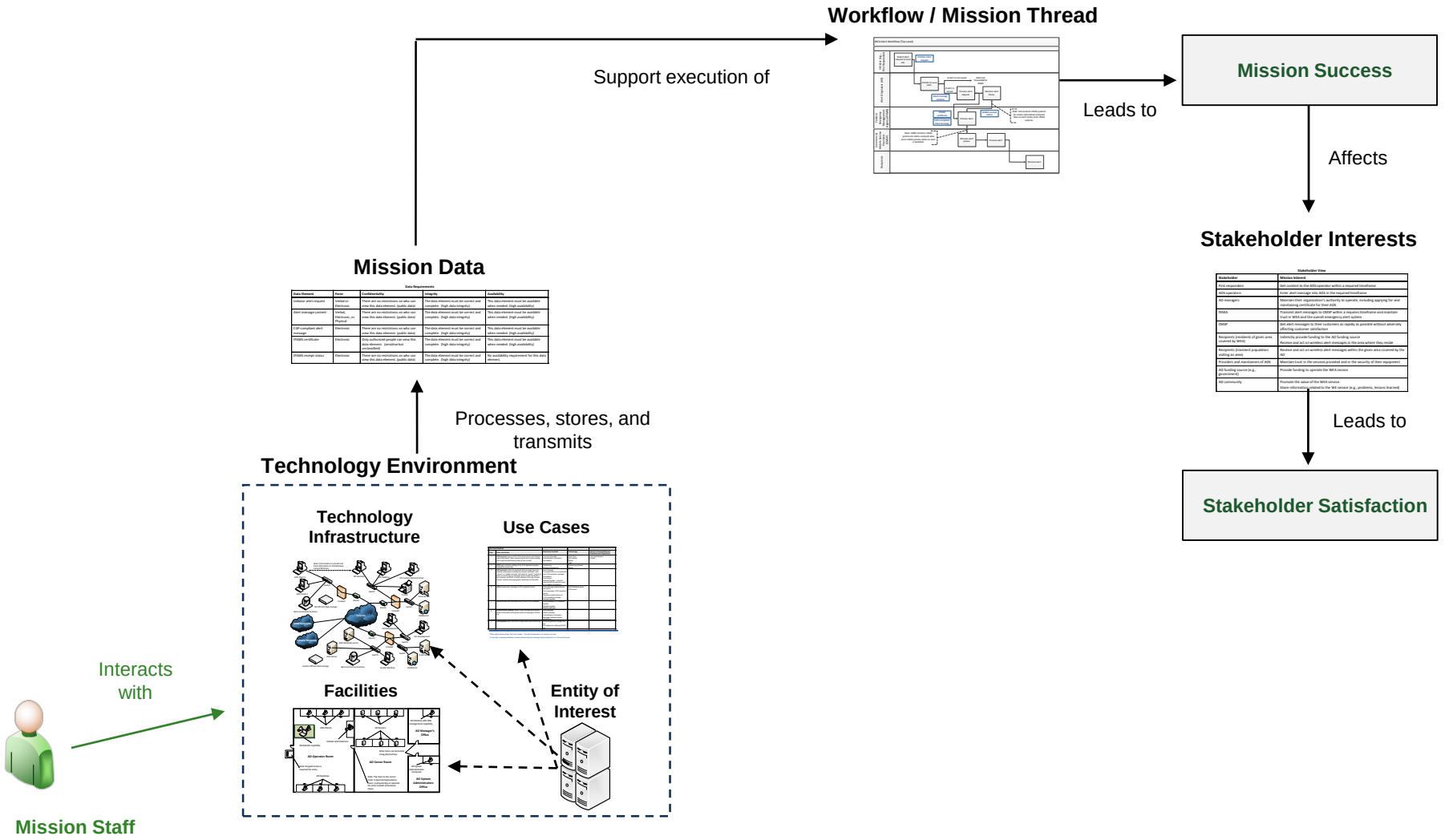
The entity of interest (e.g., the software application or system that is being analyzed) is identified.

The operational environment for the entity of interest is characterized to establish a baseline of operational performance.

Security risks are analyzed in relation to this baseline.

Steps	
1.1	Determine entity of interest.
1.2	Select workflow/mission thread.
1.3	Establish operational views.

SERA Task 1: *Expected Operational Results*



Step 1.1: *Determine Entity of Interest*

Step 1.1:

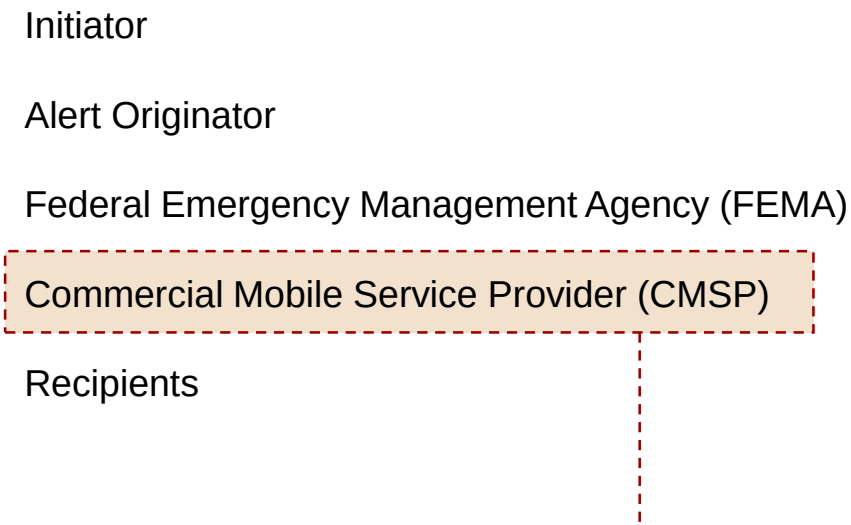
- The Analysis Team identifies the entity of interest for the analysis

Entity of interest:

- The entity that is the focus of the analysis. Examples include:
  - System
  - Application
  - Component
  - Workflow/mission thread activity
  - Others
- Selecting the entity of interest starts to define the scope of the subsequent analysis.

Example: *Entity of Interest*

Step 1.1



The Analysis Team was asked to conduct a SERA of a CMSP WEA alerting system.

The entity of interest is the CMSP WEA alerting system.

Step 1.2: *Workflow/Mission Thread - 1*

Workflow

- A collection of interrelated work tasks that achieves a specific result
- Includes all tasks, procedures, organizations, people, technologies, tools, data, inputs, and outputs required to achieve the desired objectives

Mission thread

- The term that the military uses in place of workflow
- A sequence of end-to-end activities and events that takes place to accomplish the execution of a military operation.

Note: We use the terms workflow and mission thread synonymously.

Step 1.2: *Workflow/Mission Thread - 2*

A workflow/mission thread defines expected operational results.

- Failure modes are not identified.
- Attacks (such as cyber attacks) are not considered.

The SERA Method analyzes how cyber attacks can

- Disrupt a workflow/mission thread
- Produce unexpected operational consequences (i.e., mission degradation or mission failure)

Step 1.2: *Select Workflow/Mission Thread*

Step 1.2:

- The Analysis Team selects which workflows or mission threads to include in the analysis.

An entity of interest might support multiple workflows or mission threads during operations.

Selecting relevant workflows or mission threads helps to refine the scope of the analysis further.

Example: *Selected Workflow/Mission Thread*

Step 1.2

Initiator

Alert Originator

Federal Emergency Management Agency (FEMA)

Commercial Mobile Service Provider (CMSP)

Recipients

The Analysis Team was asked to examine how cyber attacks to the CMSP WEA alerting system could disrupt the WEA Service.

The workflow/mission thread of interest is the WEA Service.

Step 1.3: *Establish Operational Views -1*

Step 1.3:

- The Analysis Team establishes a common view of the operational environment in which the entity of interest must function.

Most traditional risk-identification methods rely on peoples' tacit assumptions about the operational environment.

- The tacit assumptions tend to be incorrect, incomplete or in conflict with the assumptions of other people.
- The identified risks can be incorrect or incomplete.

The SERA Method requires the Analysis Team to explicitly describe the operational environment in which the entity of interest will be deployed.

Step 1.3: *Establish Operational Views - 2*

Operational views define the environment in which the entity of interest must function.

The Analysis Team uses various diagramming or modeling techniques to capture operational views. For example,

- A swimlane diagram can be used to document a workflow/mission thread.
- A network topology diagram can be used to document an organization's computer network architecture.
- A Unified Modeling Language (UML) diagram can be used to document a use case.

The Analysis Team documents only those operational views that it needs to support the security risk analysis.

Step 1.3: *Operational Views - 3*

View	Description
Workflow/Mission Thread	The sequence of end-to-end activities and events that take place to achieve a specific result
Stakeholder	The set of people with an interest or concern in (1) the workflow/mission thread and (2) the outcomes (e.g., products, services) produced by it.
Data	The data items required when executing the workflow/mission and their associated security attributes (e.g., confidentiality, integrity, availability).
Technology	The projected technologies that constitute the entity of interest. The technology view can include multiple models, such as system architecture, software architecture, and network topology.

Step 1.3: *Operational Views - 4*

View	Description
Physical	The projected physical layout of the facilities in which components of the entity of interest are located.
Use Case	A description of a set of steps that define the interactions between a role/actor and a system to achieve a goal. (The actor can be a human or an external system.)

Example: *Operational Views for CMSP Analysis*

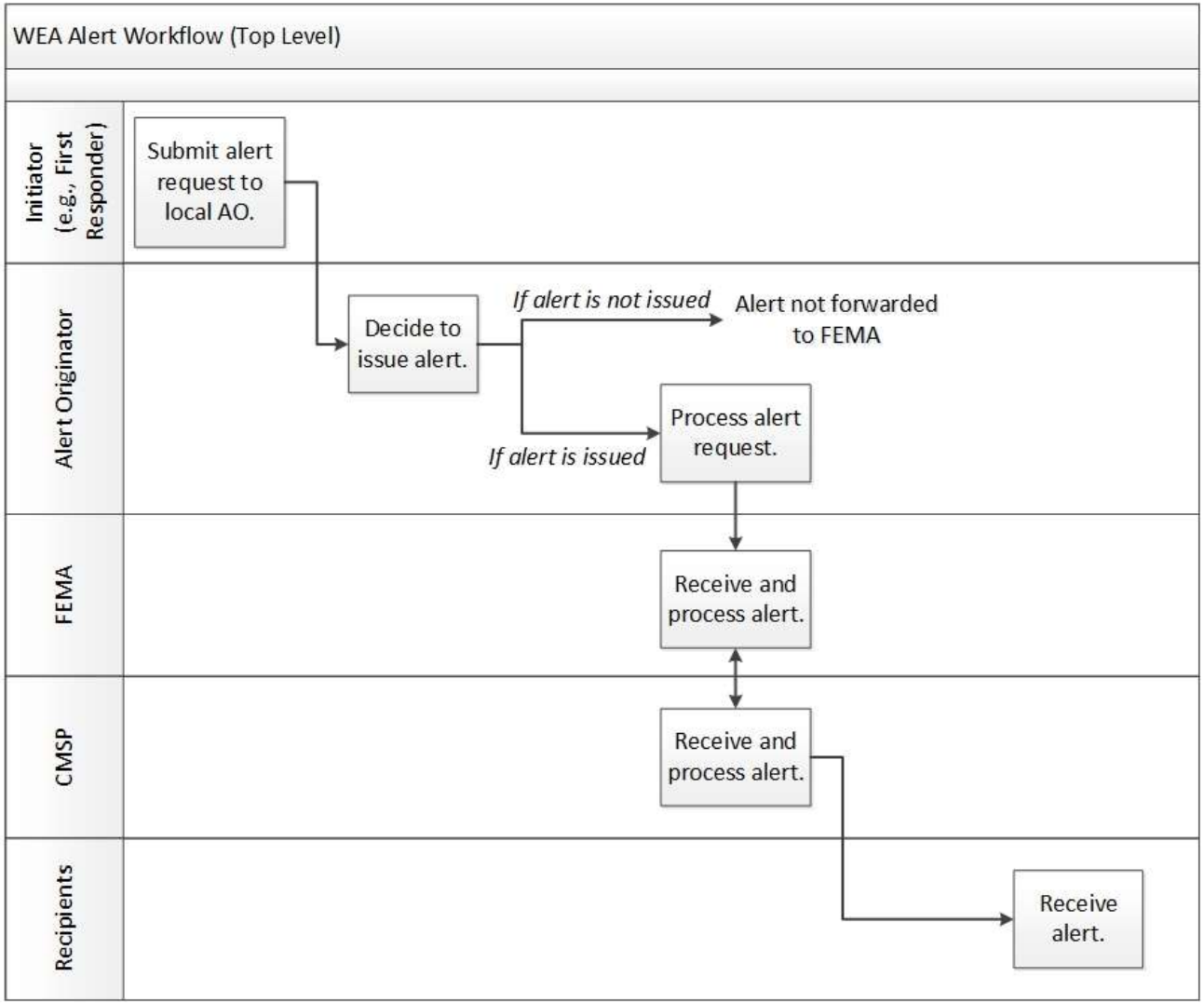
Step 1.3

The Analysis Team developed the following models to support the analysis:

- WEA workflow
- WEA system of systems
- CMSP workflow
- CMSP architecture
- CMSP dataflow
- CMSP data security attributes
- CMSP workflow stakeholders

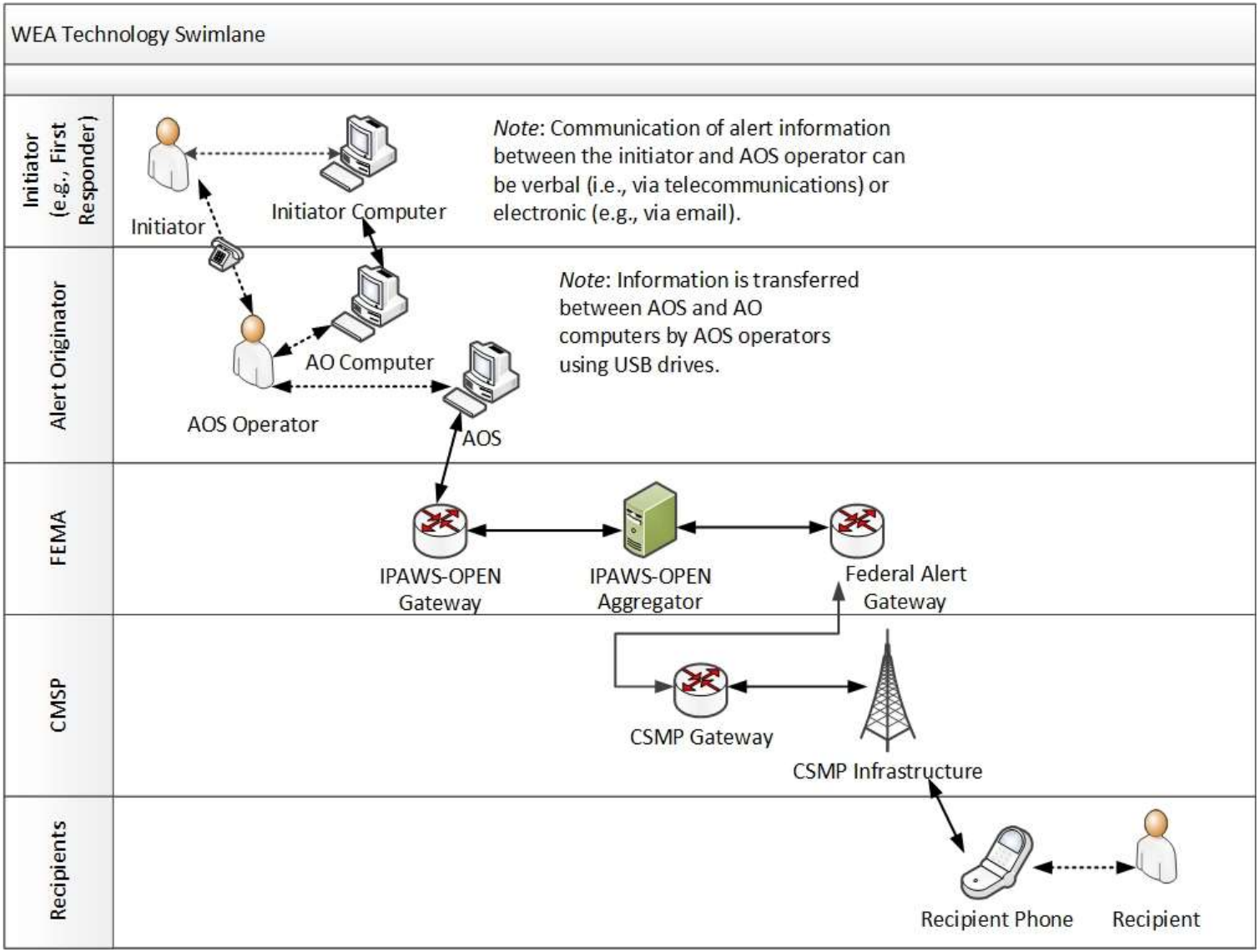
Example: *WEA Workflow*

Step 1.3



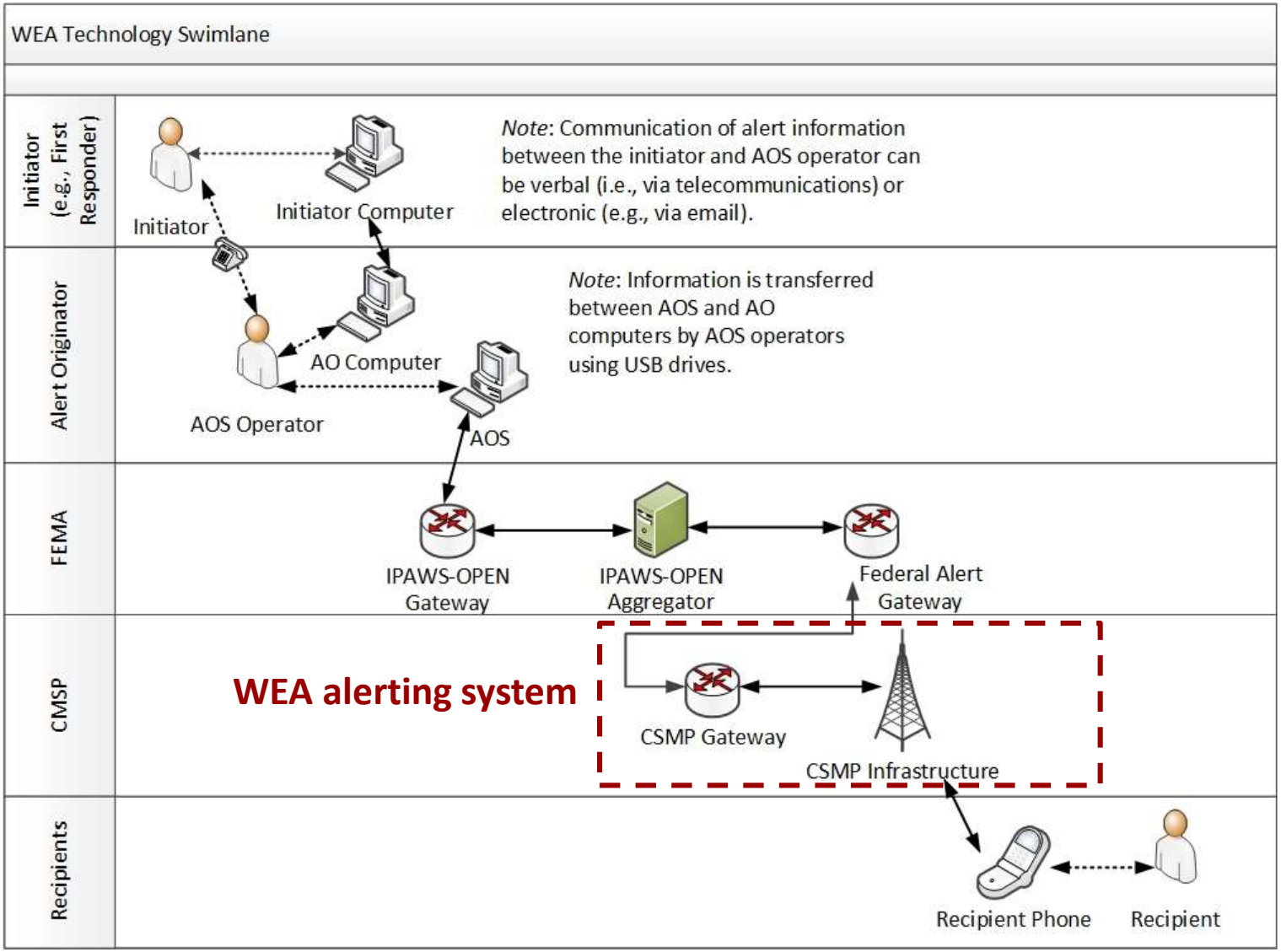
Example: *WEA Systems of Systems*

Step 1.3



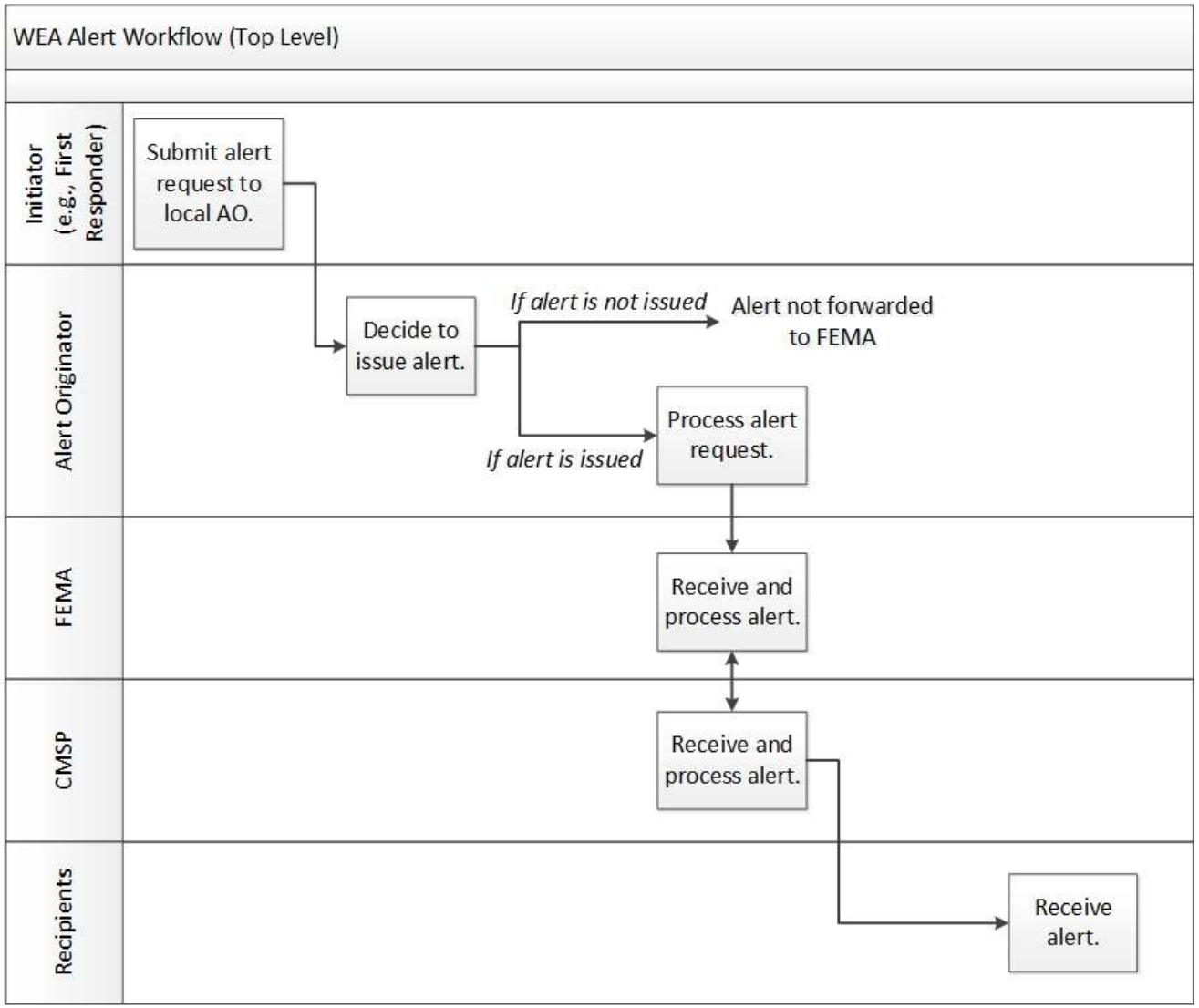
Example: *Entity of Interest*

Step 1.3



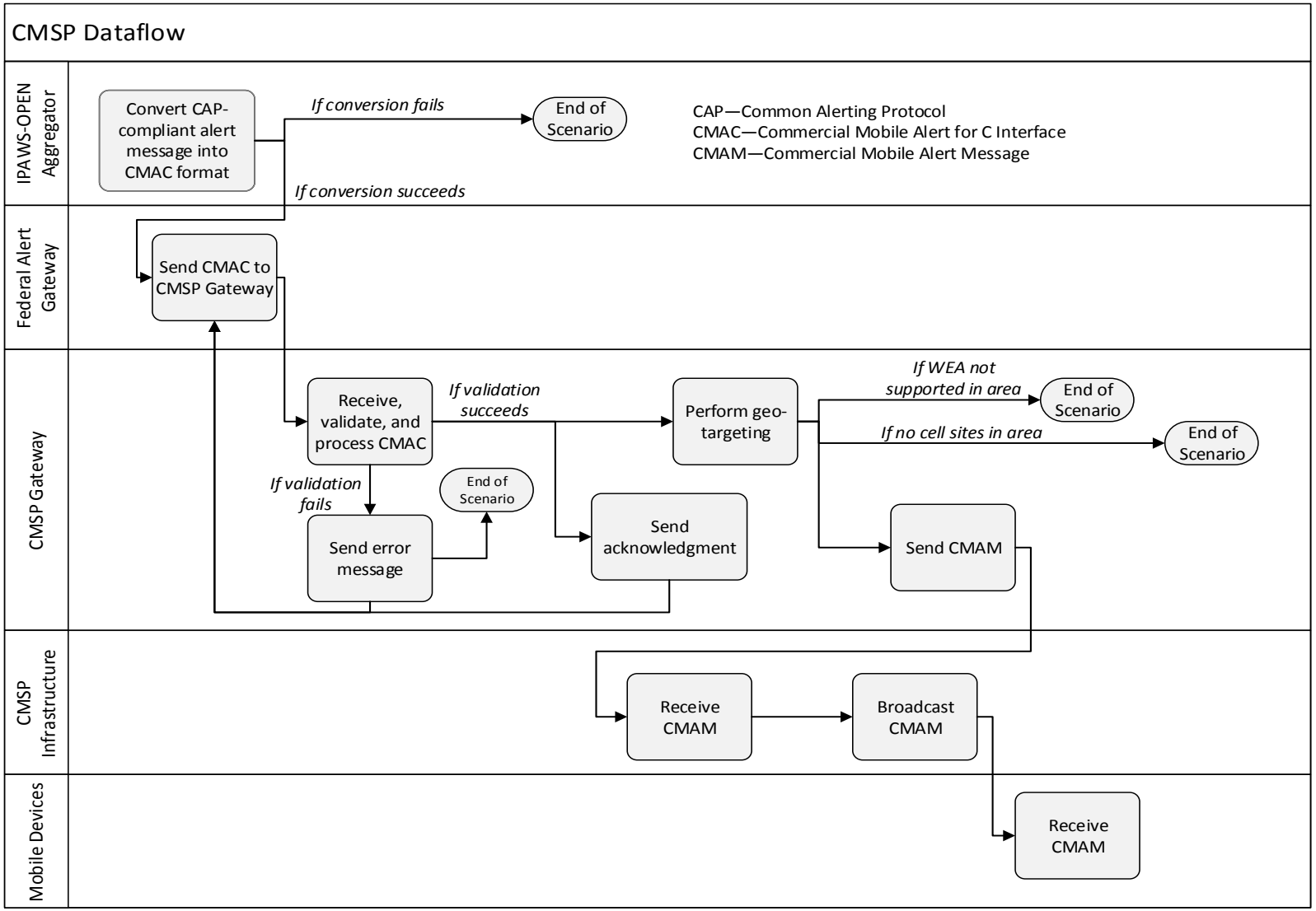
Example: *Focus of CMSP Analysis*

Step 1.3



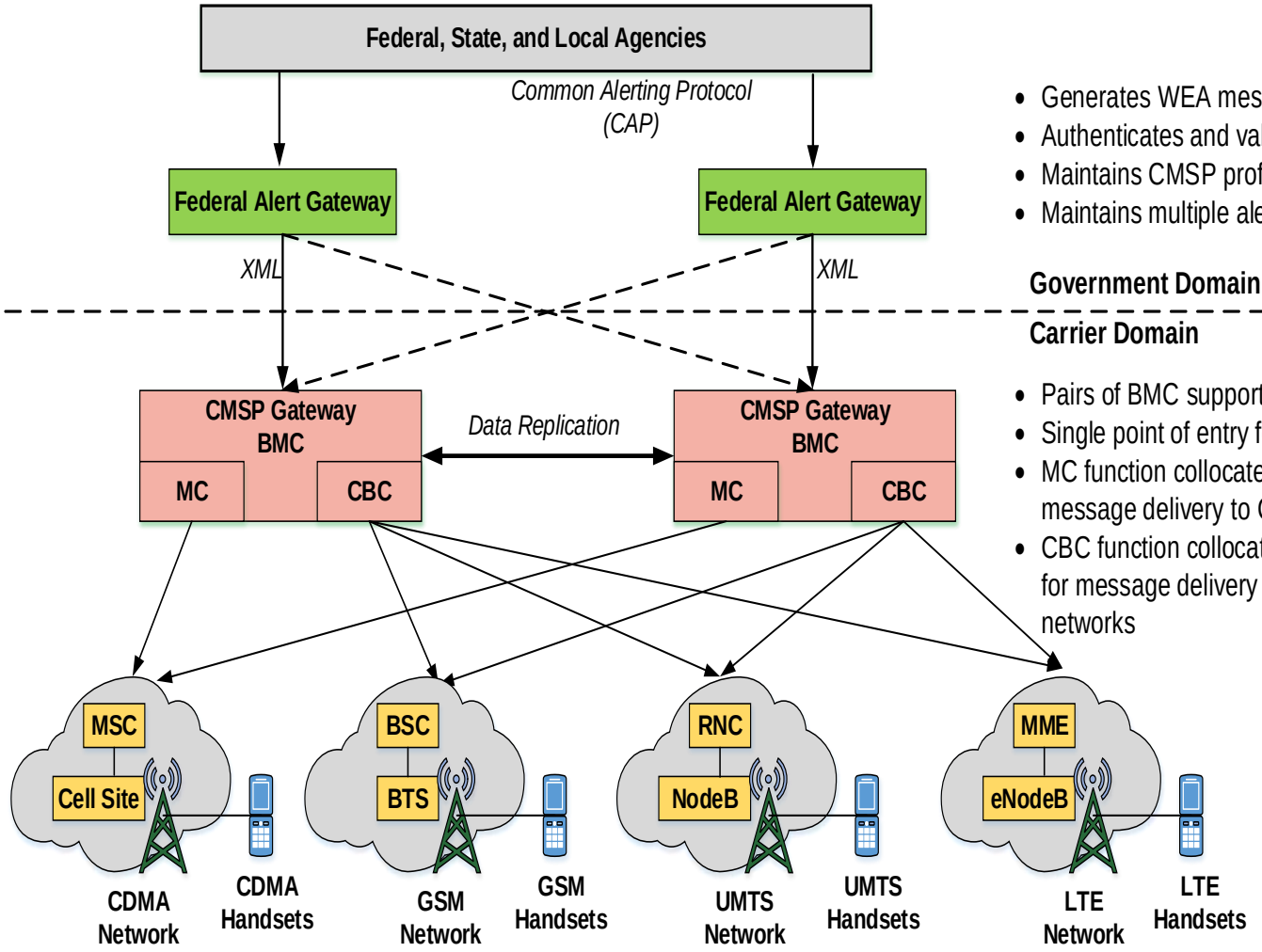
Example: *CMSP Workflow*

Step 1.3



Example: *CMSP Architecture*

Step 1.3



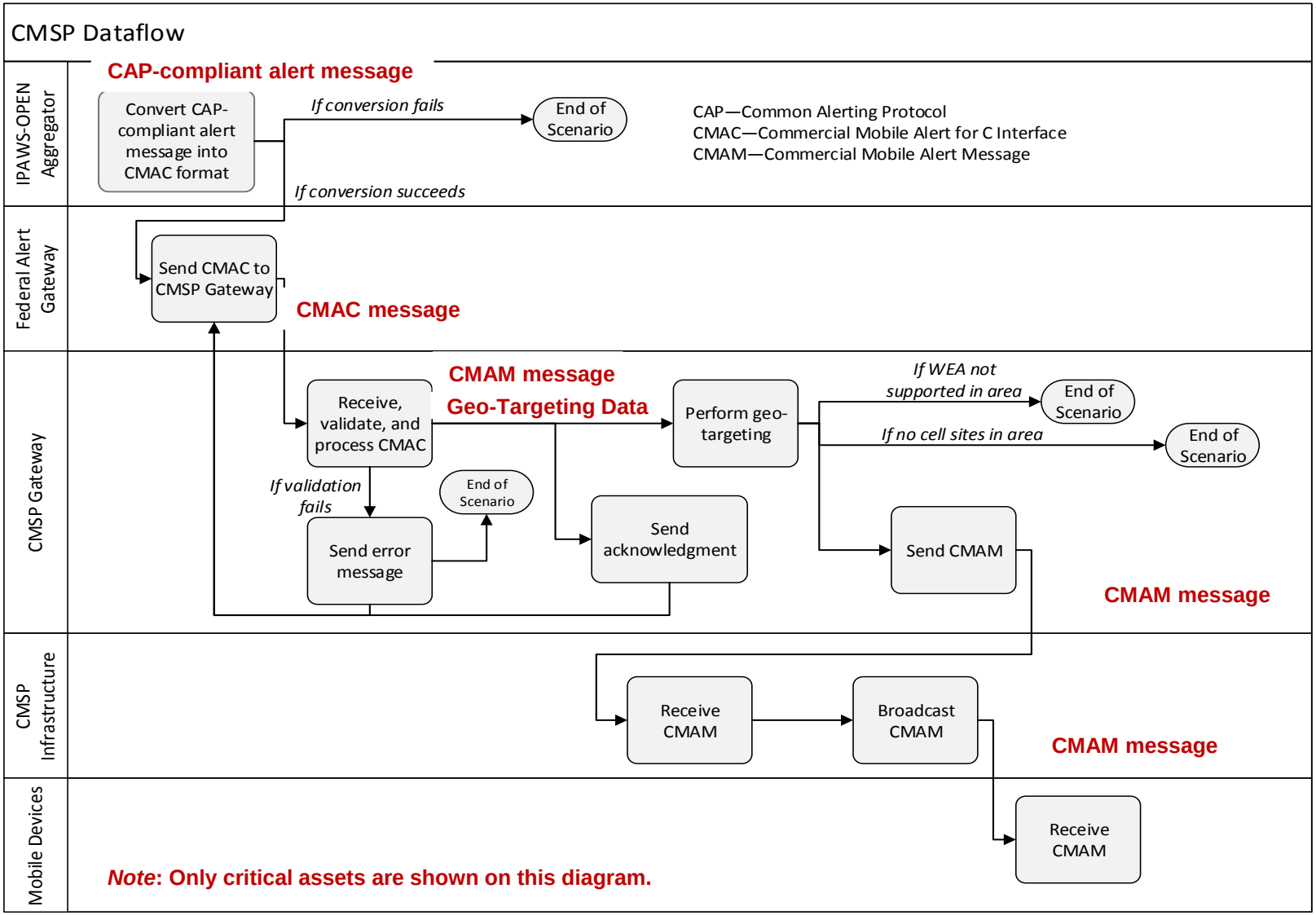
- Generates WEA messages
- Authenticates and validates alerts
- Maintains CMSP profiles
- Maintains multiple alert gateways

- Pairs of BMC support external CMSP
- Single point of entry for WEA messages
- MC function collocated with CMSP Gateway for message delivery to CDMA network
- CBC function collocated with CMSP Gateway for message delivery to GSM, UMTS, and LTE networks

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

Example: *CMSP Dataflow*

Step 1.3



Example: *CMSP Data Security Attributes*

Step 1.3

Data Element	Form	Confidentiality	Integrity	Availability
CAP-compliant alert message	Electronic	There are no restrictions on who can view this data asset. (public data)	The data asset must be correct and complete. (high data integrity)	This data asset must be available when needed. (high availability)
CMAC message	Electronic	There are no restrictions on who can view this data asset. (public data)	The data asset must be correct and complete. (high data integrity)	This data asset must be available when needed. (high availability)
CMAM message	Electronic	There are no restrictions on who can view this data asset. (public data)	The data asset must be correct and complete. (high data integrity)	This data asset must be available when needed. (high availability)
Geo-targeting data	Electronic	There are no restrictions on who can view this data asset. (public data)	The data asset must be correct and complete. (high data integrity)	This data asset must be available when needed. (high availability)

Example: *CMSP Workflow Stakeholders*

Step 1.3

Stakeholder	Mission Interest
FEMA	Transmit alert messages to carriers within a required time frame and maintain trust in WEA and the overall Emergency Alert System
Carrier	Deliver alert messages to customers as rapidly as possible without adversely affecting customer satisfaction Implement best security practices to reduce risk of security incidents (and avoid additional mandated security regulations)
Recipients	Receive and act on WEA messages

Exercise 2: *Critical Data Asset Identification - 1*

Turn to Exercise 2 in the tutorial workbook.

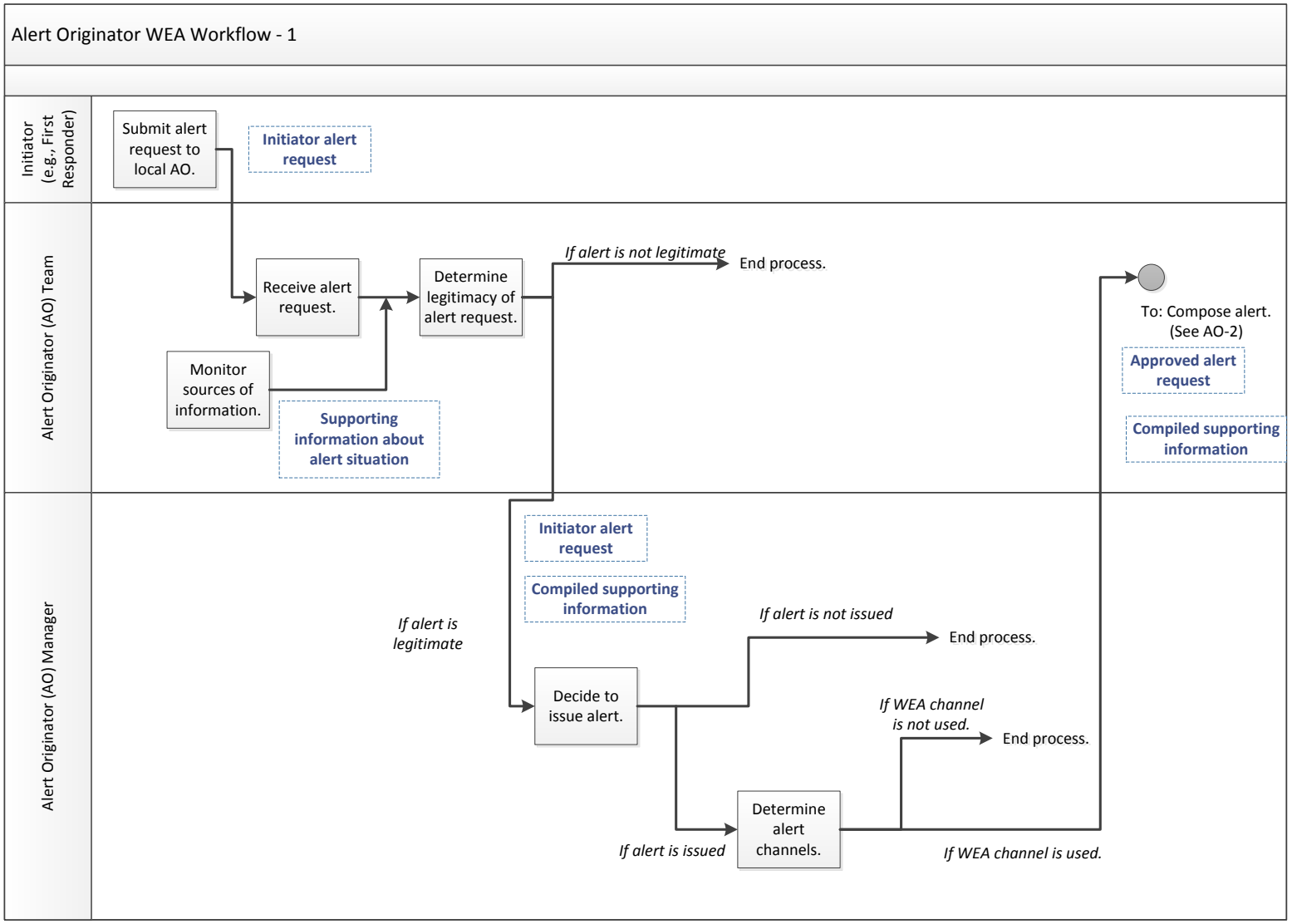
In this exercise you will be identifying critical data assets.

You will examine the following information for this exercise:

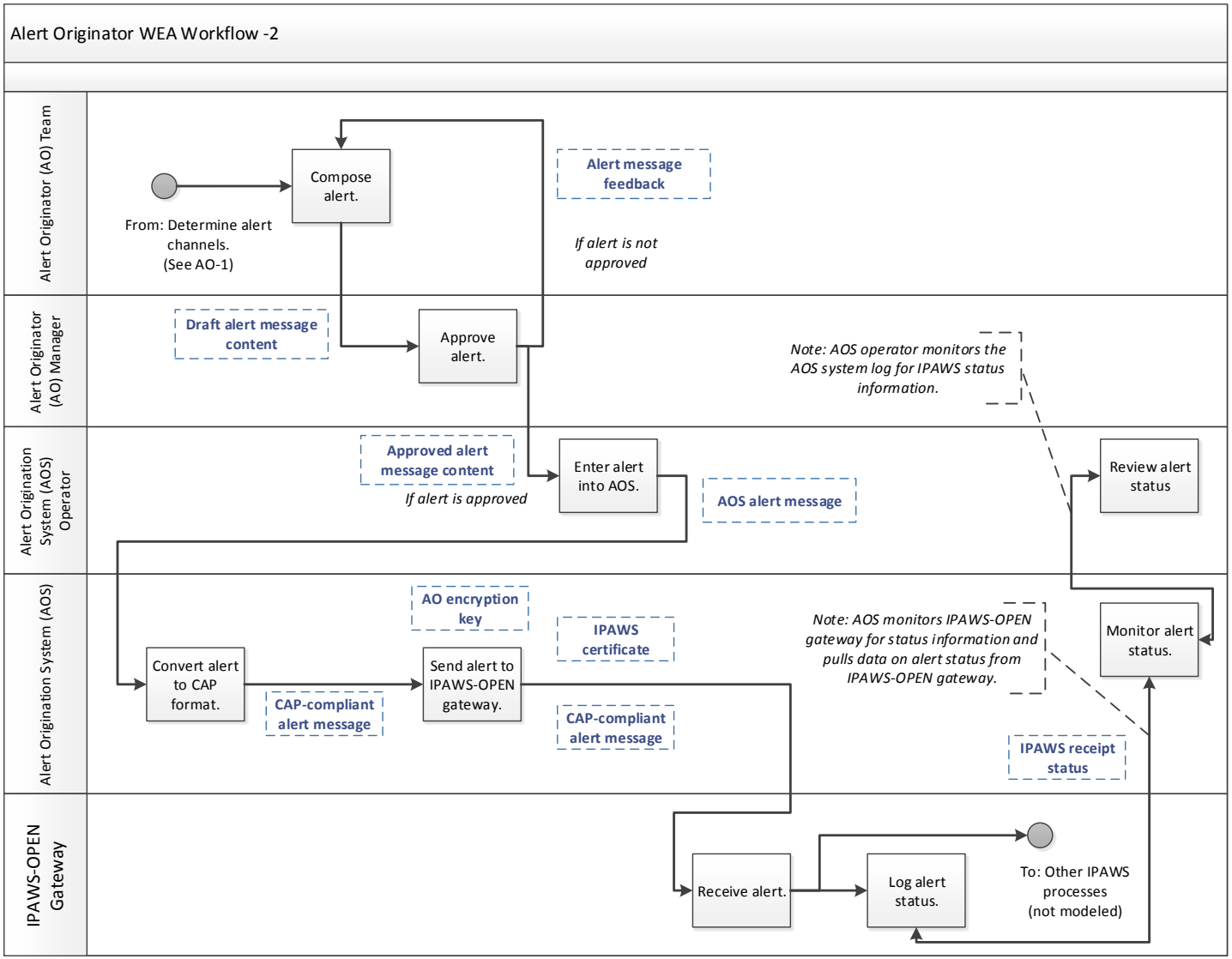
- Alert Originator (AO) detailed workflow
- Table that describes each data asset featured in the workflow.

Review the workflow and table and identify which assets are most critical to the mission.

Exercise 2: *Critical Data Asset Identification - 2*



Exercise 2: *Critical Data Asset Identification - 3*



Exercise 2: *Critical Data Asset Identification - 4*

The workbook provides detailed information for each data asset featured in the Alert Originator workflow:

- Initiator alert request
- Supporting information about alert situation
- Compiled supporting information
- Approved alert request
- Draft alert message content
- Alert message feedback
- Approved alert message content
- AOS alert message
- CAP-compliant alert message
- AO encryption key
- IPAWS certificate
- IPAWS status receipt

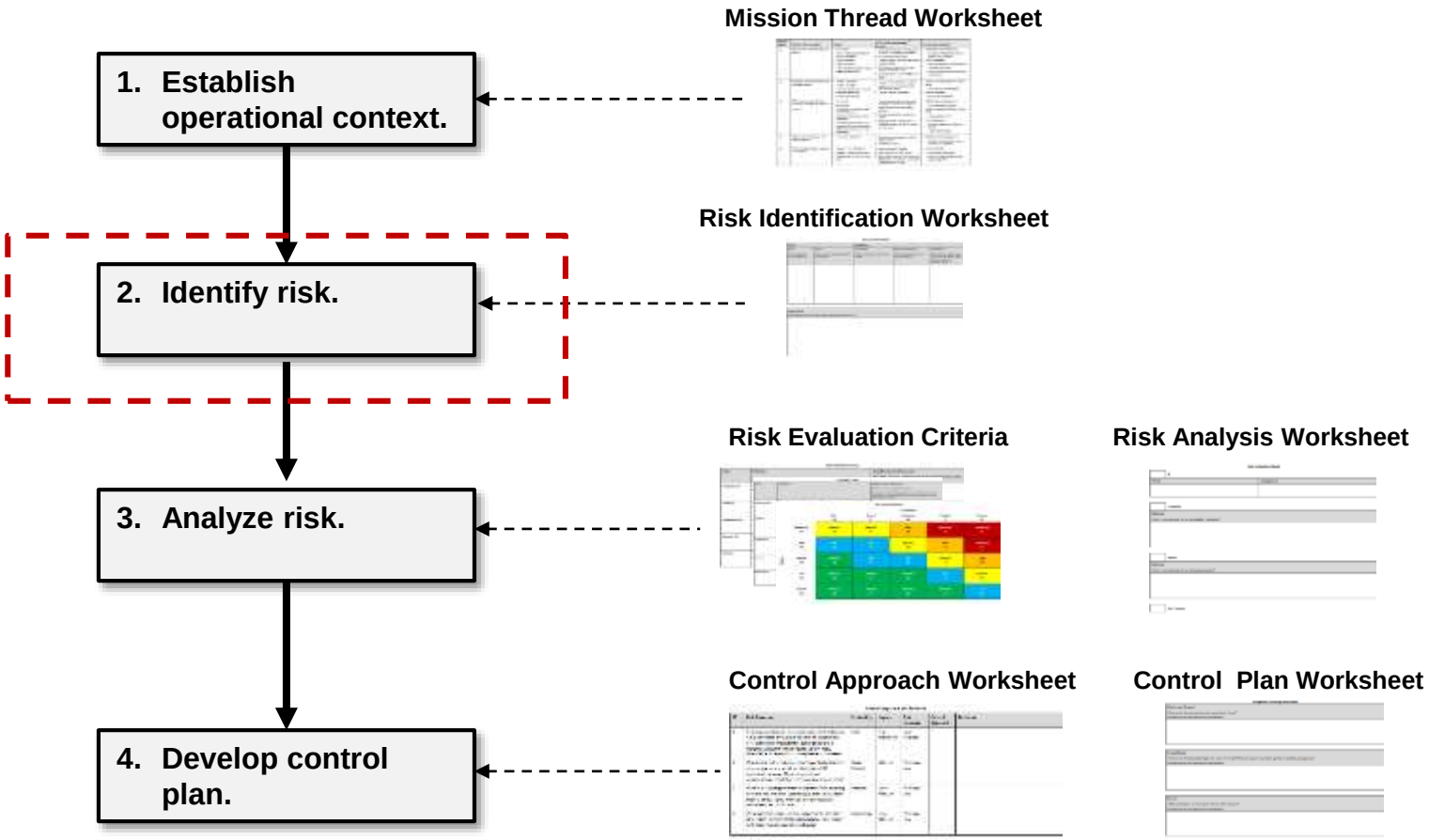
Consider the following questions:

- What is the most critical data asset(s)? Why?

Security Engineering Risk Analysis (SERA) Tutorial

Identify Risk (Task 2)

Identify Risk (SERA Task 2)

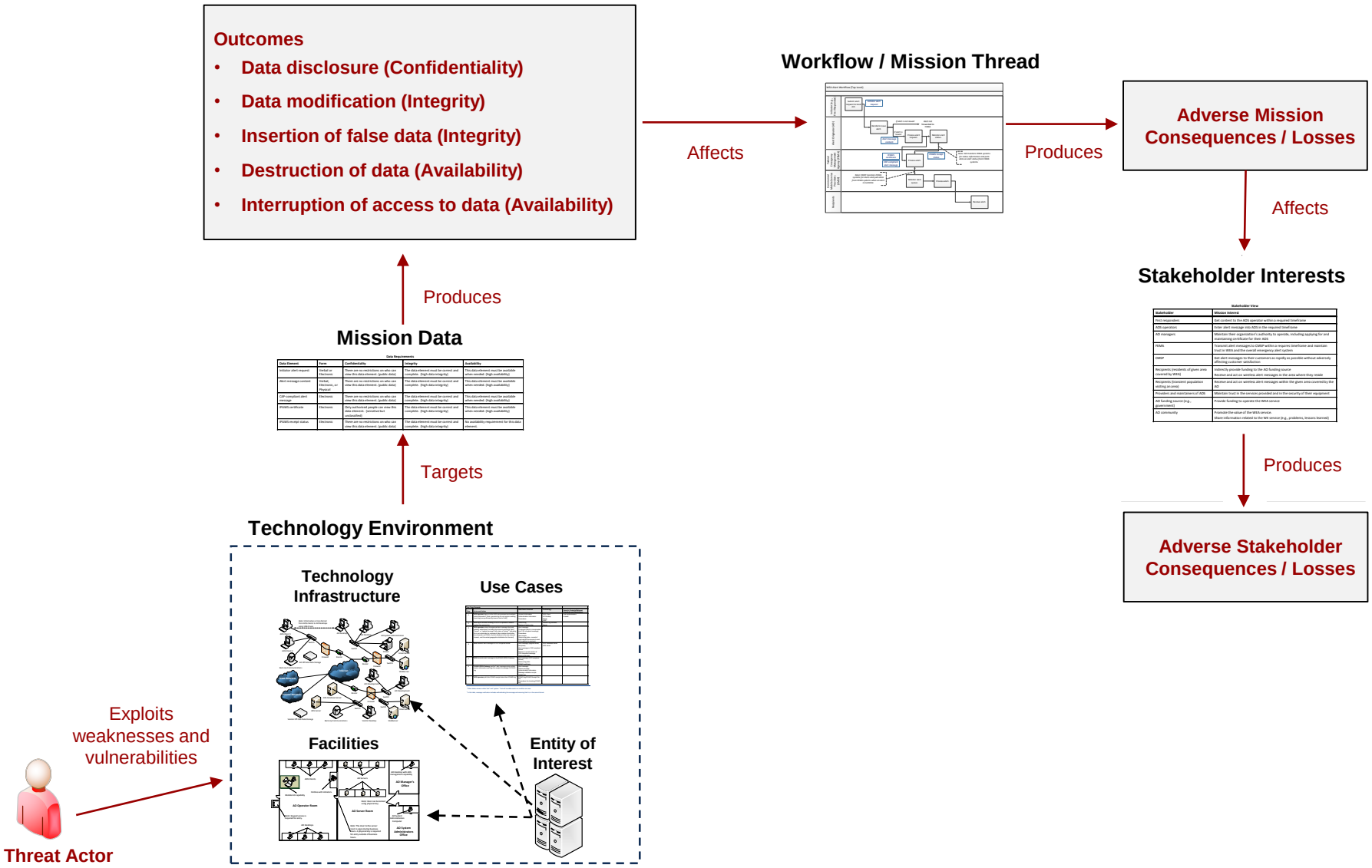


Identify Risk (SERA Task 2)

Security concerns are transformed into distinct, tangible risk scenarios that can be described and measured.

Steps	
2.1	Identify threat.
2.2	Establish consequences.
2.3	Identify enablers and amplifiers.
2.4	Develop risk scenario.

SERA Task 2: *Security Risk Scenarios*



SERA Task 2: *Elements of Security Risk Scenario*

Threat Components

- Actor – Motive – Goal – Outcome – Means – Threat Complexity

Threat Sequence

- Threat Step – Enabler(s)

Workflow Consequences

- Consequence – Amplifier(s)

Stakeholder Consequences

- Consequence – Amplifier(s)

Step 2.1: *Identify Threat*

Step 2.1

- The Analysis Team examines how threat actors might violate the security attributes (i.e., confidentiality, integrity, and availability) of the critical data.
  - The team brainstorms threats to critical assets.
  - For threats that the team will analyze further, it documents the following information:
    - Components of the threat
    - Sequence of steps required to execute the threat (i.e., threat sequence)

Example: *Candidate Threats*

Step 2.1

An outside actor with malicious intent obtains a valid certificate through social engineering and uses it to send an illegitimate alert message by spoofing the Federal Alert Gateway.

Malicious code prevents the CMSP Gateway from processing an alert.

An insider with malicious intent uses the CMSP infrastructure to send illegitimate messages.

An outside actor with malicious intent launches a distributed denial of service (DDoS) attack against the CMSP Gateway.

An attacker in the mobile-device supply chain inserts malicious code into mobile devices sold by carriers. The malicious code captures legitimate WEA messages and replays them repeatedly at a later time. (supply chain attack)

An upstream replay attack targets an alert originator (AO) and sends repeated messages to a geographic area which could result in a denial of service for the carriers.

An outside actor with malicious intent spoofs a cell tower and transmits an illegitimate message to mobile devices in a local area.

Step 2.1: *Threat Components - 1*

Threat

- A statement that describes the cyber-based act, occurrence, or event that exploits one or more vulnerabilities and leads to an adverse consequence or loss

Actor

- Who or what is attempting to violate the security attributes of critical data

Motive

- The intentions of a threat actor, which can be deliberate and malicious or accidental

Goal

- The end toward which the threat actor's effort is directed; the goal succinctly describes the key indirect consequence (i.e., impact on stakeholders) that the actor is trying to produce

Step 2.1: *Threat Components - 2*

Outcome

- The direct consequence of the threat (i.e., disclosure of data, modification of data, insertion of false data, destruction of data, interruption of access to data)

Means

- The resources the actor uses when executing the threat

Threat Complexity

- The degree of difficulty associated with executing the threat

Additional Context

- Any additional, relevant contextual information related to the threat

Example: *Risk 1 Threat Components - 1*

Step 2.1

Component	Description
Threat	An insider with malicious intent uses the CMSP infrastructure to send illegitimate messages.
Actor	Person with an insider's knowledge of the organization
Motive	The threat is a deliberate/malicious act. The actor is disgruntled (e.g., has been passed over for promotion or has been notified of performance issues). The actor has visibly expressed frustration/anger.
Goal	The actor seeks to erode trust in the carrier. If this is a major carrier, the attack will also erode trust in the WEA service (e.g., people will turn off alerts) due to the large impact.
Outcome	Illegitimate alerts are generated by the CMSP infrastructure (integrity issue).
Means	The actor needs access to the carrier's systems, access to public documents that describe the WEA service, and access to documents that describe the CMAM format.

Example: *Risk 1 Threat Components - 2*

Step 2.1

Component	Description
Threat Complexity	The attack is moderately complex, requires technical skills, and requires moderate preparation to execute.
Attack Summary	The insider inserts a logic bomb, which is designed to replay a nonsense or inflammatory CMAM message repeatedly.
Additional Context	The timing of the attack could cause critical alerts to be ignored. This threat incorporates current SEI/CERT research on Insider Threat.

Step 2.1: *Key Areas to Consider When Developing a Threat Sequence*

Planning and Reconnaissance

- What planning and reconnaissance activities does the actor need to perform?

Accessing the Entity of Interest

- How will the actor gain access to the target of the attack (i.e., the entity of interest)?

Attacking the Entity of Interest

- What is the direct consequence of the attack? How will critical data asset(s) be affected?
- How will the actor execute the attack?

Example: *Threat Sequence for Risk 1*

Step 2.1

T1. The insider is upset upon learning that he will not receive a bonus this year and has been passed over for a promotion.

T2. The insider begins to behave aggressively and abusively toward his coworkers.

T3. The insider develops a logic bomb designed to replay a nonsense CMAM message repeatedly.

T4. The insider uses a colleague's workstation to check in the modified code with the logic bomb to the CMSP Gateway code base.

T5. Seven months later, the insider voluntarily leaves the company for a position in another organization.

T6. Twenty-one days after the insider leaves the carrier, the logic bomb is activated automatically.

T7. The malicious code causes the carrier's CMSP Gateway to send a nonsense WEA message repeatedly to people across the country.

Step 2.2: *Establish Consequences*

Step 2.2:

- The Analysis Team analyzes the workflow/mission thread and stakeholder models from Task 1 to determine how the workflow/mission thread and stakeholders could be affected by that threat.

Step 2.2: *Multiple Types of Consequences*

Direct Consequence (also referred to as the outcome of a threat)

- How the security attributes (i.e., confidentiality, integrity, availability) of critical data are violated. Examples include
  - Data disclosure (confidentiality issue)
  - Data modification (integrity issue)
  - Insertion of false data (integrity issue)
  - Destruction of data (availability issue)
  - Interruption of access to data (availability issue)

Indirect Consequences

- How the mission thread and stakeholders are affected by the direct consequence

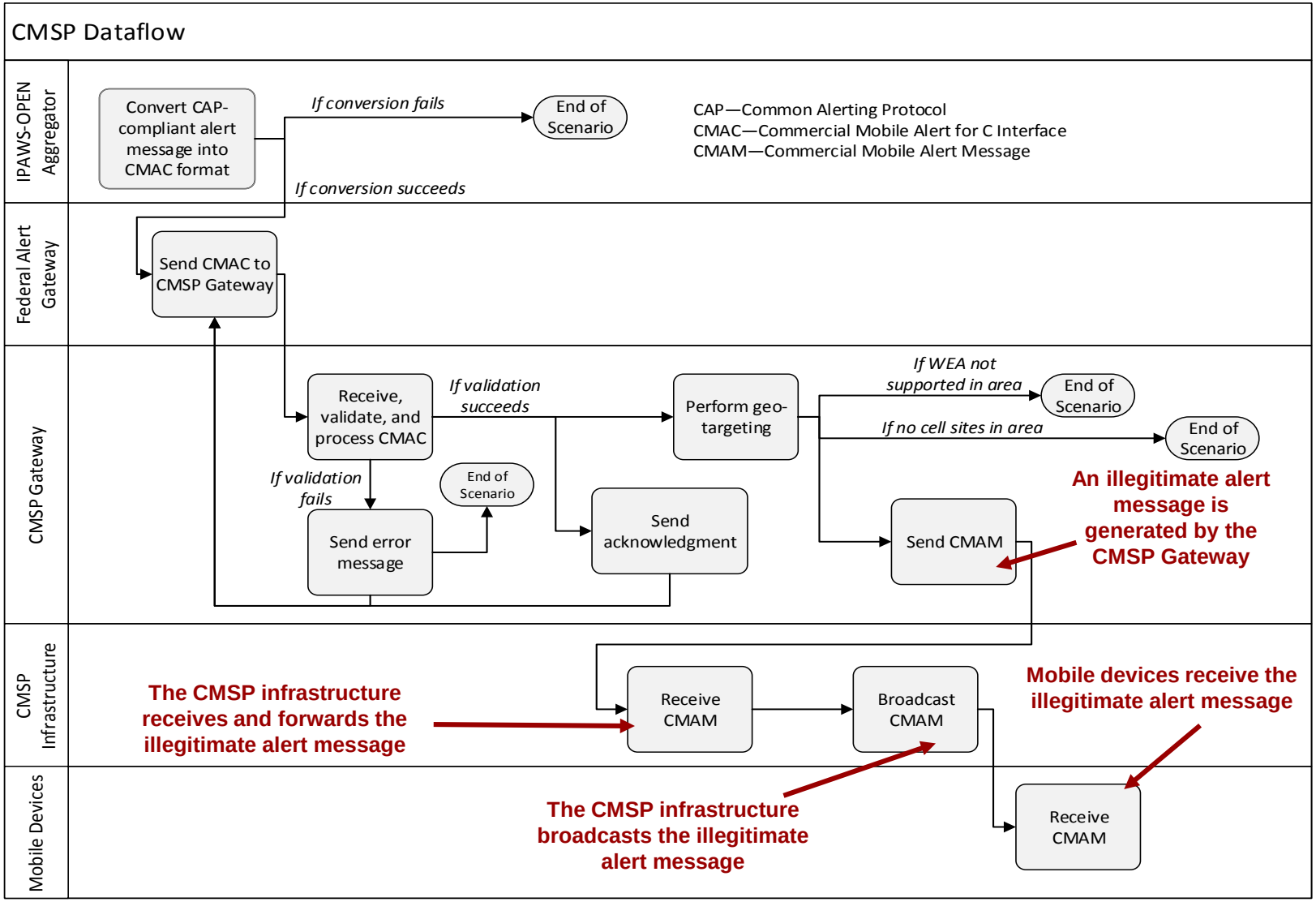
Example: *Risk 1 Direct Consequence/Outcome*

Step 2.2

Illegitimate alerts are generated by the CMSP infrastructure (integrity issue).

Example: *Risk 1 Workflow Consequences – 1*

Step 2.2



Example: *Risk 1 Workflow Consequences - 2*

Step 2.2

The carrier's infrastructure forwards the nonsense WEA message repeatedly to mobile devices in the targeted geographic area. (*Carrier Infrastructure*)

People with WEA-capable mobile devices supported by the carrier receive the nonsense message. (*Mobile Devices*)

Example: *Risk 1 Stakeholder Consequences*

Step 2.2

Recipients of the message quickly become annoyed at receiving the same nonsense message repeatedly. (*Recipients*)

Many recipients complain to the carrier's customer service operators. (*Recipients*)

A large number of recipients turn off the WEA function on their phones. Many will not turn the WEA service back on. (*FEMA, Carrier*)

The carrier responds to the attack. It removes the malicious code from its infrastructure. The cost to do so is considerable. (*Carrier*)

People leave the carrier for another carrier because of the incident. (*Carrier*)

People lose trust in the WEA service. (*FEMA, Carrier*)

Step 2.3: *Identify Enablers and Amplifiers*

Step 2.3:

- The Analysis Team identifies conditions and circumstances that
  - Facilitate the execution of a threat step (called *enablers*)
  - Propagate or increase the consequences triggered by the occurrence of a threat (called *amplifiers*)

Example: *Enabler for Threat Step 3*

Step 2.3

Threat Step	T3. The insider develops a logic bomb designed to replay a nonsense CMAM message repeatedly.
Focus	Technology CMSP Gateway (focus of the logic bomb)
Enabler	An employee that has technical skills can use those skills to inflict damage on information systems.

Example: *Enabler for Threat Step 4*

Step 2.3

Threat Step

T4. The insider uses a colleague's workstation to check-in the modified code with the logic bomb.

Focus

Organization

Carrier's physical security practices

Technology

Workstation security (e.g., screen locking)

CMSP Gateway

Change management/configuration management system

Enablers

Leaving a workstation unattended while logged in can allow malicious actors to gain illegitimate access to information and services.

An insufficient change management/configuration management capability can prevent the carrier from knowing if software has been modified inappropriately.

Example: *Risk 1 Threat Sequence Table (Excerpt)*

Step 2.3

Threat Step (Risk 1)		Focus	Enabler	Candidate Control
T1.	The insider is upset upon learning that he is not receiving a bonus this year and has been passed over for a promotion.	Organization Carrier—human resource practices	A lack of proper feedback provided to an employee can result in the employee being unaware of performance issues that could affect his/her career.	***Note*: This column is completed during SERA Task 4.**
T2.	The insider begins to behave aggressively and abusively toward his coworkers.	Organization Carrier—human resource practices	An employee's inappropriate behavior can be an indicator of more serious actions.	
T3.	The insider develops a logic bomb designed to replay a nonsense CMAM message repeatedly.	Technology CMSP Gateway (focus of the logic bomb)	An employee that has technical skills can use those skills to inflict damage on information systems.	
T4.	The insider uses a colleague's workstation to check-in the modified code with the logic bomb.	Organization Carrier's physical security practices Technology Workstation security (e.g., screen locking) CMSP Gateway Change management/ configuration management system	Leaving a workstation unattended while logged in can allow malicious actors to gain illegitimate access to information and services.	
			An insufficient change management/configuration management capability can prevent the carrier from knowing if software has been modified inappropriately.	

Example: *Amplifier for a Workflow Consequence*

Step 2.3

Consequence	The carrier's infrastructure forwards the nonsense WEA message repeatedly to mobile devices in the targeted geographic area.
Workflow Actor	Carrier infrastructure
Amplifier	Insufficient monitoring of the network for abnormal activity can result in a delayed response to the attack (e.g., no response until customer complaints are received).

Example: *Risk 1 Workflow Consequence Table*

Step 2.3

Consequence	Workflow Actor	Amplifier	Candidate Control
The carrier's infrastructure forwards the nonsense WEA message repeatedly to mobile devices in the targeted geographic area.	Carrier infrastructure	Insufficient monitoring of the network for abnormal activity can result in a delayed response to the attack (e.g., no response until customer complaints are received).	***Note*: This column is completed during SERA Task 4.**
People with WEA-capable mobile devices supported by the carrier receive the nonsense message.	Mobile devices	Enabling the WEA service on a mobile device allows the owner of that device to receive CMAM messages.	

Example: *Amplifier for a Stakeholder Consequence*

Step 2.3

Consequence	Recipients of the message quickly become annoyed at receiving the same nonsense message repeatedly.
Stakeholder	Recipients
Amplifier	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients.

Example: *Risk 1 Stakeholder Consequence Table (Excerpt)*

Step 2.3

Consequence	Stakeholder	Amplifier	Candidate Control
Recipients of the message quickly become annoyed at receiving the same nonsense message repeatedly.	Recipients	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients	***Note*:** **This column is completed during SERA Task 4.**
Many recipients complain to the carrier's customer service operators.	Recipients	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients.	
A large number of recipients turn off the WEA function on their phones. Many will not turn the WEA service back on.	FEMA Carrier	Peoples' ability to disable the WEA service on their mobile devices helps them deal with the attack. They might decide not to (or might forget to) re-enable the WEA service after the attack.	

Step 2.4: *Develop Risk Scenario*

Step 2.4:

- The Analysis Team documents the following:
  - Narrative description of the security risk based on the information generated in steps 2.1 through 2.3
  - Risk statement that provides a succinct and unique description of the security risk scenario that is used for tracking purposes

Step 2.4: *Risk Statement and Scenario*

Many risk assessments use if-then statements to represent a risk.

- Those assessments rely on the if-then structure to convey all relevant information about the risk.

The SERA Method uses

- Security risk scenario and supporting data structures (e.g., threat sequence tables, consequence tables) when performing detailed analysis of security risks
- Risk statements to facilitate the tracking of multiple security risk scenarios during analysis and control

Example: *Security Risk Statement Risk 1*

Step 2.4

An insider is employed by a wireless carrier . The insider is a software developer and is responsible for developing applications that support the company's wireless infrastructure . The insider is upset that he will not receive a bonus this year and also has been passed over for a promotion . Both of these perceived slights anger the insider . As a result, he begins to behave aggressively and abusively toward his coworkers . For example, he downplays their achievements , brags about his own abilities , takes credit for the work of others and delays progress on projects . The insider's anger builds over time until he finally convinces himself to take action against the carrier .

His plan is to plant a logic bomb in the CMSP Gateway , hoping to send "custom" WEA messages to all WEA -capable wireless devices supported by the carrier . His ultimate goal is to bring negative publicity to the company . As a function of his job, the insider has unlimited access to the company's software code and is able to modify the company's code at will. While on site and during work hours , the insider develops a logic bomb designed to replay a nonsense CMAM message repeatedly .

The insider shares an office with another software developer , who often leaves her workstation unlocked when she is out of the office. The insider uses his colleague's workstation to check in the modified code with the logic bomb . Seven months later, the insider voluntarily leaves the company for a position in another organization . Twenty-one days after the insider leaves the carrier , the logic bomb is activated automatically . The malicious code causes the carrier's WEA service to send a nonsense WEA message repeatedly to people across the country .

Many recipients become annoyed at receiving the same alert repeatedly . Some of these people complain to the carrier's customer service operators . A large number of recipients turn off the WEA function on their phones in response to the attack.

The carrier responds to the attack by taking the infected CMSP Gateway offline . The broadcast of the illegitimate messages stops. The carrier then responds aggressively to the attack by investigating the source of the attack , locating the malicious code and removing that code from its infrastructure . Once the malicious code is removed from the CMSP Gateway, the carrier brings the CMSP Gateway back online . The cost to recover from the attack is considerable .

As a result of the attack , some customers leave their carrier for other carriers . In addition, many people lose trust in the WEA service. Many of these recipients will permanently disable the WEA service on their mobile devices after experiencing this attack .

The overall risk exposure of this scenario is low . This scenario has a remote probability of occurrence because it is reasonably complex and requires considerable preparation to execute . A disgruntled insider must have physical access to a workstation that can update CMSP production code , which limits the number of potential attackers . In addition, the disgruntled insider must have the technical skills needed to execute the attack and must be familiar with the CMSP Gateway. Field experience indicates that the number of cyber attacks by disgruntled insiders continues to grow across all sectors, however. As a result , an insider attack like this is not considered to be a rare event .

The consequences of this risk scenario are moderate in severity . Customers might not have much flexibility to change carriers easily , which can limit the potential for loss of business . Carriers already maintain help desk capabilities to respond to customer complaints , which helps with the response to this attack . In addition, tech-savvy customers can turn off the WEA service and eliminate the annoyance . The experience of SMEs related to malicious code indicate that the typical costs to find and remove malicious code from a networked environment are *considerable* , a term used in this report to refer to all of the external and internal costs to recover from a cyber attack . External cost factors can include business disruption , information loss or theft , revenue loss and equipment damages . Internal cost factors can include funds required for detection , investigation and escalation , containment, recovery and subsequent efforts to ward off future attacks.

See the workbook for the Risk 1's security risk scenario.

Example: *Risk Statement Risk 1*

Step 2.4

IF an insider with malicious intent uses the CMSP infrastructure to send nonsense alert messages repeatedly, **THEN** customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.

Example: *Risk Worksheet*

Step 2.4

ID	Risk Statement	Imp	Prob	RE
R1	**Insider Sends False Alerts**: IF an insider with malicious intent uses the CMSP infrastructure to send nonsense alert messages repeatedly, THEN customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.			
R2	**Inherited Replay Attack**: IF the carrier receives emergency alerts from an upstream replay attack on an AO and sends these messages repeatedly to customers in the designated geographic area, THEN customers could become annoyed with the carrier; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.			
R3	**Malicious Code in the Supply Chain**: IF malicious code (designed to disseminate alerts as broadly as possible and change the priority of all alerts into Presidential alerts) is inserted into the WEA alerting system by a supply-chain subcontractor, THEN customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.			
R4	**Denial of Service**: IF an outside actor with malicious intent uses a DoS attack on a carrier's WEA alerting system to prevent the dissemination of an alert about an impending physical terrorist attack, THEN people could be unaware of the attack and put in harm's way; the number of injuries and deaths could increase; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.			

Exercise 3: Threat Components

Turn to Exercise 3 in the tutorial workbook.

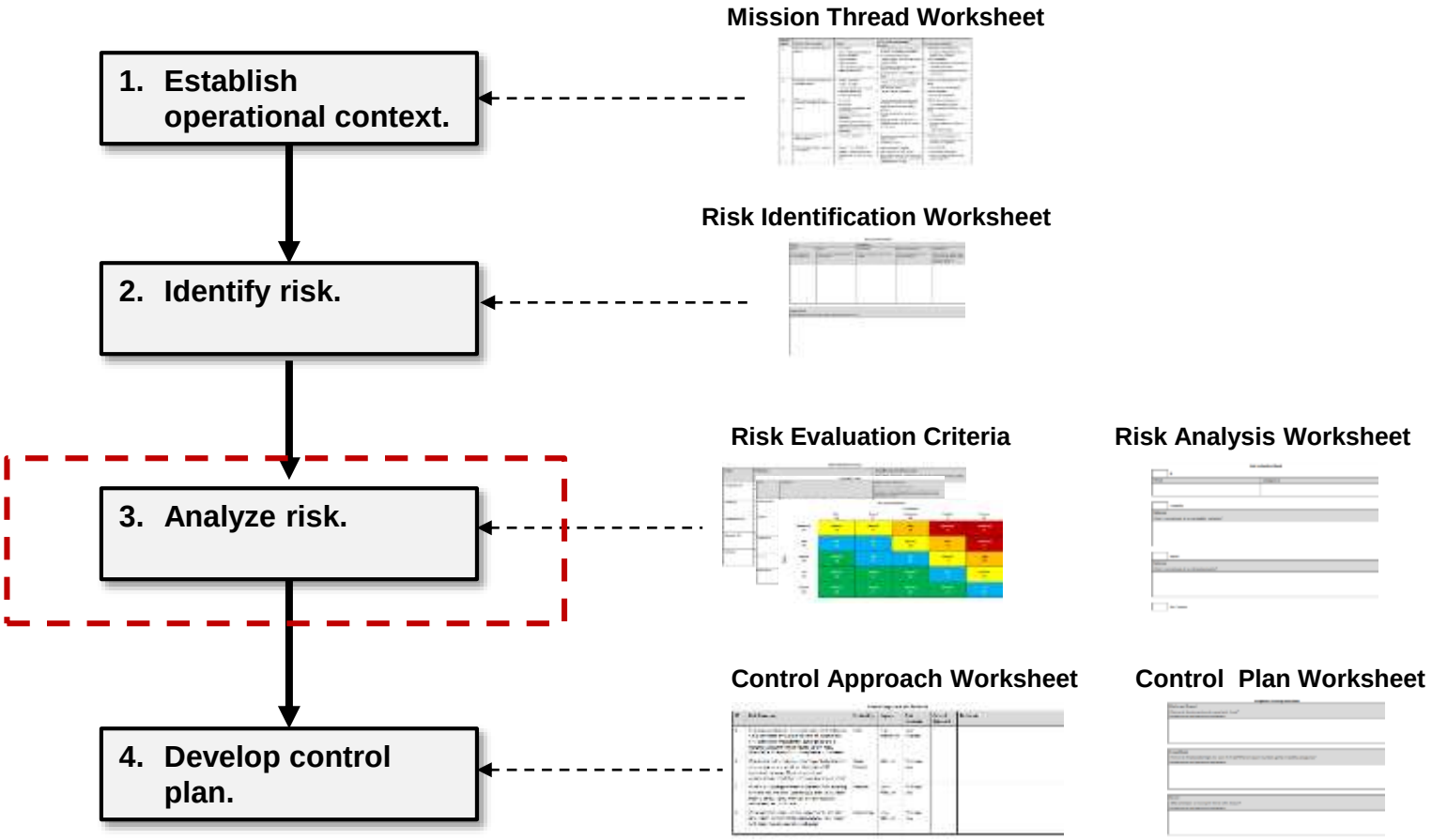
This exercise consists of a series of short scenarios describing threats to an Alert Originating System (AOS). For each scenario, do the following:

1. Read the scenario.
2. Identify the following elements of threat for the scenario from the information provided:
   - Actor
   - Motive
   - Enablers
   - Outcome

Security Engineering Risk Analysis (SERA) Tutorial

Analyze Risk (Task 3)

Analyze Risk (SERA Task 3)



Analyze Risk (SERA Task 3)

Each risk is analyzed in relation to predefined criteria.

Steps	
3.1	Establish probability.
3.2	Establish impact.
3.3	Determine risk exposure.

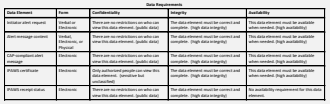
SERA Task 3: *Risk Measures*

Outcomes

- **Data disclosure (Confidentiality)**
- **Data modification (Integrity)**
- **Insertion of false data (Integrity)**
- **Destruction of data (Availability)**
- **Interruption of access to data (Availability)**

Produces

Mission Data



Targets

Technology Environment

Technology Infrastructure

Use Cases

Facilities

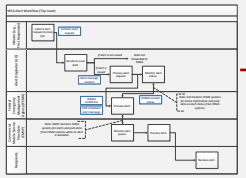
Entity of Interest

Exploits weaknesses and vulnerabilities

Threat Actor

Affects

Workflow / Mission Thread

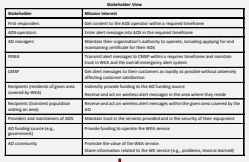


Produces

Adverse Mission Consequences / Losses

Affects

Stakeholder Interests



Produces

Adverse Stakeholder Consequences / Losses

Probability

Impact

Risk Exposure

SERA Task 3: *Risk Analysis Criteria*

Predefined criteria for risk analysis include:

- Probability evaluation criteria
- Impact evaluation criteria
- Risk exposure matrix

Each set of criteria must be tailored to represent the risk tolerance of key stakeholders.

The risk criteria presented in this section

- Apply to the WEA CMSP analysis
- Should be reviewed and tailored (if appropriate) before applying to other problem spaces

SERA Task 3: *Simplifying Assumptions*

To simplify the analysis, we make the following assumptions:

- Probability represents the likelihood that the threat will occur.
- Impact represents the most likely loss.

A threat can trigger a variety of potential consequences, for example

- Best case
- Worst case
- Most likely

Each potential consequence has associated impact and probability values.

- Evaluating multiple impact values complicates the analysis.
- The SERA Method focuses on the most likely impact to keep the risk analysis relatively simple (i.e., remove analysis of additional probabilities).

Step 3.1: *Establish Probability*

Step 3.1:

- The Analysis Team evaluates and documents the probability of occurrence for the threat.
  - Reviews the probability evaluation criteria that they established for the analysis
  - Assigns a probability measure to the likelihood that the threat will occur
  - Documents the rationale for selecting that probability measure

Probability evaluation criteria establish a set of qualitative measures for assessing the likelihood that the threat will occur.

- The Analysis Team defines a set of probability evaluation criteria when it is preparing to conduct the SERA Method.

Step 3.1: *Questions to Consider When Evaluating Probability*

How motivated is the actor?

Does the actor have the means to carry out the attack?

- Funding
- Technical skills
- Specialized technology

How complex is the threat?

Has this threat occurred successfully in the past? How often?

- Within the organization
- Across the community

Will the actor have the opportunity to carry out the attack?

Example: *Probability Evaluation Criteria*

Step 3.1

Value	Definition	Guidelines/Context/Examples
Frequent (5)	The threat occurs on numerous occasions or in quick succession. It tends to occur quite often or at close intervals.	≥ one time per month (≥ 12 / year)
Likely (4)	The threat occurs on multiple occasions. It tends to occur reasonably often, but not in quick succession or at close intervals.	
Occasional (3)	The threat occurs from time to time. It tends to occur “once in a while.”	~ one time per 6 months (~ 2 / year)
Remote (2)	The threat can occur, but it is not likely to occur. It has "an outside chance" of occurring.	
Rare (1)	The threat infrequently occurs and is considered to be uncommon or unusual. It is not frequently experienced.	≤ one time every 3 years (≤ .33 / year)

Example: *Probability Value for Risk 1*

Step 3.1

Probability Value:

- **Remote**

Rationale:

- The attack is moderately complex and requires moderate preparation to execute.
- The disgruntled insider must have physical access to a workstation with access to CMSP production code.
- The disgruntled insider must have the technical skills needed to execute the attack.
- The disgruntled insider must be familiar with the CMSP Gateway.
- The number of cyber attacks by disgruntled insiders continues to grow (i.e., an insider attack like this is not a rare event).
- Public data do not indicate that the probability is higher than remote.

Step 3.2: *Establish Impact*

Step 3.2:

- The Analysis Team evaluates and documents the impact for the security risk scenario.
  - Reviews the impact evaluation criteria that they established for the analysis
  - Assigns an impact measure to the scenario
  - Documents the rationale for selecting that measure

Impact evaluation criteria establish a set of qualitative measures for assessing the loss that will occur if the risk is realized.

- The Analysis Team defines a set of impact evaluation criteria when it is preparing to conduct the SERA Method.

Example: *Impact Evaluation Criteria*

Step 3.2

Value	Definition
Maximum (5)	The impact on the organization is severe. Damages are extreme in nature. Mission failure has occurred. Stakeholders will lose confidence in the organization and its leadership. The organization either will not be able to recover from the situation, or recovery will require an extremely large investment of capital and resources. Either way, the future viability of the organizational is in doubt.
High (4)	The impact on the organization is large. Significant problems and disruptions are experienced by the organization. As a result, the organization will not be able to achieve its current mission without a major re-planning effort. Stakeholders will lose some degree of confidence in the organization and its leadership. The organization will need to reach out to stakeholders aggressively to rebuild confidence. The organization should be able to recover from the situation in the long run. Recovery will require a significant investment of organizational capital and resources.
Medium (3)	The impact on the organization is moderate. Several problems and disruptions are experienced by the organization. As a result, the organization will not be able to achieve its current mission without some adjustments to its plans. The organization will need to work with stakeholders to ensure their continued support. Over time, the organization will be able to recover from the situation. Recovery will require a moderate investment of organizational capital and resources.
Low (2)	The impact on the organization is relatively small, but noticeable. Minor problems and disruptions are experienced by the organization. The organization will be able to recover from the situation and meet its mission. Recovery will require a small investment of organizational capital and resources.
Minimal (1)	The impact on the organization is negligible. Any damages can be accepted by the organization without affecting operations or the mission being pursued. No stakeholders will be affected. Any costs incurred by the organization will be incidental.

Example: *Impact Value*

Step 3.2

Impact Value:

- **Medium**

Rationale:

- Customers might not have much flexibility to change carriers easily, which can limit the potential for loss of business.
- Carriers already have help desk capabilities in place to respond to customer complaints.
- Tech-savvy customers can turn off the WEA service.
- The costs required to recover from this attack (e.g., remove the malicious code, perform public relations outreach) will not be excessive.
- Public data indicate that the impact of this type of attack is generally moderate.

Step 3.3: *Determine Risk Exposure*

Step 3.3:

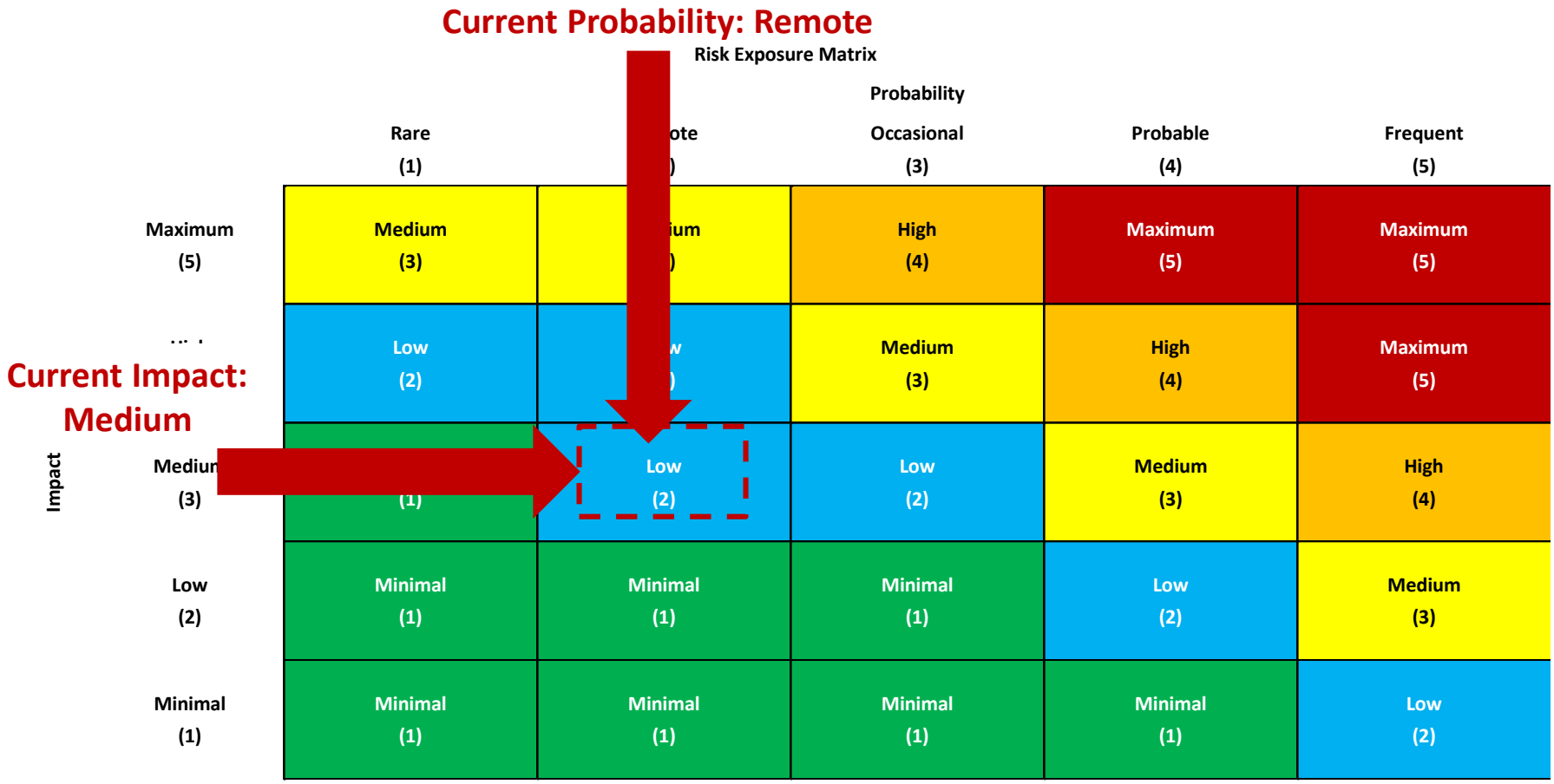
- The Analysis Team determines and documents the risk exposure for the security risk scenario.
  - Uses the risk exposure matrix established for the analysis
  - Maps the current values of probability and impact to the measurement scales on the matrix
  - Selects the risk exposure value where the current probability and impact values intersect

A risk exposure matrix provides a way of estimating the magnitude of a risk based on current values of probability and impact.

- The Analysis Team defines a risk exposure matrix when it is preparing to conduct the SERA Method.

SERA Task 3: *R1 Risk Analysis*

Step 3.3



Example: *Analyzed Risks*

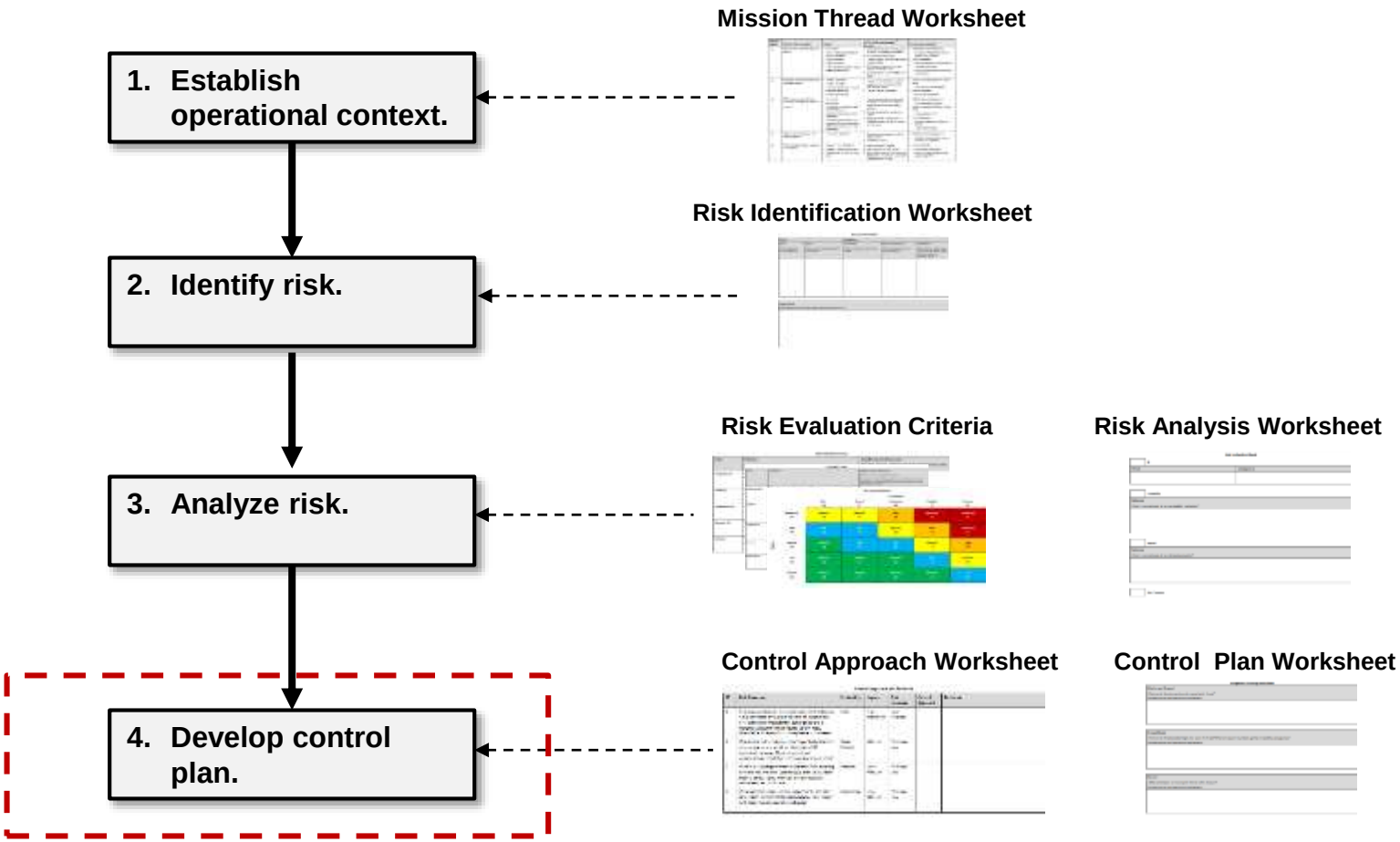
Step 3.3

ID	Risk Statement	Imp	Prob	RE
R1	**Insider Sends False Alerts**: IF an insider with malicious intent uses the CMSP infrastructure to send nonsense alert messages repeatedly, THEN customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Med	Remote	Low
R2	**Inherited Replay Attack**: IF the carrier receives emergency alerts from an upstream replay attack on an AO and sends these messages repeatedly to customers in the designated geographic area, THEN customers could become annoyed with the carrier; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Med	Remote	Low
R3	**Malicious Code in the Supply Chain**: IF malicious code (designed to disseminate alerts as broadly as possible and change the priority of all alerts into Presidential alerts) is inserted into the WEA alerting system by a supply-chain subcontractor, THEN customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Med	Rare	Min
R4	**Denial of Service**: IF an outside actor with malicious intent uses a DoS attack on a carrier's WEA alerting system to prevent the dissemination of an alert about an impending physical terrorist attack, THEN people could be unaware of the attack and put in harm's way; the number of injuries and deaths could increase; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Max	Rare	Med

Security Engineering Risk Analysis (SERA) Tutorial

Develop Control Plan (Task 4)

Develop Control Plan (SERA Task 4)



Develop Control Plan (SERA Task 4)

A strategy for controlling each risk is determined.

Control plans are developed and documented for all security risks that are not accepted.

Steps	
4.1	Prioritize risks.
4.2	Select control approach.
4.3	Establish control actions.

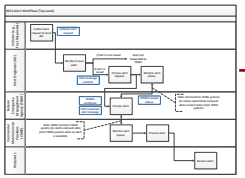
SERA Task 4: *Controls*

Outcomes

- **Data disclosure (Confidentiality)**
- **Data modification (Integrity)**
- **Insertion of false data (Integrity)**
- **Destruction of data (Availability)**
- **Interruption of access to data (Availability)**

Affects

Workflow / Mission Thread

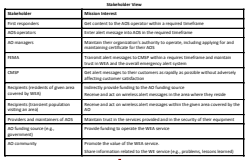


Produces

Adverse Mission Consequences / Losses

Affects

Stakeholder Interests

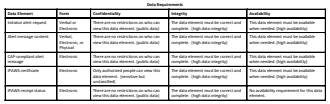


Produces

Adverse Stakeholder Consequences / Losses

Produces

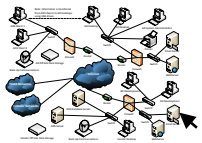
Mission Data



Targets

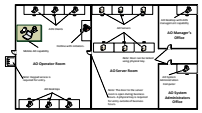
Technology Environment

Technology Infrastructure



Use Cases

Facilities



Entity of Interest

Reduce mission consequence amplifiers

Reduce stakeholder consequence amplifiers

Controls

Reduce threat enablers (e.g., weaknesses, vulnerabilities)

Exploits weaknesses and vulnerabilities

Threat Actor

Step 4.1: *Prioritize Risks*

Step 4.1:

- The Analysis Team prioritizes all security risk scenarios based on their impact, probability, and risk exposure measures.
- The team documents the ranked risk scenarios in a tracking spreadsheet.

Example: *Prioritization Criteria*

Step 4.1

Analysis Team used the following guidelines for prioritizing the list of WEA risks:

- Impact is the primary factor for prioritizing security risks.
  - Risks with the largest impacts are deemed to be of highest priority.

- Probability is the secondary factor for prioritizing security risks.
  - It is used to prioritize risks that have equal impacts.
    - Risks of equal impact with the largest probabilities are considered to be the highest priority risks.

Example: *Prioritized Risk Spreadsheet*

Step 4.1

ID	Risk Statement	Imp	Prob	RE
R4	**Denial of Service**: IF an outside actor with malicious intent uses a DoS attack on a carrier's WEA alerting system to prevent the dissemination of an alert about an impending physical terrorist attack, THEN people could be unaware of the attack and put in harm's way; the number of injuries and deaths could increase; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Max	Rare	Med
R1	**Insider Sends False Alerts**: IF an insider with malicious intent uses the CMSP infrastructure to send nonsense alert messages repeatedly, THEN customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Med	Remote	Low
R2	**Inherited Replay Attack**: IF the carrier receives emergency alerts from an upstream replay attack on an AO and sends these messages repeatedly to customers in the designated geographic area, THEN customers could become annoyed with the carrier; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Med	Remote	Low
R3	**Malicious Code in the Supply Chain**: IF malicious code (designed to disseminate alerts as broadly as possible and change the priority of all alerts into Presidential alerts) is inserted into the WEA alerting system by a supply-chain subcontractor, THEN customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Med	Rare	Min

Step 4.2: *Select Control Approach*

Step 4.2:

- The Analysis Team determines how it will handle each risk.
  - Accept
    - If a risk is accepted, its consequences will be tolerated; no proactive action to address the risk will be taken.
  - Control
    - If the team decides to take action to control a risk, it will develop a control plan for that risk in Step 4.3.
    - The team documents its control approach and the rationale for selecting that approach.

Example: *Control Approach*

Step 4.2

Control Approach:

- **Control**

Rationale:

- This risk will be actively controlled. Reasons for developing a control plan include the following:
  - A motivated insider with the right set of technical skills could easily execute this attack. An effective set of controls will reduce the probability of occurrence.
  - The impact of this risk (i.e., moderate) is high enough to warrant taking action. An effective set of controls will reduce the impact of and recovery costs for this risk.
  - This risk affects the customer base and could affect the reputation of the carrier, which makes addressing it a strategic priority for the carrier. The carrier needs to show due diligence in controlling this type of risk.

Example: *Risk Spreadsheet with Control Decisions*

Step 4.2

ID	Risk Statement	Imp	Prob	RE	Appr
R4	**Denial of Service**: IF an outside actor with malicious intent uses a DoS attack on a carrier's WEA alerting system to prevent the dissemination of an alert about an impending physical terrorist attack, THEN people could be unaware of the attack and put in harm's way; the number of injuries and deaths could increase; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Max	Rare	Med	Control
R1	**Insider Sends False Alerts**: IF an insider with malicious intent uses the CMSP infrastructure to send nonsense alert messages repeatedly, THEN customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Med	Remote	Low	Control
R2	**Inherited Replay Attack**: IF the carrier receives emergency alerts from an upstream replay attack on an AO and sends these messages repeatedly to customers in the designated geographic area, THEN customers could become annoyed with the carrier; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Med	Remote	Low	Control
R3	**Malicious Code in the Supply Chain**: IF malicious code (designed to disseminate alerts as broadly as possible and change the priority of all alerts into Presidential alerts) is inserted into the WEA alerting system by a supply-chain subcontractor, THEN customers could become annoyed with the carrier; the carrier could incur considerable costs to recover from the attack; the carrier's reputation could be tarnished; and public trust in the WEA service could erode.	Med	Rare	Min	Control

Step 4.3: *Establish Control Actions*

Step 4.3:

- The Analysis Team defines and documents a plan for all risks that are being controlled.
- At this point, the team can begin to prioritize controls (across all control plans) and begin to implement the highest priority actions.

Control Plan: *Key Questions*

Step 4.3

Threat Steps

- What controls are recommended to counteract conditions and circumstances that facilitate the execution of each threat step (i.e., enablers)?

Consequences

- What controls are recommended to counteract conditions and circumstances that propagate or increase each consequence (i.e., amplifiers)?

Note: Consider controls intended to

- Recognize and respond to threats
- Resist the threat and potential consequences
- Recover from consequences when they occur

Example: *Controls for Threat Step 3*

Step 4.3

Threat Step

T3. The insider develops a logic bomb designed to replay a nonsense CMAM message repeatedly.

Focus

Technology

CMSP Gateway (focus of the logic bomb)

Enabler

An employee that has technical skills can use those skills to inflict damage on information systems.

Control

The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.

Example: *Controls for Threat Step 4*

Step 4.3

Threat Step

T4. The insider uses a colleague's workstation to check-in the modified code with the logic bomb.

Focus

Organization

Carrier's physical security practices

Technology

Workstation security; CMSP Gateway; Change management system

Enablers

Leaving a workstation unattended while logged in can allow malicious actors to gain illegitimate access to information and services.

An insufficient change management/ configuration management capability can prevent the carrier from knowing if software has been modified inappropriately.

Control

The carrier implements physical access controls for workstations and workspaces.

Controls

The carrier implements/improves a change management/configuration management system.

The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.

Example: *Risk 1 Threat Table (Excerpt)*

Step 4.3

Threat Step (Risk 1)		Focus	Enabler	Candidate Control
T1.	The insider is upset upon learning that he is not receiving a bonus this year and has been passed over for a promotion.	Organization Carrier—human resource practices	A lack of proper feedback provided to an employee can result in the employee being unaware of performance issues that could affect his/her career.	The carrier's managers are trained to provide constructive feedback on performance issues.
T2.	The insider begins to behave aggressively and abusively toward his coworkers.	Organization Carrier—human resource practices	An employee's inappropriate behavior can be an indicator of more serious actions.	The carrier's managers recognize inappropriate behavior when it occurs and respond appropriately.
T3.	The insider develops a logic bomb designed to replay a nonsense CMAM message repeatedly.	Technology CMSP Gateway (focus of the logic bomb)	An employee that has technical skills can use those skills to inflict damage on information systems.	The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.
T4.	The insider uses a colleague's workstation to check-in the modified code with the logic bomb.	Organization Carrier's physical security practices Technology Workstation security (e.g., screen locking) CMSP Gateway Change management/ configuration management system	Leaving a workstation unattended while logged in can allow malicious actors to gain illegitimate access to information and services.	The carrier implements physical access controls for workstations and workspaces.
			An insufficient change management/configuration management capability can prevent the carrier from knowing if software has been modified inappropriately.	The carrier implements/improves a change management/configuration management system.
				The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.

Example: *Controls for a Workflow Consequence*

Step 4.3

Consequence
The carrier's infrastructure forwards the nonsense WEA message repeatedly to mobile devices in the targeted geographic area.

Workflow Actor
Carrier infrastructure

Amplifier
Insufficient monitoring of the network for abnormal activity can result in a delayed response to the attack (e.g., no response until customer complaints are received).

Controls
The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.

The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.

The carrier implements an incident response capability to minimize the consequences of the event.

Example: *Risk 1 Workflow Consequence Table*

Step 4.3

Consequence	Workflow Actor	Amplifier	Candidate Control
The carrier's infrastructure forwards the nonsense WEA message repeatedly to mobile devices in the targeted geographic area.	Carrier infrastructure	Insufficient monitoring of the network for abnormal activity can result in a delayed response to the attack (e.g., no response until customer complaints are received).	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.
			The carrier maintains situational awareness of the WEA environment and responds to any issues appropriately.
			The carrier implements an incident response capability to minimize the consequences of the event.
People with WEA-capable mobile devices supported by the carrier receive the nonsense message.	Mobile devices	Enabling the WEA service on a mobile device allows the owner of that device to receive CMAM messages.	Recipients can disable the WEA service on their mobile devices.

Example: *Controls for a Stakeholder Consequence*

Step 4.3

Consequence

Recipients of the message quickly become annoyed at receiving the same nonsense message repeatedly.

Stakeholder

Recipients

Amplifier

Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients.

Controls

The carrier implements incident response capability plan to minimize the consequences of the event.

The carrier controls access to sensitive information based on organizational role.

Example: *Risk 1 Stakeholder Consequence Table (Excerpt)*

Step 4.3

Consequence	Stakeholder	Amplifier	Candidate Control
Recipients of the message quickly become annoyed at receiving the same nonsense message repeatedly.	Recipients	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients	The carrier implements incident response capability plan to minimize the consequences of the event.
			The carrier controls access to sensitive information based on organizational role.
Many recipients complain to the carrier's customer service operators.	Recipients	Knowledge of the system's geo-targeting capability can enable the attacker to expand the geographic area being targeted and affect a greater number of recipients.	The carrier implements a recovery plan to minimize the consequences of the event.
			The carrier controls access to sensitive information based on organizational role.
			The carrier's customer service operators are trained in handling complaints about incorrect or errant WEA alerts.
A large number of recipients turn off the WEA function on their phones. Many will not turn the WEA service back on.	FEMA Carrier	People's ability to disable the WEA service on their mobile devices helps them deal with the attack. They might decide not to (or might forget to) re-enable the WEA service after the attack.	The carrier implements a recovery plan to minimize the consequences of the event.

Example: *CMSP Cybersecurity Guidelines*

Step 4.3

The CMSP Cybersecurity Guidelines comprise 35 high-priority security controls that address the four WEA risk scenarios included in this study

Controls were identified in the following areas:

- Human Resources
- Training
- Contracting
- Physical Security
- Change Management
- Access Control
- Information Management
- Vulnerability Management
- System Architecture
- System Configuration
- Code Analysis
- Technical Monitoring
- Independent Reviews
- Incident Response
- Disaster Recovery

SERA Task 4: *Control-to-Risk Mapping (Excerpt)*

Step 4.3

Category	Control	R1	R2	R3	R4
Human Resources	The carrier's managers are trained to provide constructive feedback on performance issues.	X			
	The carrier's managers recognize inappropriate behavior when it occurs and respond appropriately.	X			
	The carrier performs targeted monitoring of individuals with suspected behavioral issues and responds appropriately.	X			
Physical Security	The carrier implements physical access controls for workstations and workspaces.	X			
System Architecture	Security controls are implemented in systems and network devices based on cybersecurity risk.				X
	The carrier's WEA alerting system has a backup capability that uses a separate communication channel.				X
Technical Monitoring	The carrier monitors messages for suspicious content (e.g., illegitimate messages, duplicate messages) and responds appropriately.	X	X	X	
	The carrier monitors its network for abnormal activity (e.g., abnormal traffic patterns, spikes in traffic) and responds appropriately.	X	X	X	X
Contracting	All contracts with third parties specify security standards that must be met.			X	X

Controls with Design Implications

Step 4.3

Access Control

- The carrier controls access to sensitive information based on organizational role.

System Architecture

- The carrier's WEA alerting system has a backup capability that uses a separate communication channel.

Technical Monitoring

- The carrier monitors messages for suspicious content (e.g., illegitimate messages, duplicate messages) and responds appropriately.
- The carrier monitors the WEA alerting system for abnormal activity and responds appropriately.

Exercise 4: *Control Planning*

Turn to Exercise 4 in the tutorial workbook.

Read the security risk scenario and supporting information provided:

- Context
- Threat sequence
- Workflow consequences
- Stakeholder consequences

Think about conditions that might enable the threat or amplify consequences.

Answer the following questions:

- What controls would you suggest to reduce the risk described in this scenario? Why?

Security Engineering Risk Analysis (SERA) Tutorial

Summary

Key Points - 1

Cybersecurity engineering integrates the following technical perspectives:

- Operational security
- System and software engineering

75% of the Top 25 Common Weakness Enumerations (CWEs) are caused by design weaknesses (not coding issues).

Interactions among software components must be managed.

- Software components are often related sets of layered functionality. (One layer is not contained inside another layer.)
- Security properties relate to composite interactions among multiple components (not to individual components).

Key Points - 2

System and mission dependency on software is increasing. For example,

- 1960 – 8% of the F-4 aircraft functionality
- 1982 – 45% of the F16 aircraft functionality
- 2000 – 80% of the F-22 aircraft functionality

Three main security attributes:

- Confidentiality
- Integrity
- Availability

Security risk is a measure of the

1. Likelihood that a threat will exploit a vulnerability to produce an adverse consequence, or loss
2. Magnitude of the loss

Key Points - 3

Three components of security risk:

- Threat
- Vulnerability
- Consequence

Key limitations of traditional software security risk analysis:

- Simplistic risk analysis
- Ad hoc risk analysis

SERA defines a systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain.

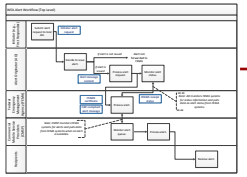
SERA Method: *Developing Security Risk Scenarios*

Outcomes

- **Data disclosure (Confidentiality)**
- **Data modification (Integrity)**
- **Insertion of false data (Integrity)**
- **Destruction of data (Availability)**
- **Interruption of access to data (Availability)**

Affects

Workflow / Mission Thread

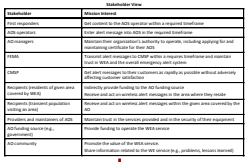


Produces

Adverse Mission Consequences / Losses

Affects

Stakeholder Interests

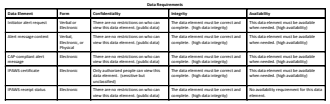


Produces

Adverse Stakeholder Consequences / Losses

Produces

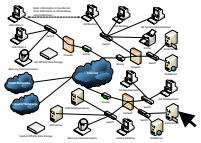
Mission Data



Targets

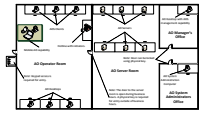
Technology Environment

Technology Infrastructure



Use Cases

Facilities



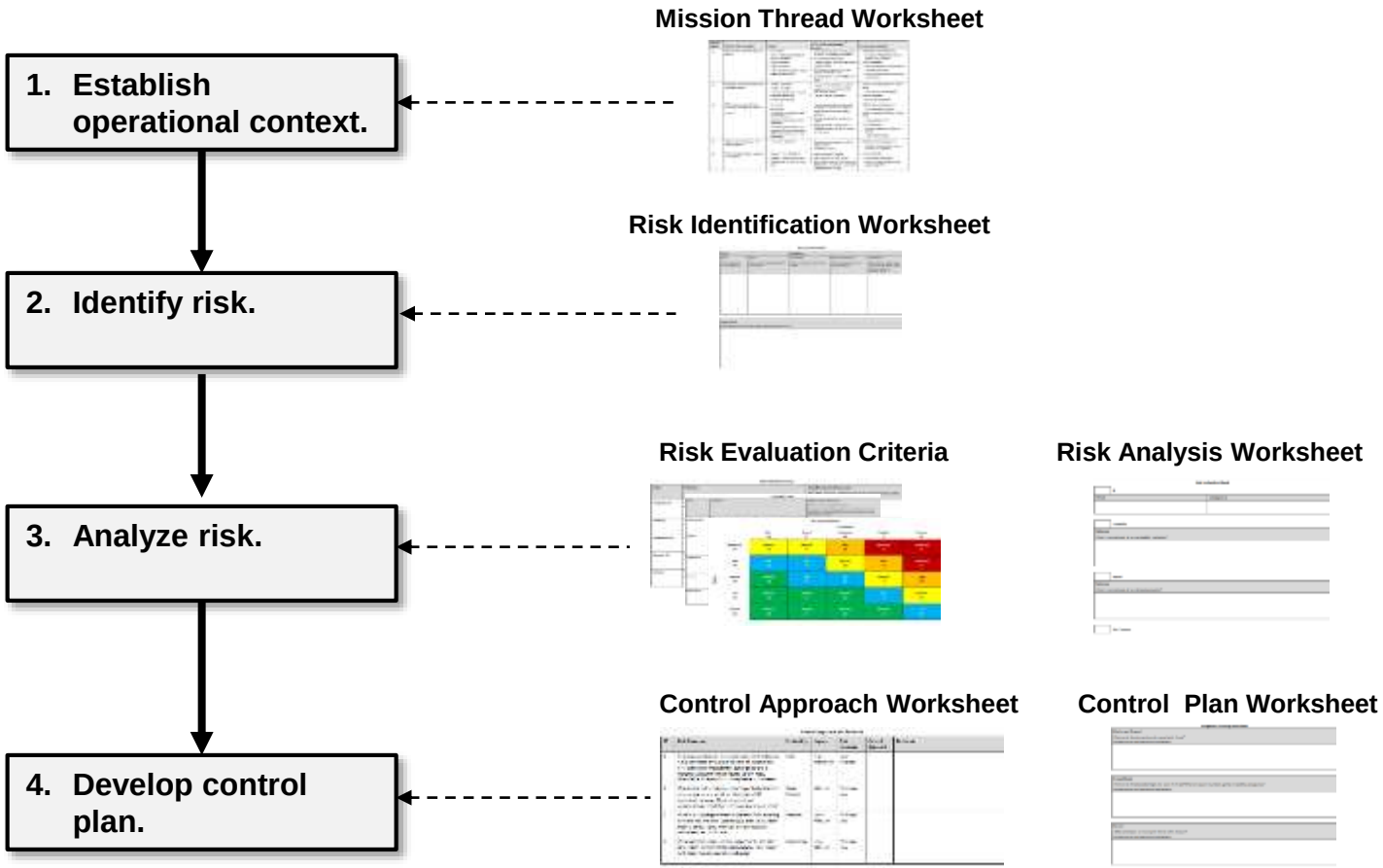
Entity of Interest

Exploits weaknesses and vulnerabilities

Threat Actor

SERA requires the development of security risk scenarios to analyze the mission impact of data security breaches.

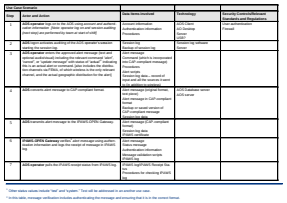
SERA Method: *Four Tasks*



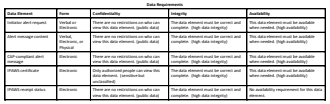
SERA Method: *Developing Security Risk Scenarios*

Threat Identification Models

Use-Case View

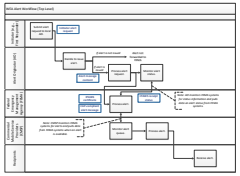


Data View



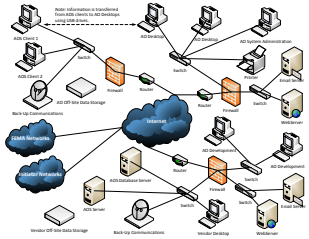
Consequence Analysis Models

Workflow View

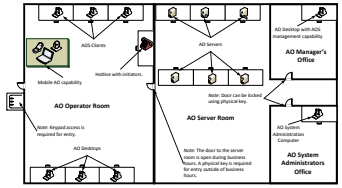


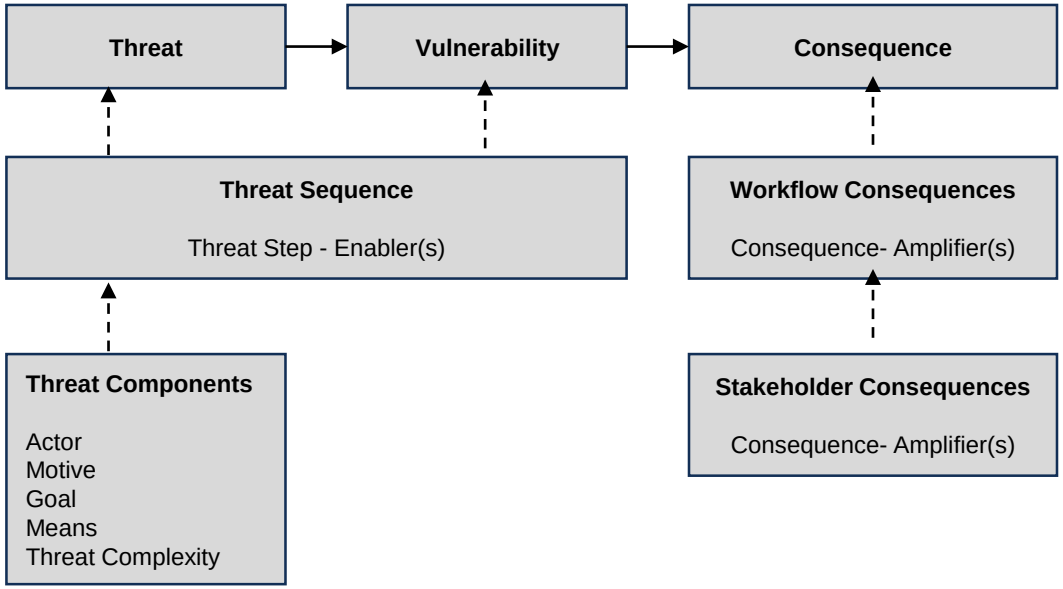
Stakeholder View

Technology View



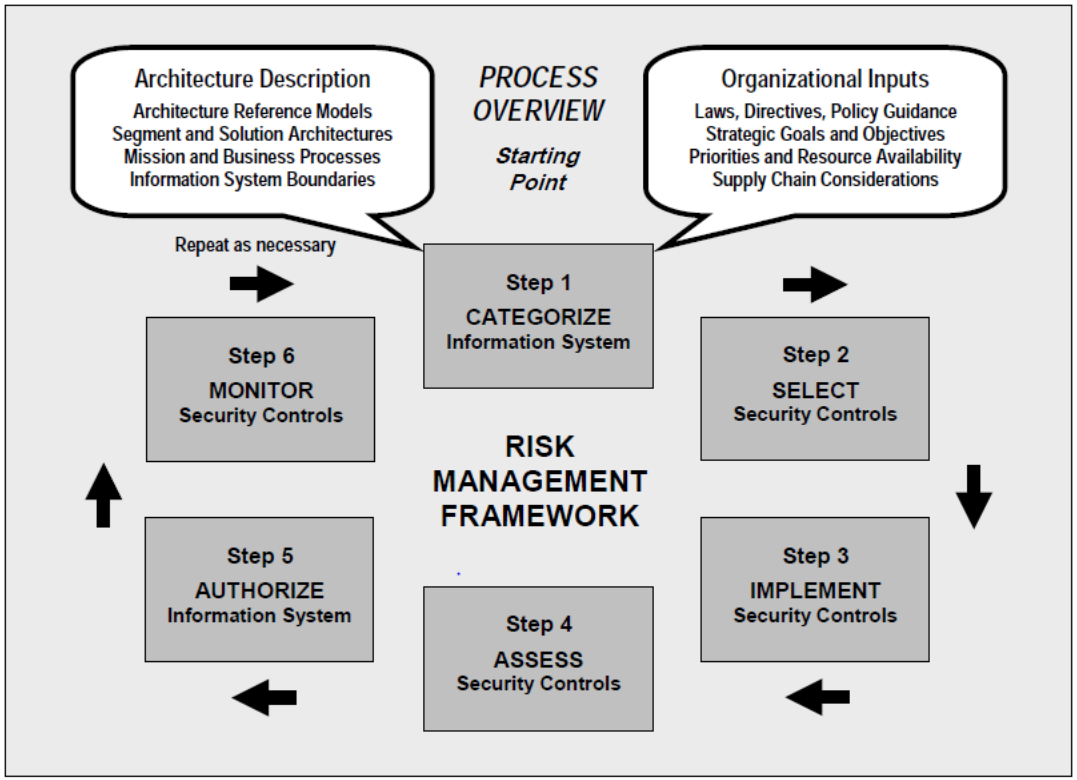
Physical View





NIST Risk Management Framework (RMF)[1]

The SERA Method supports Steps 1 and 2 of the of the NIST RMF.

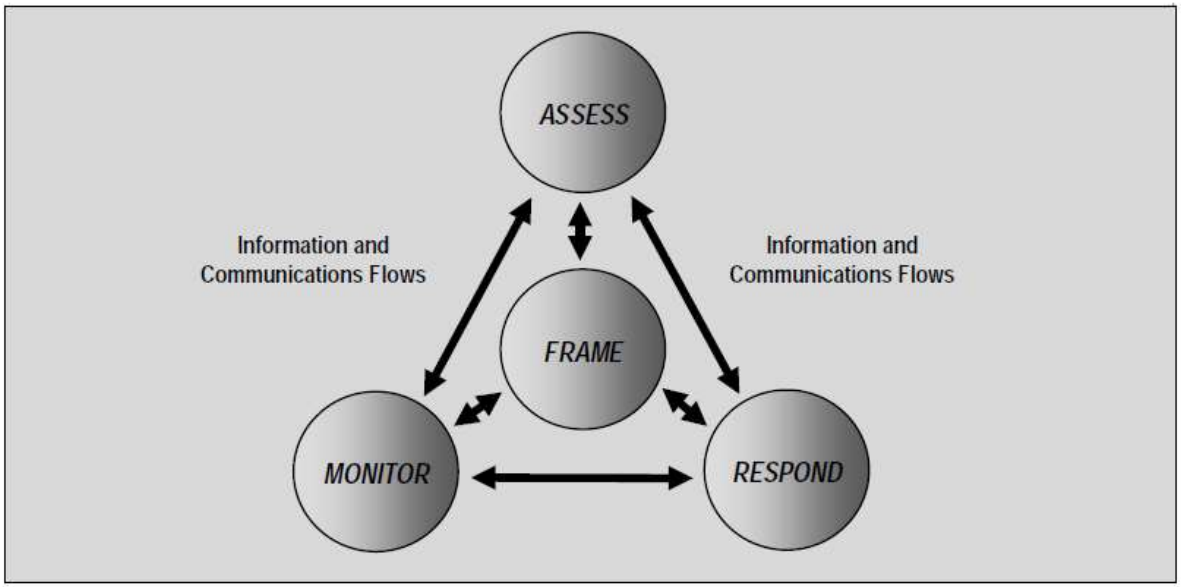


1. National Institute of Standards and Technology. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (NIST Special Publication 800-37 Revision 1). Gaithersburg, MD, National Institute of Standards and Technology, 2014.

NIST Risk Assessment Process1

The SERA Method addresses

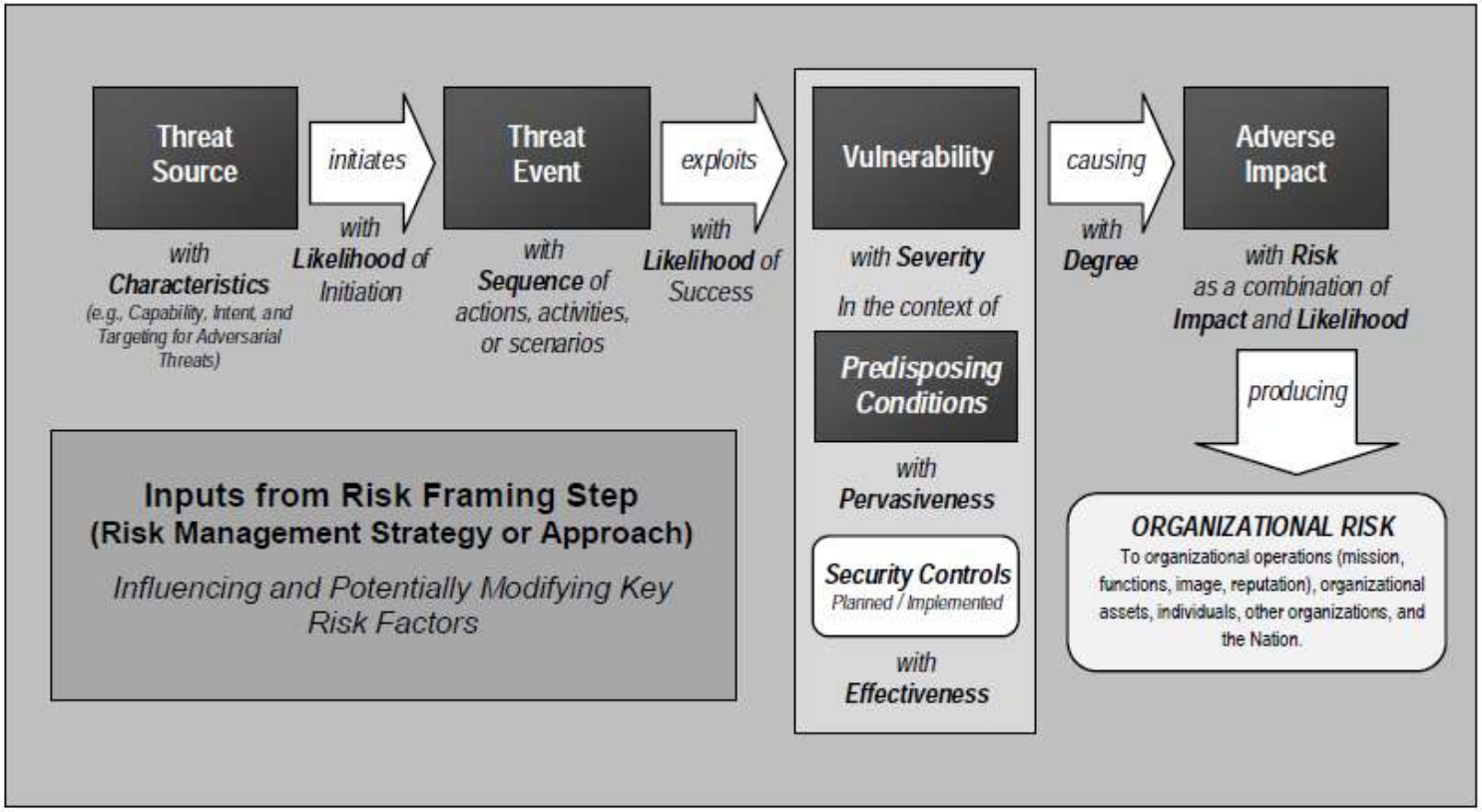
- The Frame and Assess components of the NIST risk assessment process.
- Most aspects of the Respond component



1. National Institute of Standards and Technology. *Guide for Conducting Risk Assessments* (NIST Special Publication 800-30 Revision 1). Gaithersburg, MD, National Institute of Standards and Technology, 2012.

NIST Risk Model[1]

SERA's underlying risk model is consistent with the NIST risk model.



1. National Institute of Standards and Technology. *Guide for Conducting Risk Assessments* (NIST Special Publication 800-30 Revision 1). Gaithersburg, MD, National Institute of Standards and Technology, 2012.

Key Features of the SERA Method

Implements a scenario-based structure for documenting cybersecurity risks

- Establishes a baseline of operational performance to inform cybersecurity risk identification
- Assembles a shared organizational view (business and technical) of cybersecurity risk

Enables identification and correction of design weaknesses before a system is deployed

- Reduces residual cybersecurity risk in deployed software-reliant systems
- Enables more effective management of cybersecurity risks to operational missions

Helps to ensure consistency with standards and regulations, such as the NIST Risk Management Framework (RMF)

SERA Method: *Key Publications*

Alberts, C.; Woody, C.; & Dorofee, A. Wireless Emergency Alerts Commercial Mobile Service Provider (CMSP) Cybersecurity Guidelines (CMU/SEI-2016-SR-009). Software Engineering Institute, Carnegie Mellon University, 2016.

Software Engineering Institute, WEA Project Team. Wireless Emergency Alerts (WEA) Cybersecurity Risk Management Strategy for Alert Originators (CMU/SEI-2013-SR-018). Software Engineering Institute, Carnegie Mellon University, 2014.

Alberts, C.; Woody, C.; & Dorofee, A. Introduction to the Security Engineering Risk Analysis (SERA) Framework (CMU/SEI-2014-TN-025). Software Engineering Institute, Carnegie Mellon University, 2014.

Woody, C.; & Alberts, C. “Evaluating Security Risks using Mission Threads.” CrossTalk 10, 2 (September/October 2014): 14-19.

Software Engineering Institute | Carnegie Mellon University