Practical Software and Systems Measurement

A foundation for objective project management

Measurement of Safety & Security Processes

PSM TWG Meeting
20 July 2005 / 14:15 – 17:30
21 July 2005 / 08:30 – 12:00
Paul Caseley, John Murdoch

Objectives of the Workshop

- *to assess PSM work to date (White Paper v2.0) and draw up recommendations for further work*
- *to define a plan of action for maturing measurement proposals and their take-up*
- *to identify beneficial collaborations between the PSM project effort and related programs; to define the role of the PSM project in security measurement*
- *to seek participation/ opportunities for trials, case studies and assessments*

Topics

1. Review of proposed Security Measurement framework (White Paper v2): what’s missing?
2. Information needs: how can we measure the benefit of security investment? Key Indicators: what do we need to know, as a minimum, to manage security operations and engineering?
3. Development of practical advice: security measurement process, measurement information specifications
4. Next Steps: what are the priority tasks, collaboration, trials etc ?

Workshop Format Wed 20 July

Agenda (pm)

14:15 Introduction

14:30 Topic 1 Review of proposed Security Measurement framework (White Paper v2): what's missing?

15:45 – 16:00 Break

16:00 Topic 2 Information needs: how can we measure the benefit of security investment? Key Indicators: what do we need to know, as a minimum, to manage security operations and engineering?

17:30 Close

Workshop Format Thu 21 July

Agenda (am)

08:30 Topic 3 Development of practical advice: security measurement process, measurement information specifications

10:15 – 10:30 break

10:30 Topic 4 Next Steps: what are the priority tasks, collaboration, trials etc ?

11:45 Wrap up - workshop outbrief

12:00 Close

Intended Output

1. Review and assess White Paper v2 – improvements, omissions
2. Measurement of benefit – main elements

   management - key indicators
3. Practical advice - components
4. Next steps

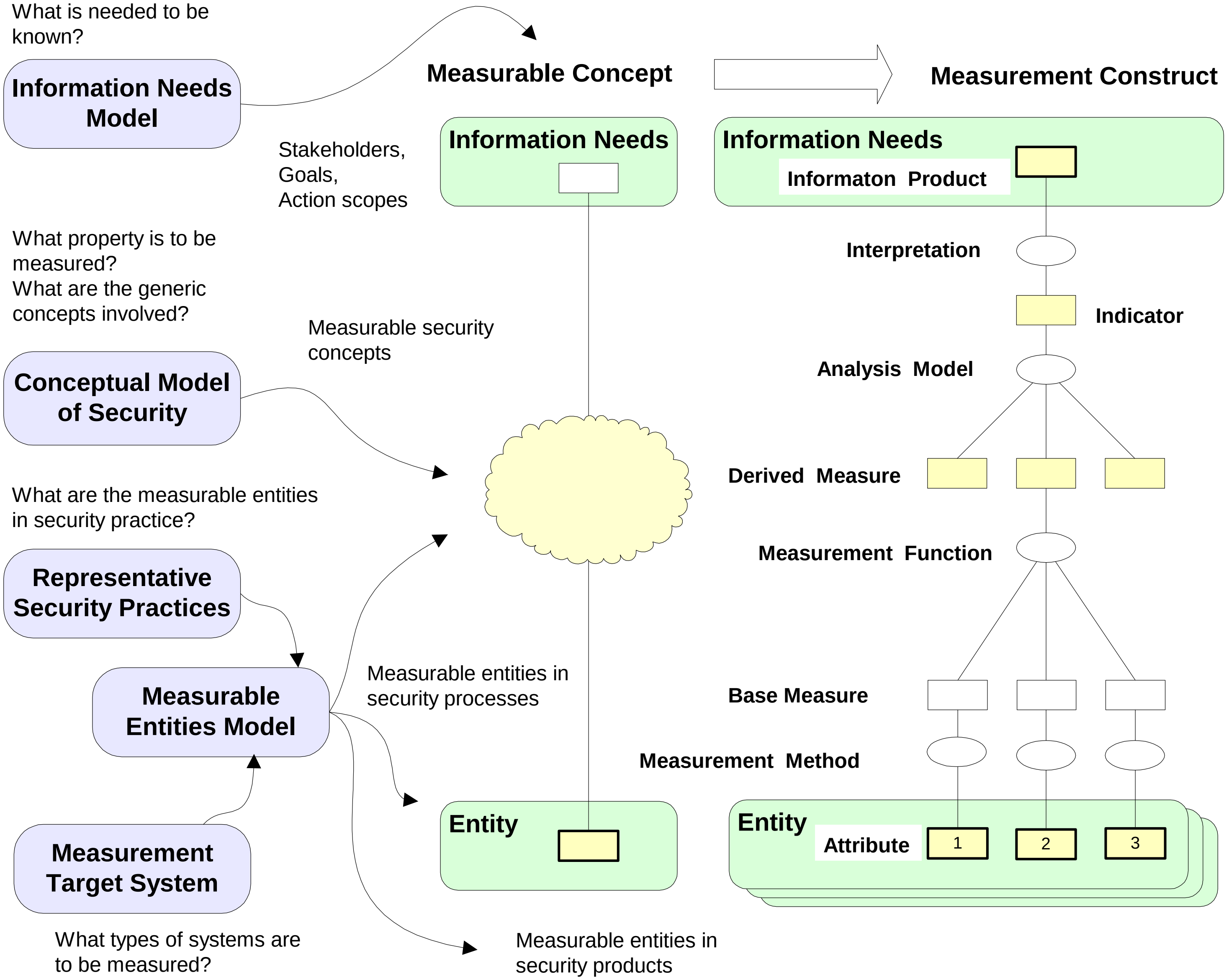
Workshop Background

- *TWG met in February and July 2004 and March 2005 PSM workshops to consider security*
- *Security Measurement White Paper, v 1.0 issued 30th November 2004, updated to v 2.0 12th July 2005*
- *Safety measurement considered through 2003. Safety White Paper v2.0 issued 13th February 2004, to be updated to v3.0 by September 2005*

Topic 1 Review of proposed Security Measurement framework (White Paper v2)

Is the proposed framework along the right lines? How can it be improved? What's missing?

Practical Software and Systems Measurement



What is needed to be known?

Information Needs Model

Measurable Concept

Measurement Construct

Stakeholders,
Goals,
Action scopes

Information Needs

Information Needs

Informaton Product

What property is to be measured?
What are the generic concepts involved?

Interpretation

Indicator

Measurable security concepts

Analysis Model

Conceptual Model of Security

Derived Measure

What are the measurable entities in security practice?

Measurement Function

Representative Security Practices

Measurable Entities Model

Measurable entities in security processes

Base Measure

Measurement Method

Entity

Entity

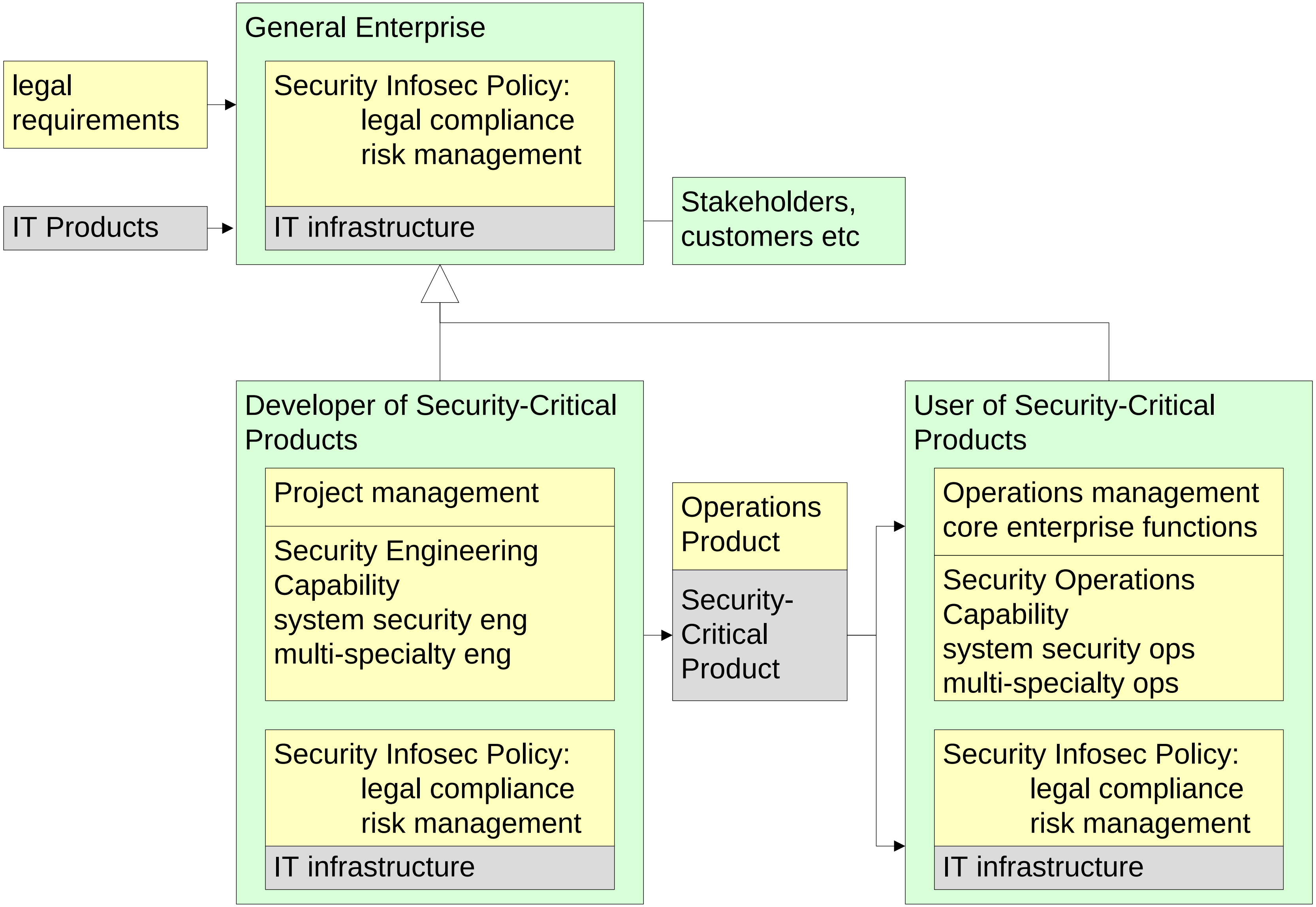
Attribute

Measurement Target System

What types of systems are to be measured?

Measurable entities in security products

Practical Software and Systems Measurement



legal requirements

IT Products

General Enterprise

Security Infosec Policy:
legal compliance
risk management

IT infrastructure

Stakeholders, customers etc

Developer of Security-Critical Products

Project management

Security Engineering Capability
system security eng
multi-specialty eng

Security Infosec Policy:
legal compliance
risk management

IT infrastructure

Operations Product

Security-Critical Product

User of Security-Critical Products

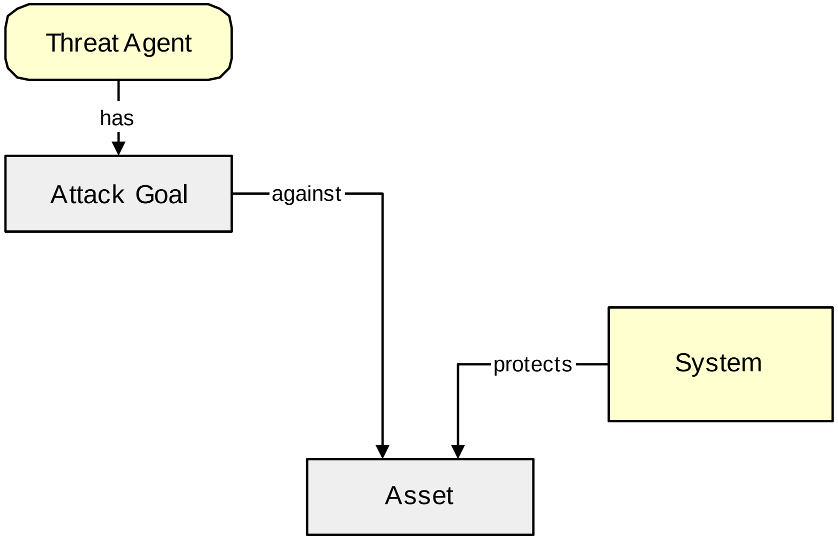
Operations management
core enterprise functions

Security Operations Capability
system security ops
multi-specialty ops

Security Infosec Policy:
legal compliance
risk management

IT infrastructure

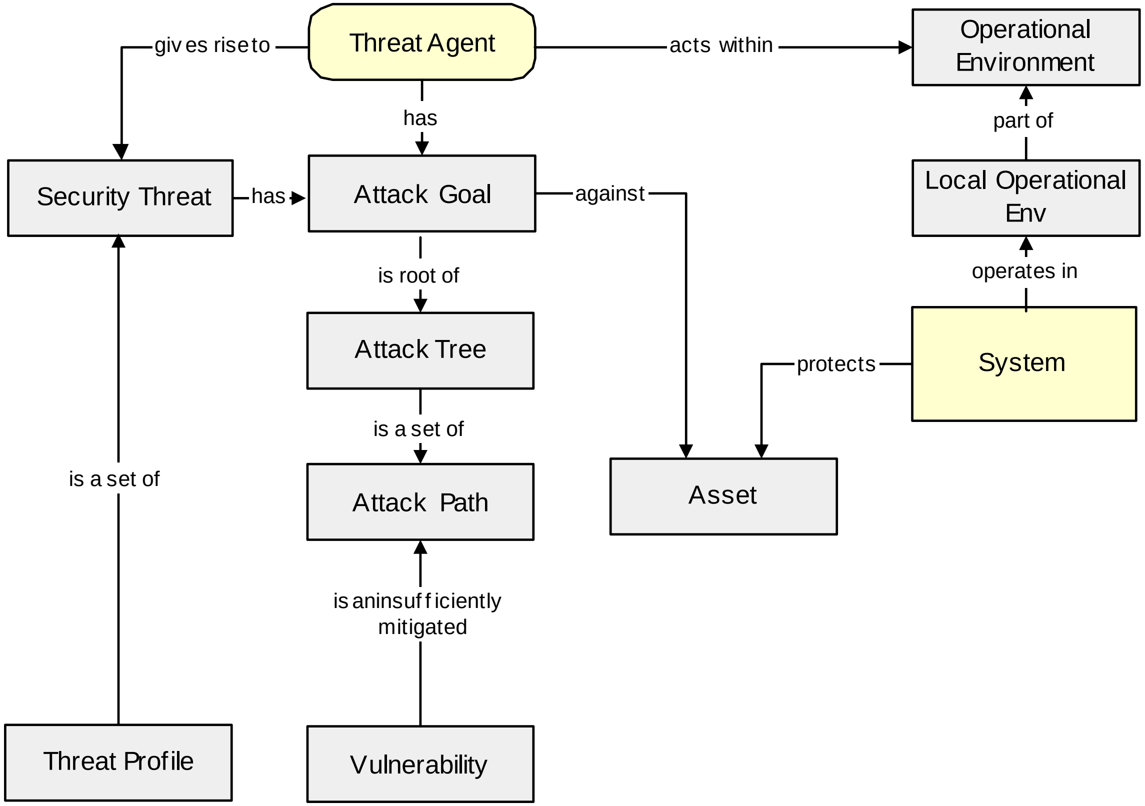
Information Model



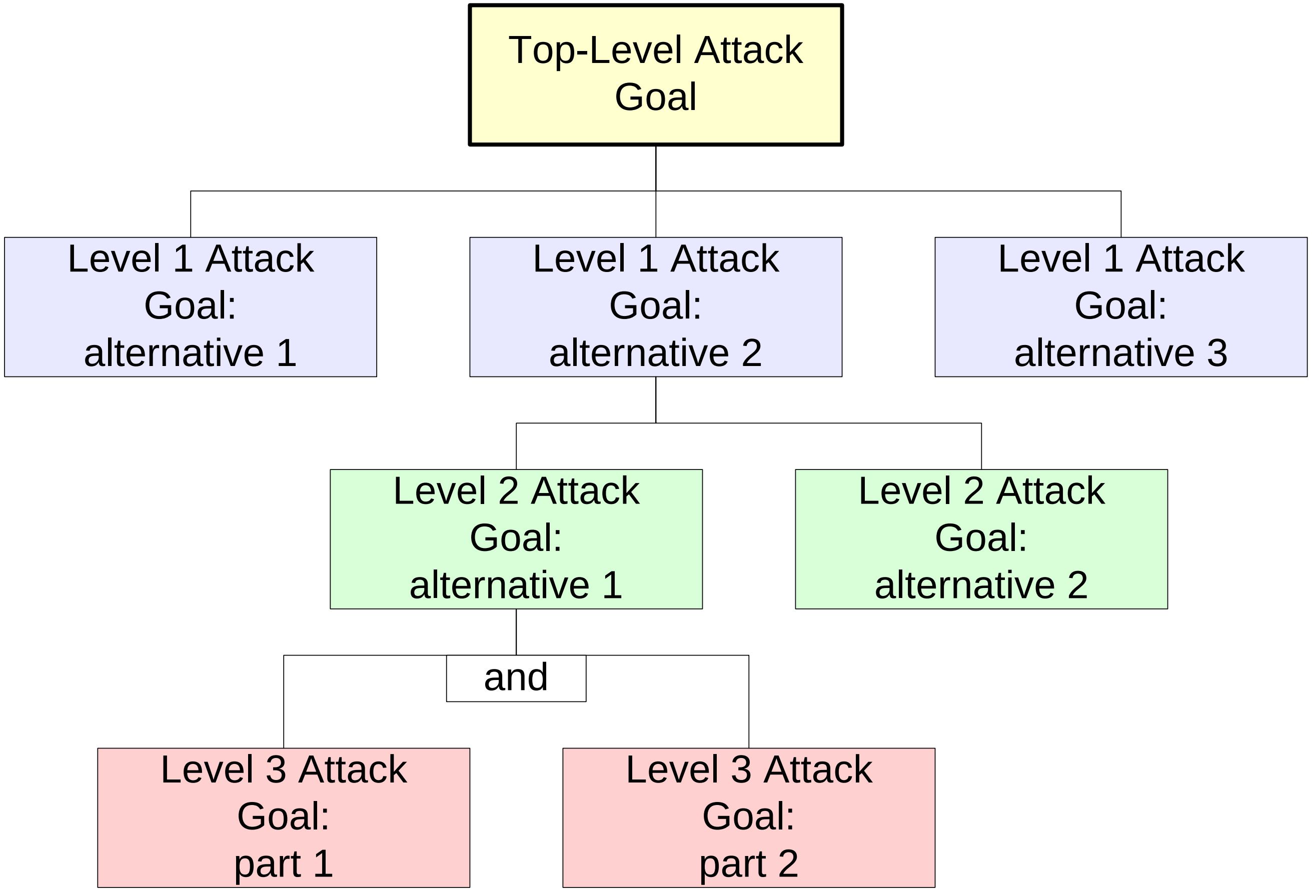
Inspired by

Firesmith D.G., Common Concepts underlying safety, security and survivability engineering, CMU/SEI-2003-TN-033

Practical Software and Systems Measurement



Threat Tree



Top-Level Attack Goal

Level 1 Attack Goal: alternative 1

Level 1 Attack Goal: alternative 2

Level 1 Attack Goal: alternative 3

Level 2 Attack Goal: alternative 1

Level 2 Attack Goal: alternative 2

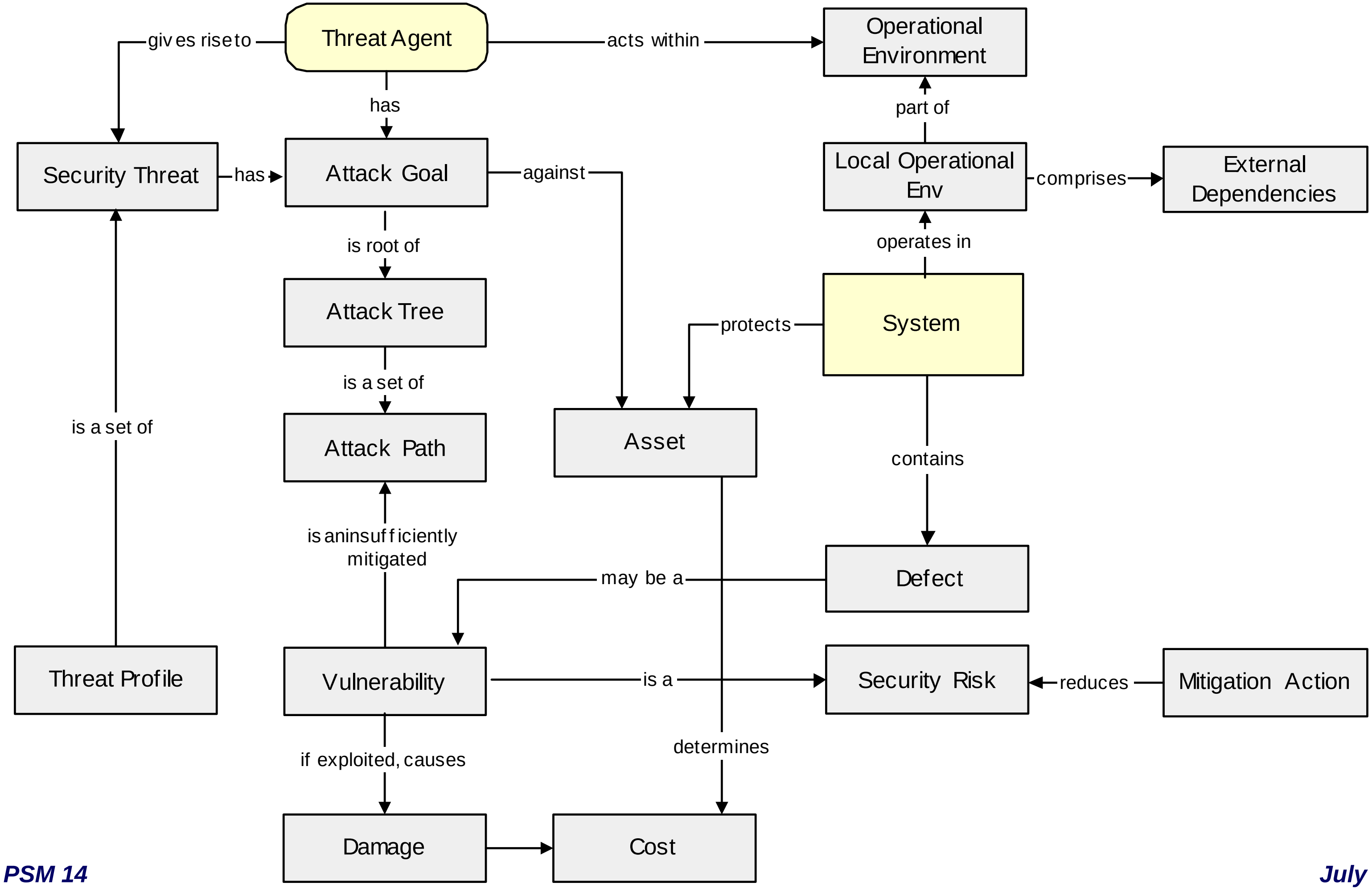
and

Level 3 Attack Goal: part 1

Level 3 Attack Goal: part 2

Swiderski F., Snyder W., Threat Modeling, Microsoft Press, Redmond, Washington, 2004

Practical Software and Systems Measurement



gives rise to

Threat Agent

acts within

Operational Environment

has

part of

Security Threat

has

Attack Goal

against

Local Operational Env

comprises

External Dependencies

is root of

operates in

Attack Tree

protects

System

is a set of

is a set of

Attack Path

Asset

contains

is an insufficiently mitigated

may be a

Defect

Threat Profile

Vulnerability

is a

Security Risk

reduces

Mitigation Action

if exploited, causes

determines

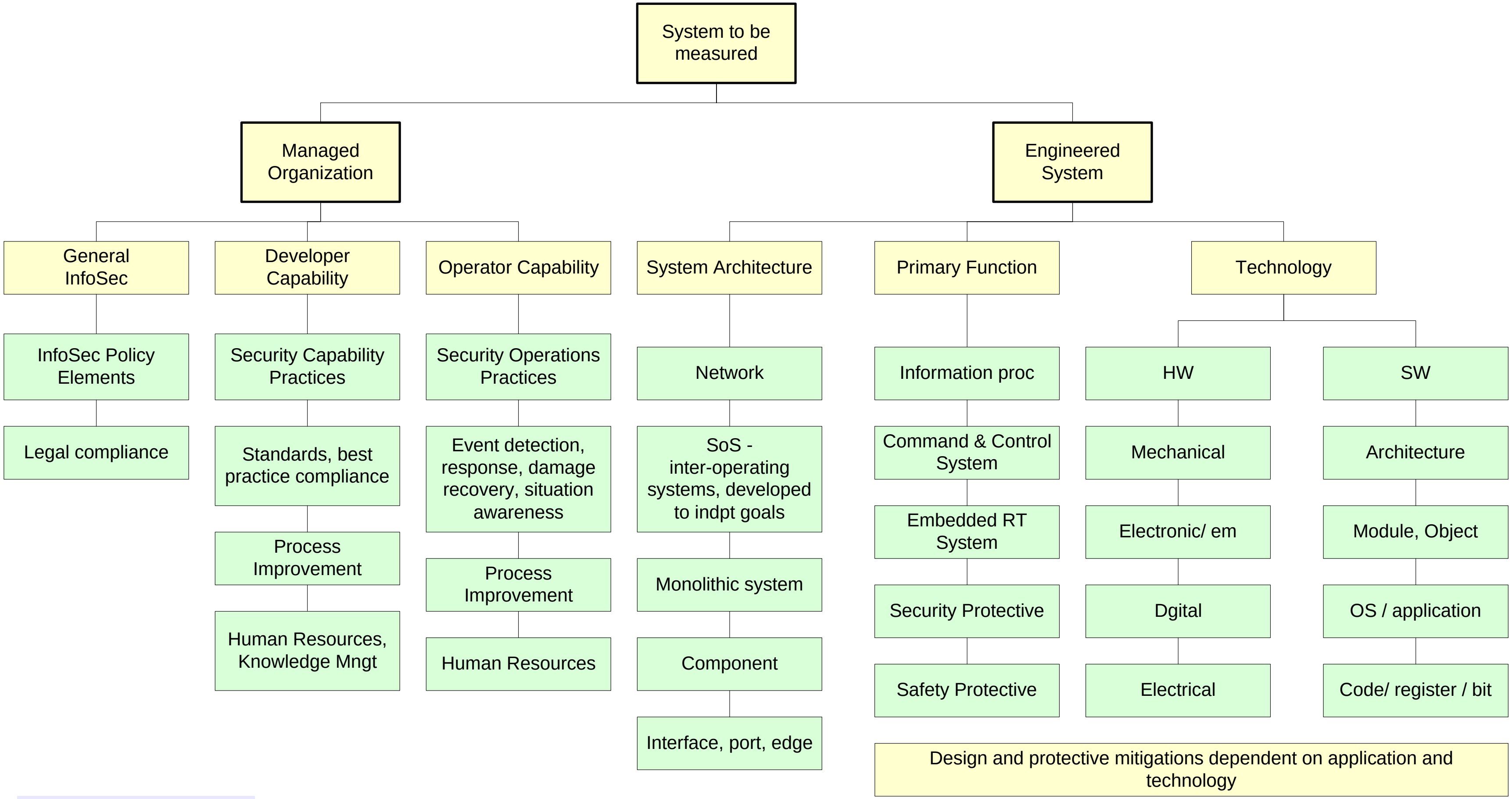
Damage

Cost

Security Concepts

- *Security: degree of protection from attack - a property of a system in relation to a threat*
- *System, assets, threats*
- *Attack Tree*
- *Defects and vulnerabilities*
- *Environment, local environment*

Practical Software and Systems Measurement

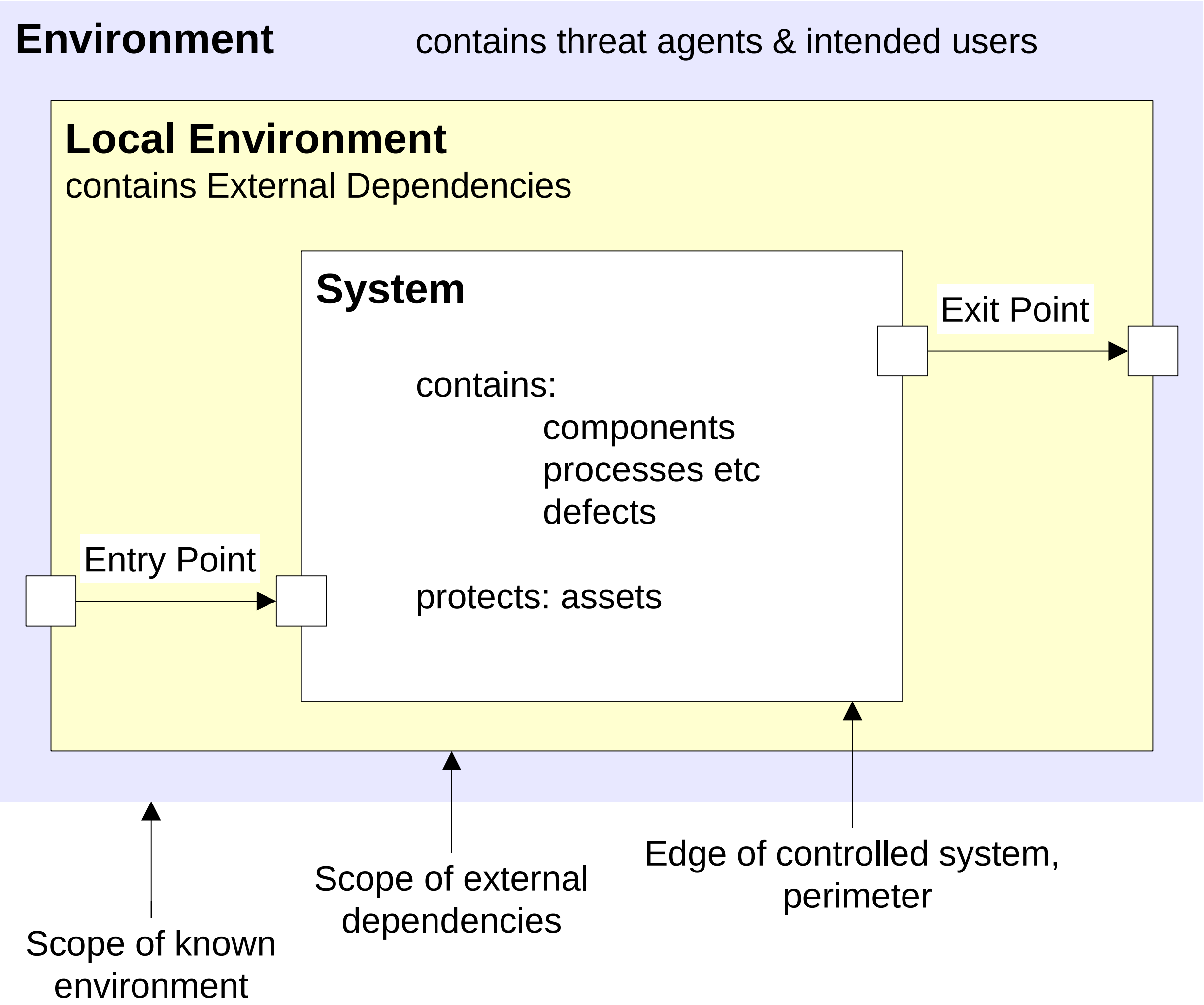


- System to be measured
  - Managed Organization
    - General InfoSec
      - InfoSec Policy Elements
      - Legal compliance
    - Developer Capability
      - Security Capability Practices
      - Standards, best practice compliance
      - Process Improvement
      - Human Resources, Knowledge Mngt
    - Operator Capability
      - Security Operations Practices
      - Event detection, response, damage recovery, situation awareness
      - Process Improvement
      - Human Resources
  - Engineered System
    - System Architecture
      - Network
      - SoS - inter-operating systems, developed to indpt goals
      - Monolithic system
      - Component
      - Interface, port, edge
    - Primary Function
      - Information proc
      - Command & Control System
      - Embedded RT System
      - Security Protective
      - Safety Protective
    - Technology
      - HW
        - Mechanical
        - Electronic/ em
        - Dgital
        - Electrical
      - SW
        - Architecture
        - Module, Object
        - OS / application
        - Code/ register / bit

Design and protective mitigations dependent on application and technology

TYPICAL RISKS	Information loss, Corruption etc	Lack of due diligence, Ineffective processes, Inefficiencies	Vulnerabilities introduced into products at requirements stage, all levels, technologies	Vulnerabilities introduced into products at design stage	Vulnerabilities introduced into products at implementation stage
TYPICAL MITIGATIONS	Mngt actions, IT architecture, 'COTS' integration & config	Continuous Process impvt, Human resource devlpt, Knowledge mngt	Threat Modeling	Vulnerabilities 'designed out' Protective components Detection & Response	Testing Analysis Assurance

Systems Approach to Security



Environment contains threat agents & intended users

Local Environment
contains External Dependencies

System

contains:
- components
- processes etc
- defects

protects: assets

Entry Point

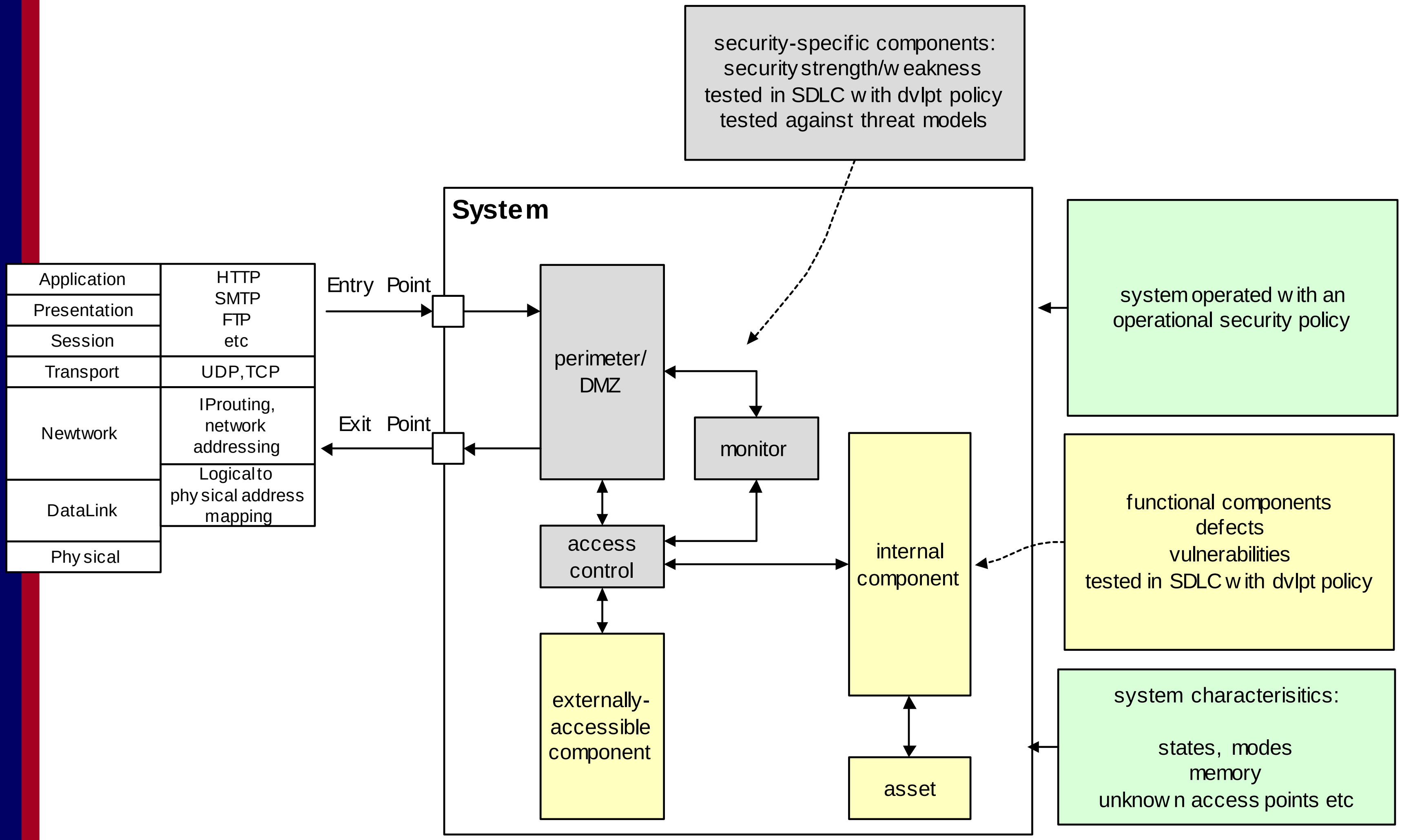
Exit Point

Scope of known environment

Scope of external dependencies

Edge of controlled system, perimeter

Practical Software and Systems Measurement



security-specific components:
security strength/weakness
tested in SDLC with dvlpt policy
tested against threat models

Application Presentation Session	HTTP SMTP FTP etc
Transport	UDP,TCP
Newtwork	IProuting, network addressing
DataLink	Logical to physical address mapping
Physical	

Entry Point

Exit Point

System

perimeter/ DMZ

monitor

access control

internal component

externally-accessible component

asset

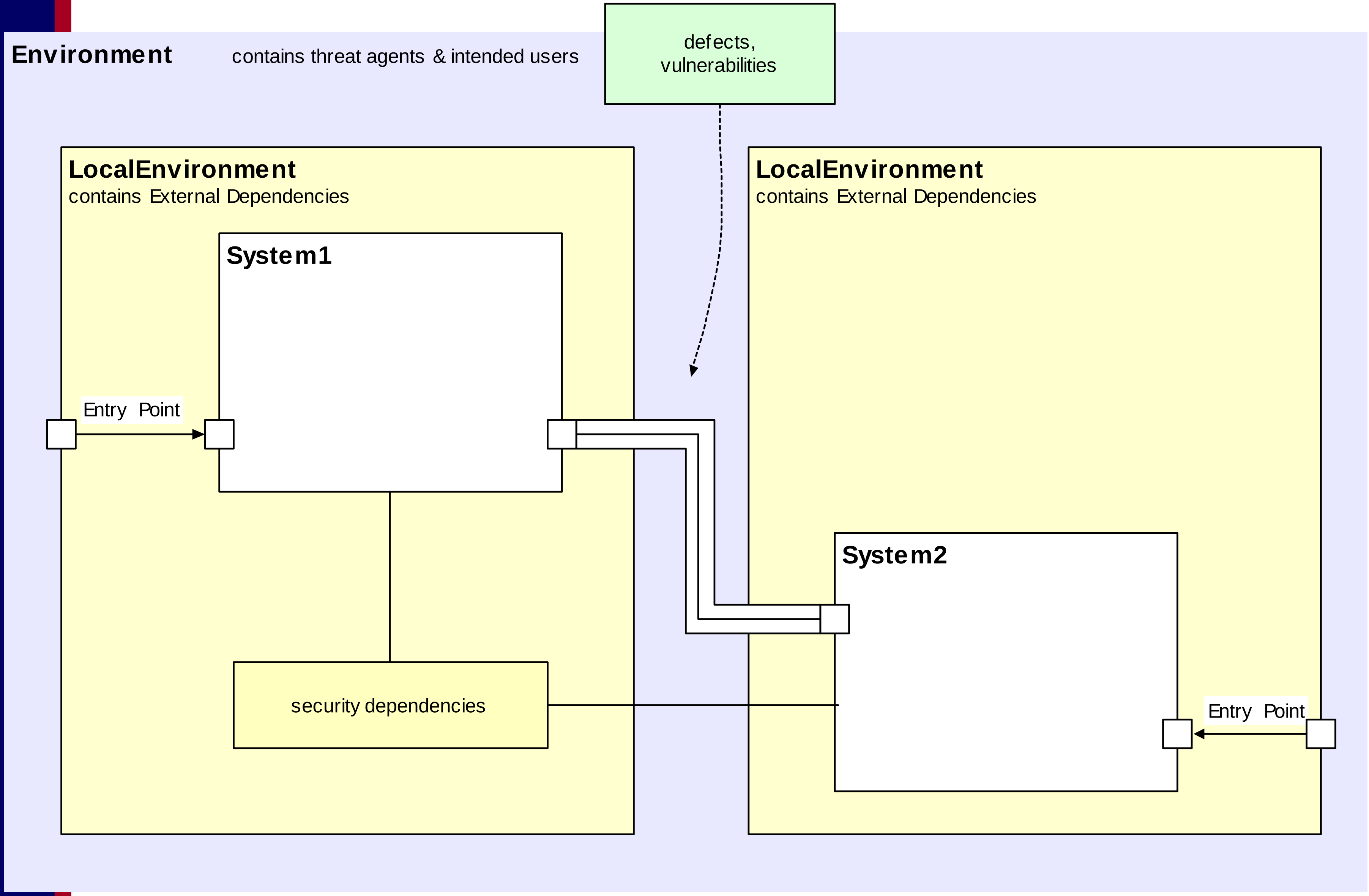
system operated with an operational security policy

functional components
defects
vulnerabilities
tested in SDLC with dvlpt policy

system characterisitics:

states, modes
memory
unknown access points etc

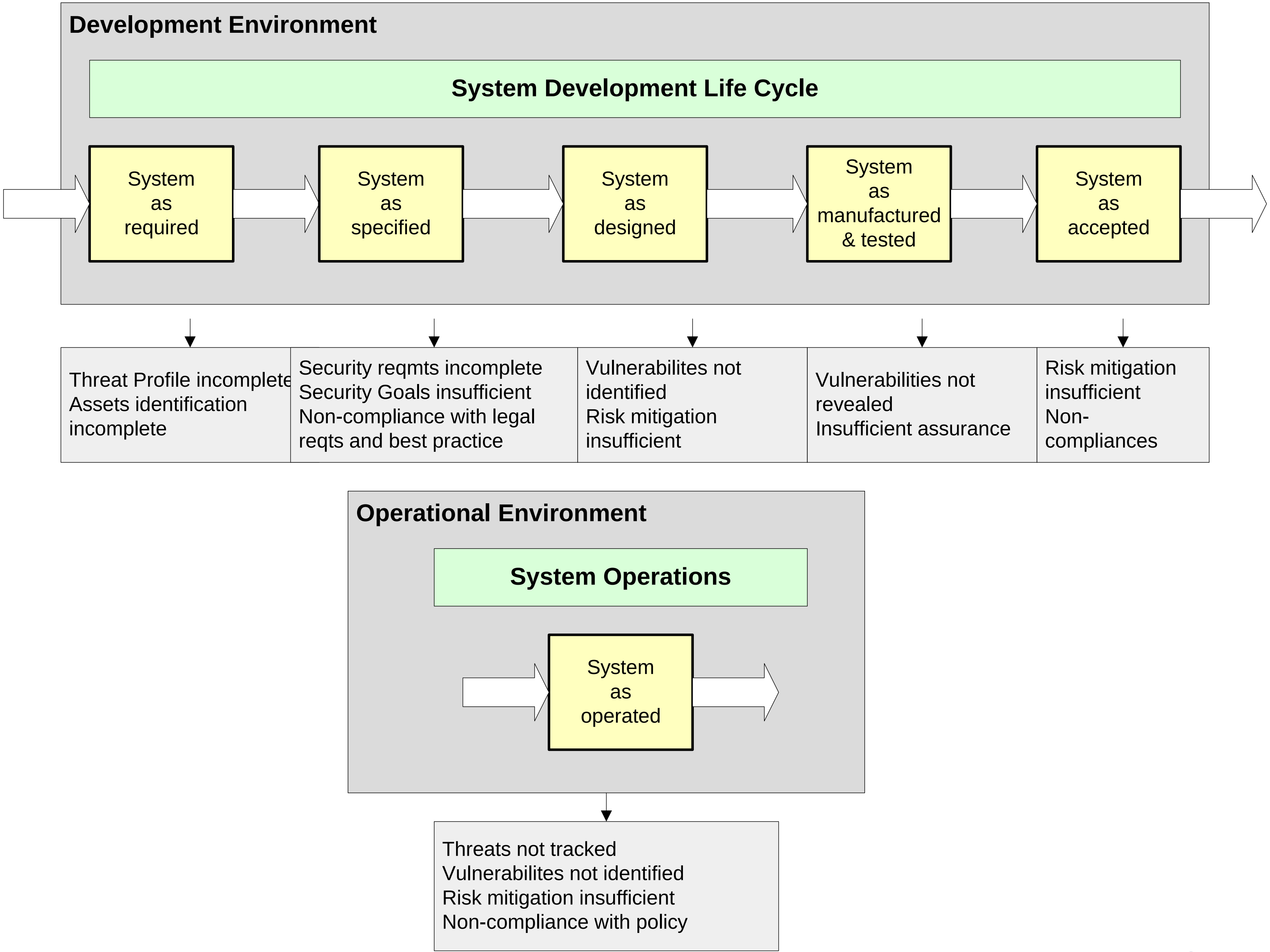
Practical Software and Systems Measurement



Security Concepts

- ***System***
- ***Boundary, perimeter***
- ***Ports, entry, exit points***
- ***Sub-components, processes***
- ***Developed: designed, manufactured***
- ***Operated: mission, purpose***
- ***Defects: in design, implementation, operation***

Practical Software and Systems Measurement



Development Environment

System Development Life Cycle

System as required

System as specified

System as designed

System as manufactured & tested

System as accepted

Threat Profile incomplete
Assets identification incomplete

Security reqmts incomplete
Security Goals insufficient
Non-compliance with legal reqts and best practice

Vulnerabilites not identified
Risk mitigation insufficient

Vulnerabilities not revealed
Insufficient assurance

Risk mitigation insufficient
Non-compliances

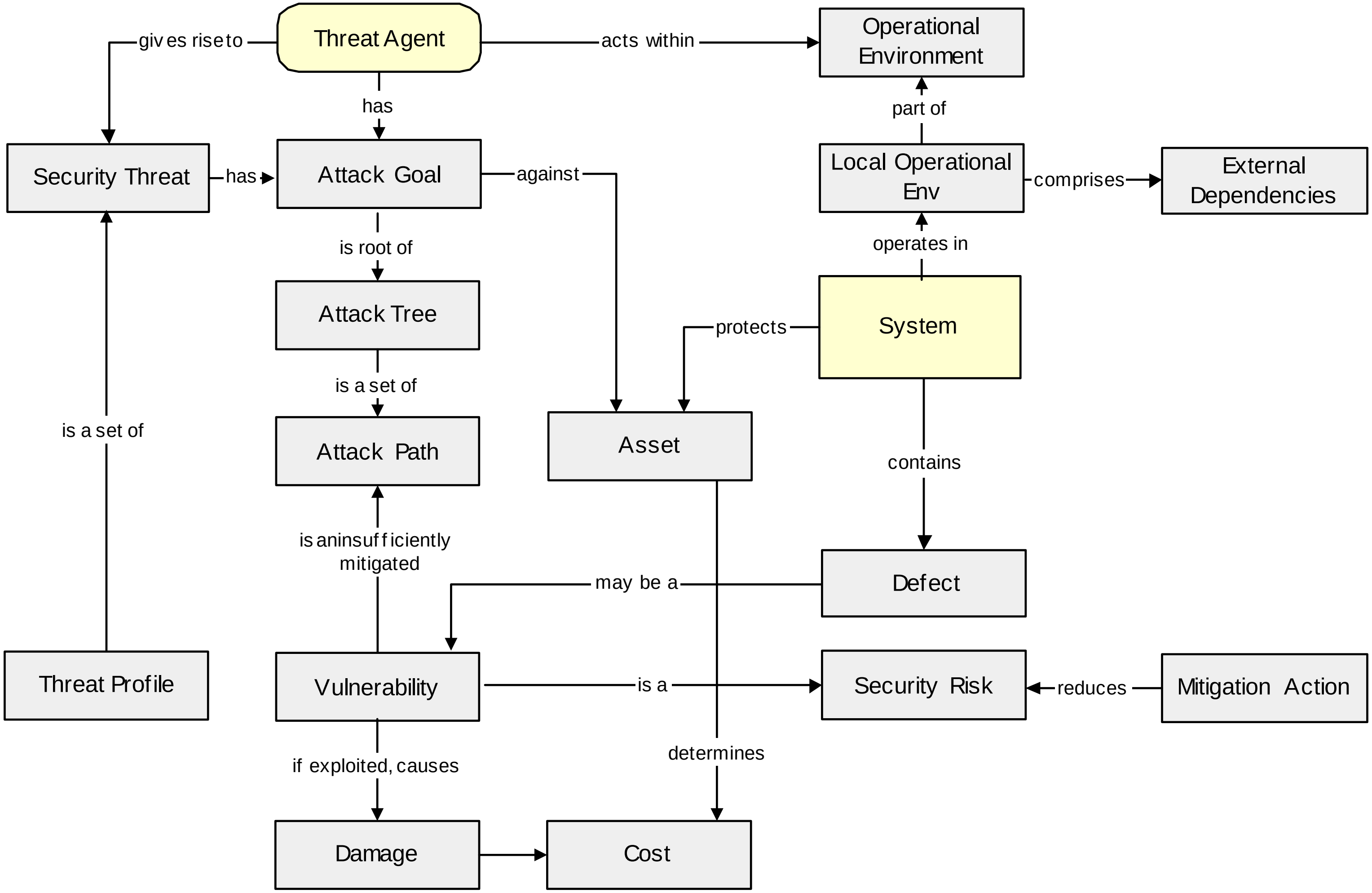
Operational Environment

System Operations

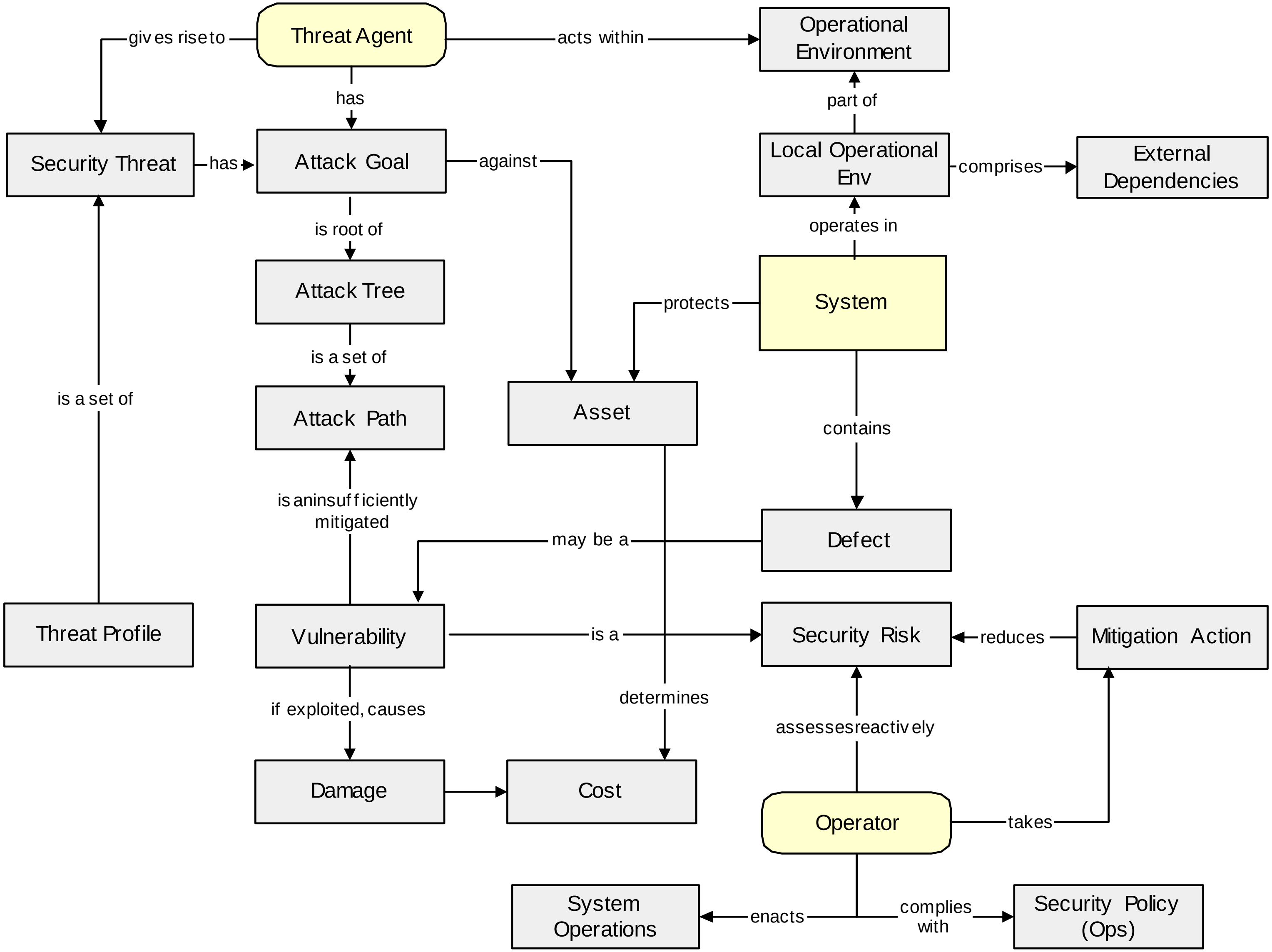
System as operated

Threats not tracked
Vulnerabilites not identified
Risk mitigation insufficient
Non-compliance with policy

Practical Software and Systems Measurement



Practical Software and Systems Measurement



Threat Agent

gives rise to

acts within

Operational Environment

has

part of

Security Threat

has

Attack Goal

against

Local Operational Env

comprises

External Dependencies

is root of

operates in

Attack Tree

protects

System

is a set of

is a set of

Attack Path

Asset

contains

is an insufficiently mitigated

may be a

Defect

Threat Profile

Vulnerability

is a

Security Risk

reduces

Mitigation Action

if exploited, causes

determines

assesses reactively

Damage

Cost

Operator

takes

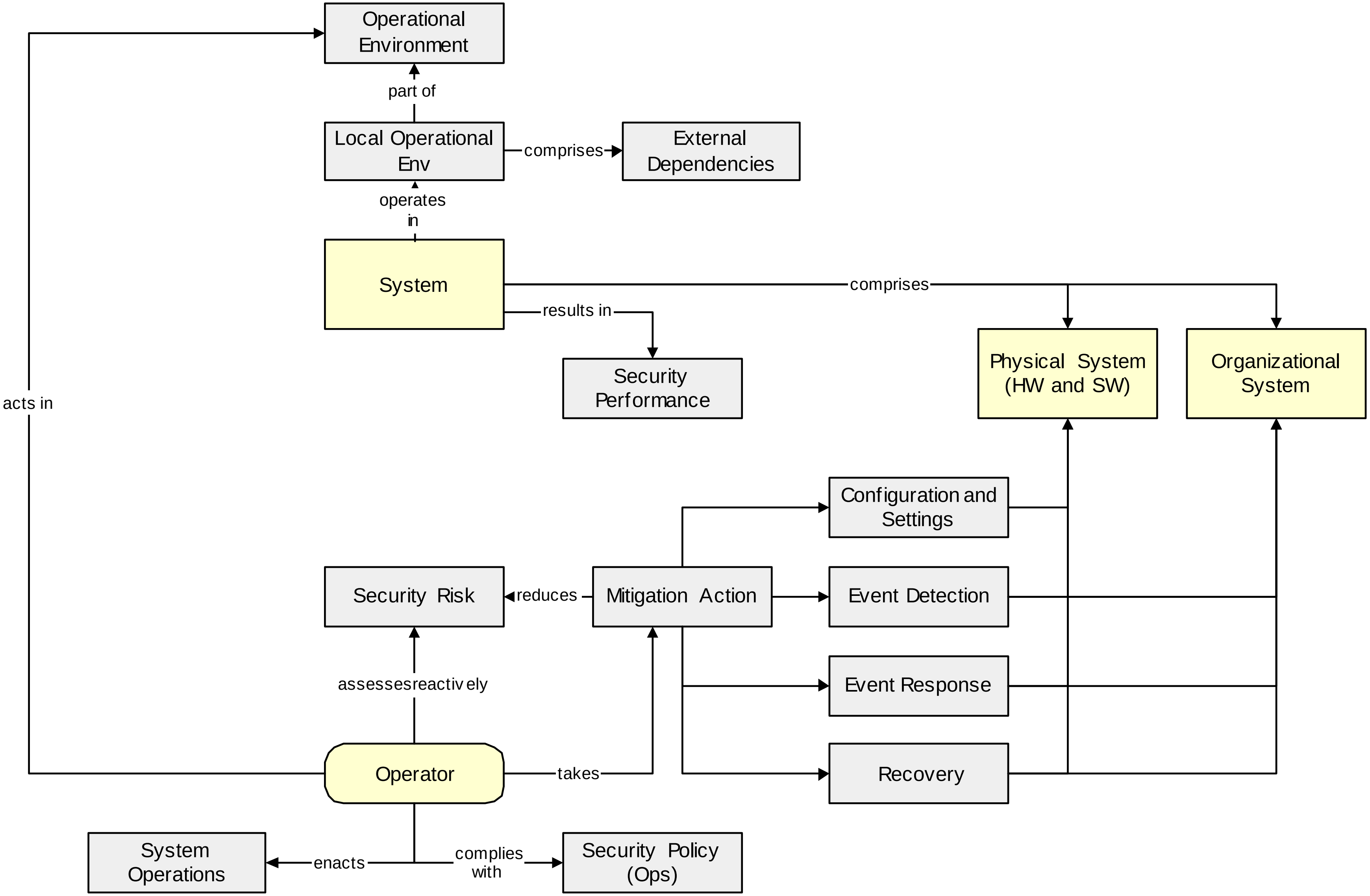
System Operations

enacts

complies with

Security Policy (Ops)

Practical Software and Systems Measurement



Operational Environment

part of

Local Operational Env

comprises

External Dependencies

operates in

System

comprises

results in

Security Performance

Physical System (HW and SW)

Organizational System

acts in

Configuration and Settings

Security Risk

reduces

Mitigation Action

Event Detection

assessesreactiv ely

Event Response

Operator

takes

Recovery

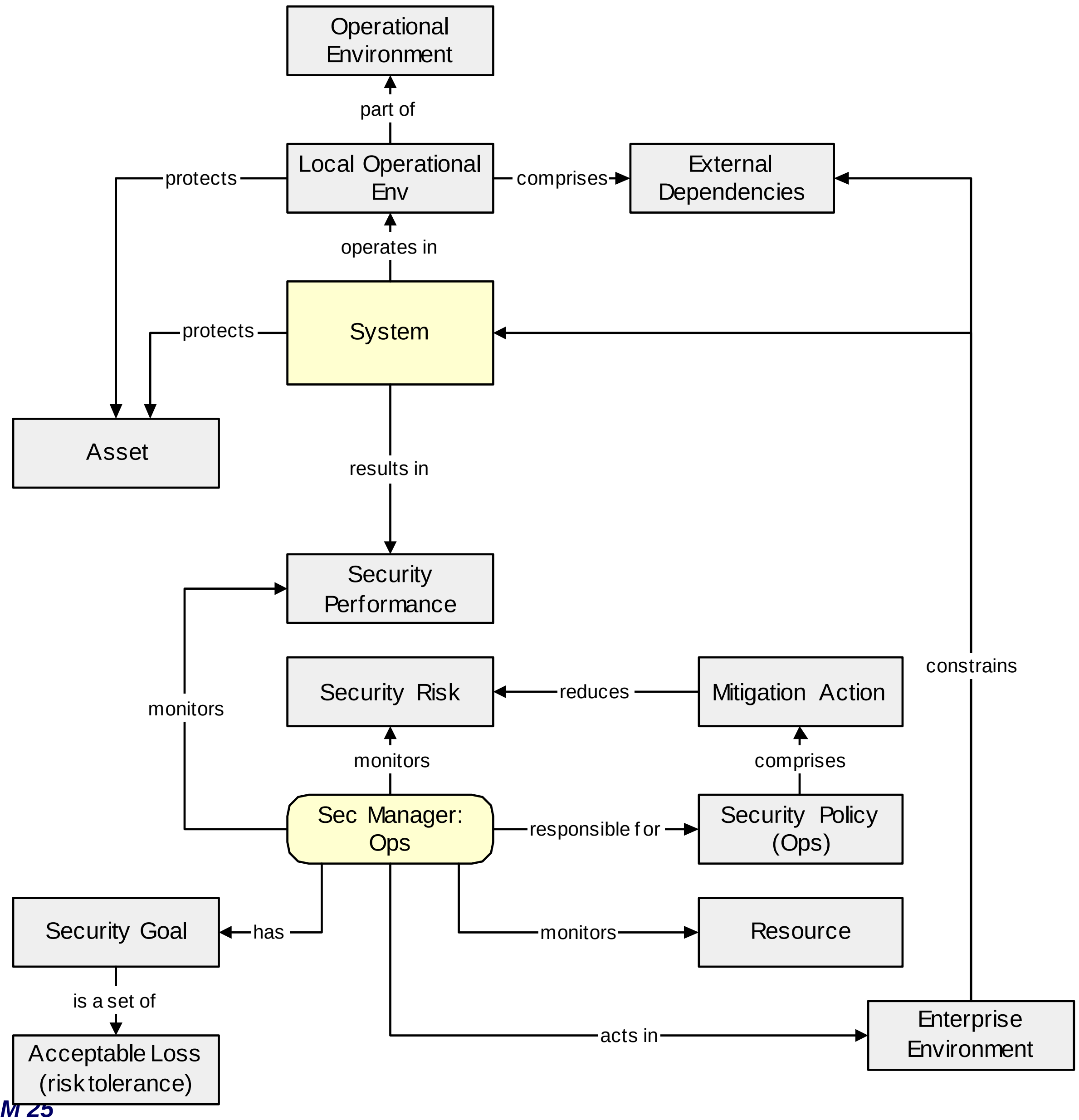
System Operations

enacts

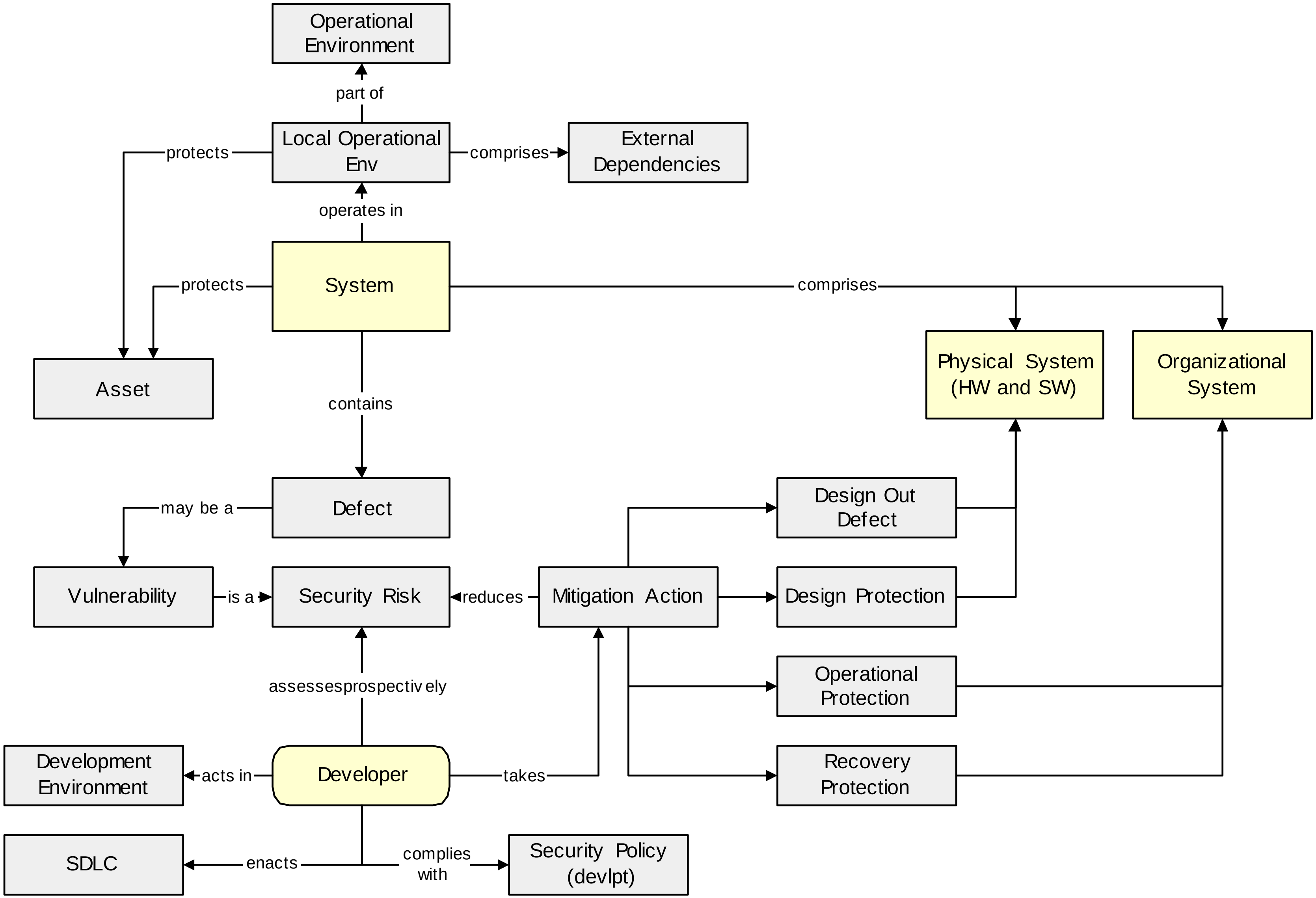
complies with

Security Policy (Ops)

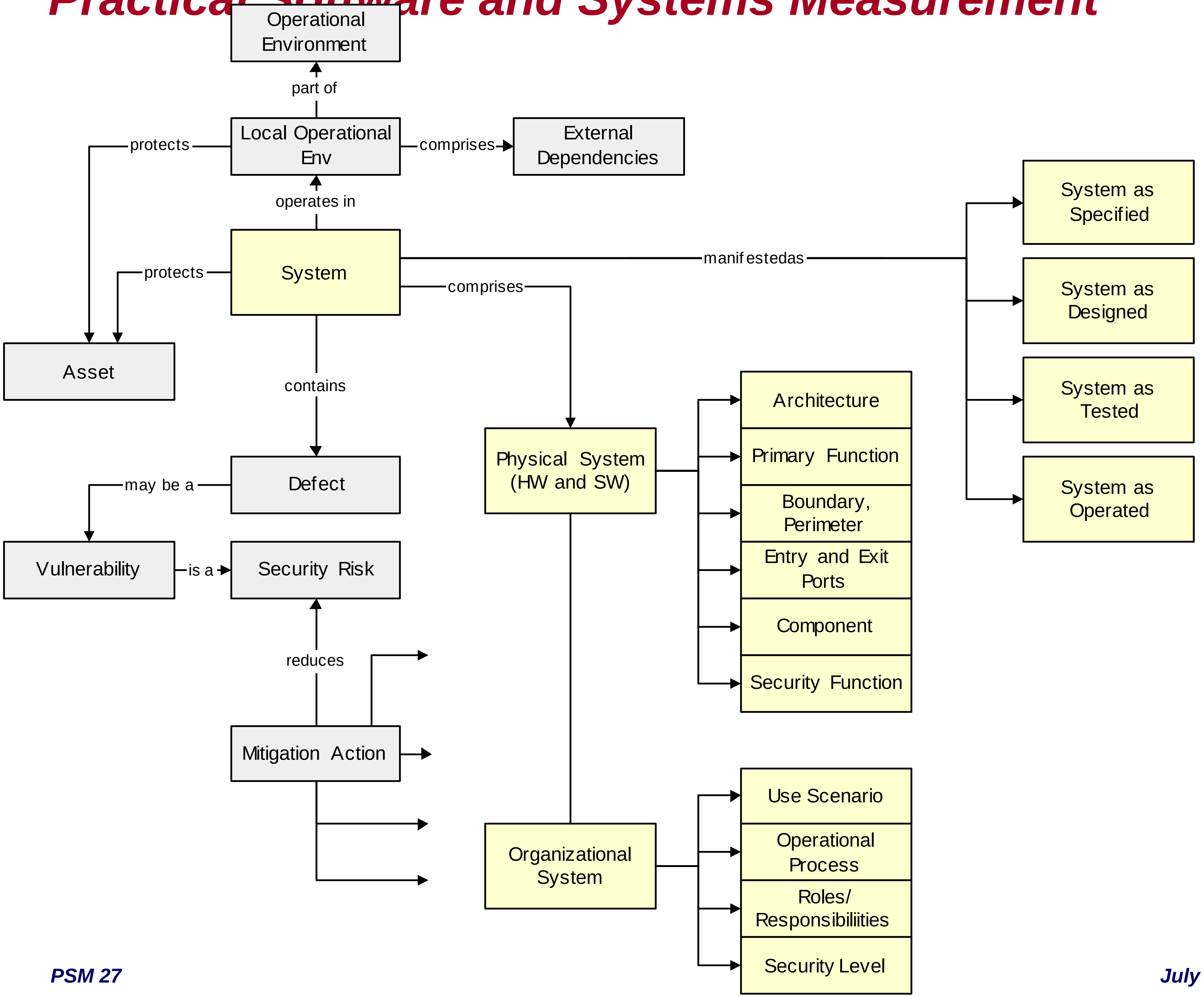
Practical Software and Systems Measurement



Practical Software and Systems Measurement



Practical Software and Systems Measurement



Operational Environment

part of

Local Operational Env

comprises

External Dependencies

protects

operates in

System

protects

Asset

manifested as

System as Specified

System as Designed

System as Tested

System as Operated

comprises

contains

Physical System (HW and SW)

Architecture

Primary Function

Boundary, Perimeter

Entry and Exit Ports

Component

Security Function

Defect

may be a

Vulnerability

is a

Security Risk

reduces

Mitigation Action

Organizational System

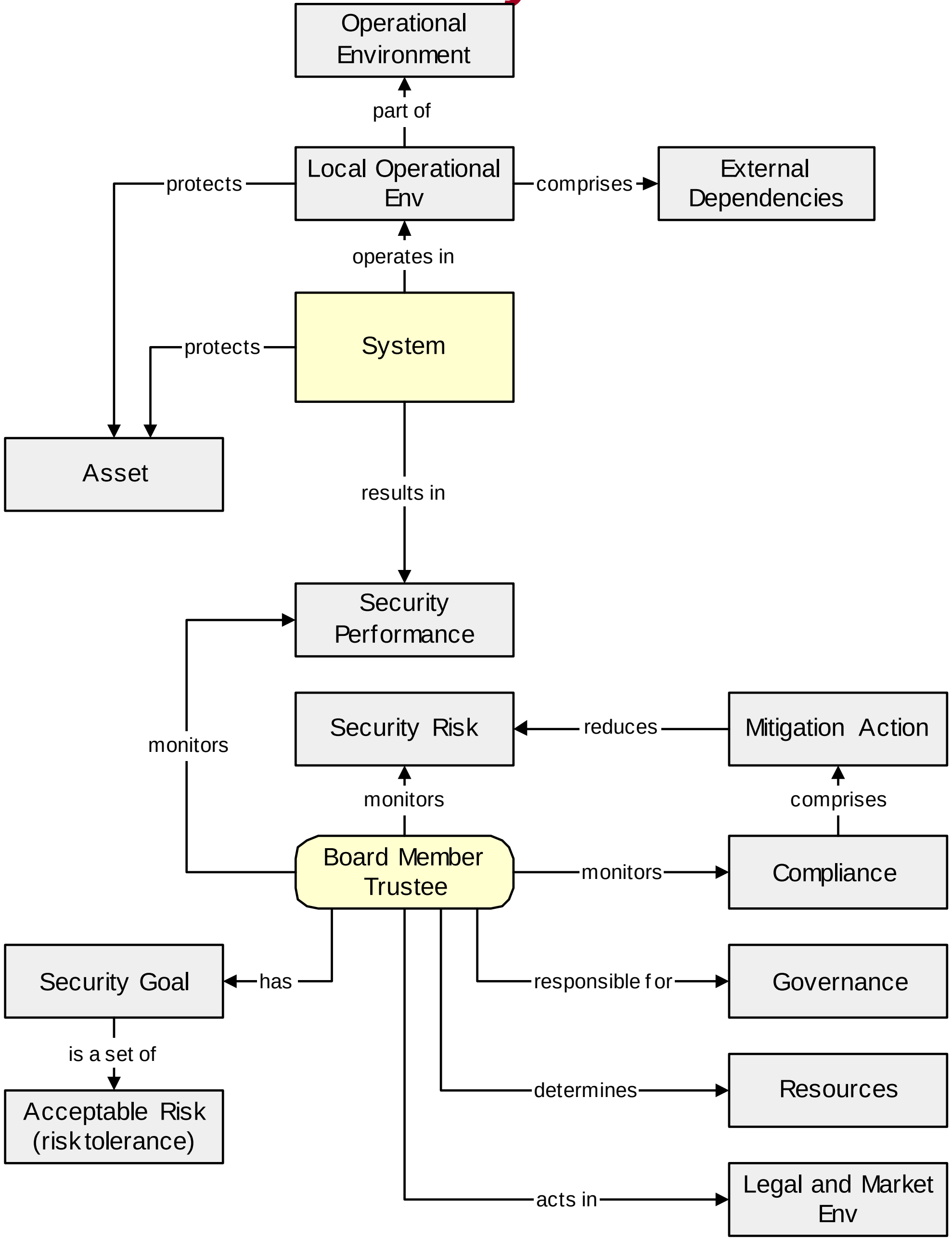
Use Scenario

Operational Process

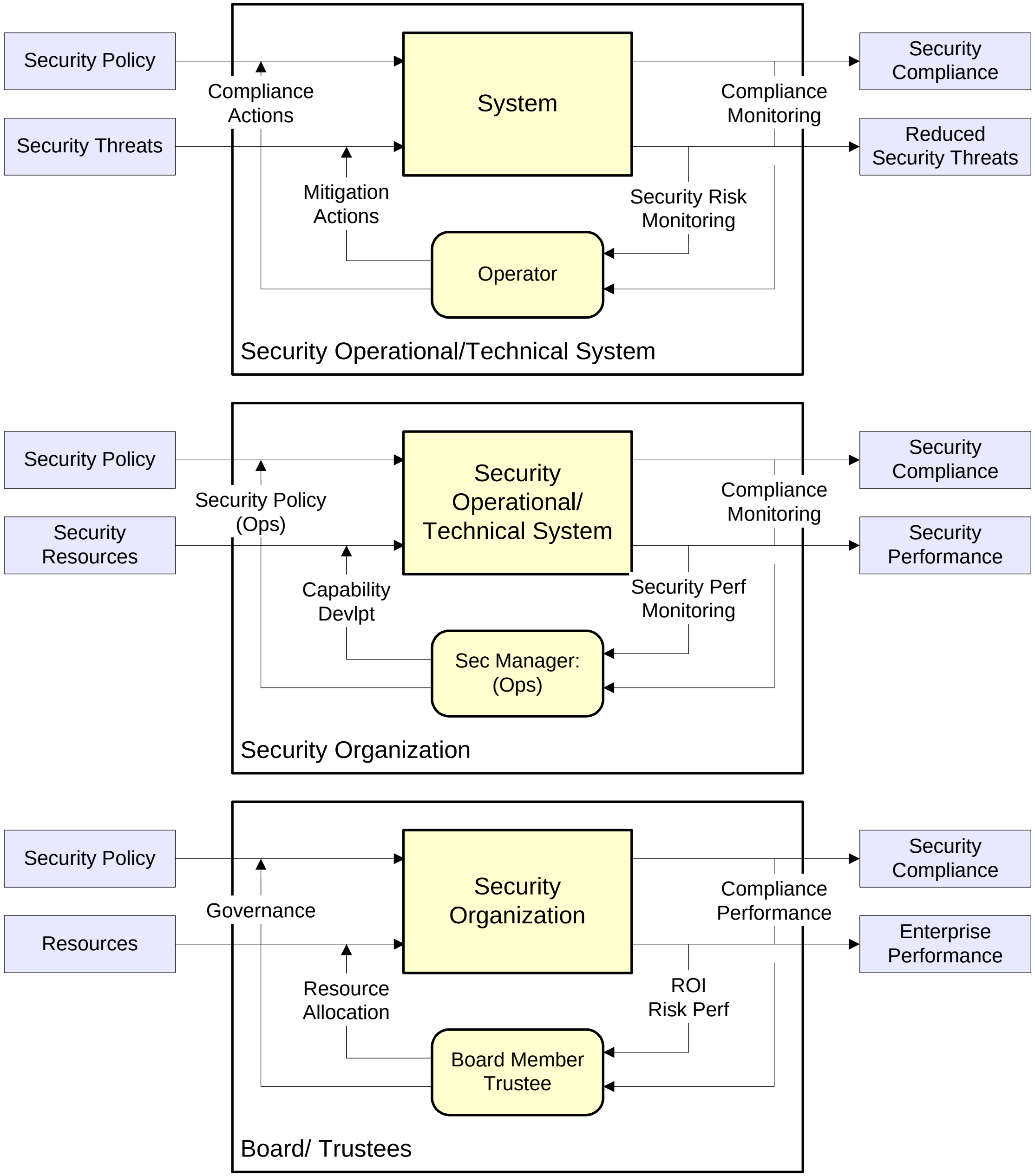
Roles/ Responsibilities

Security Level

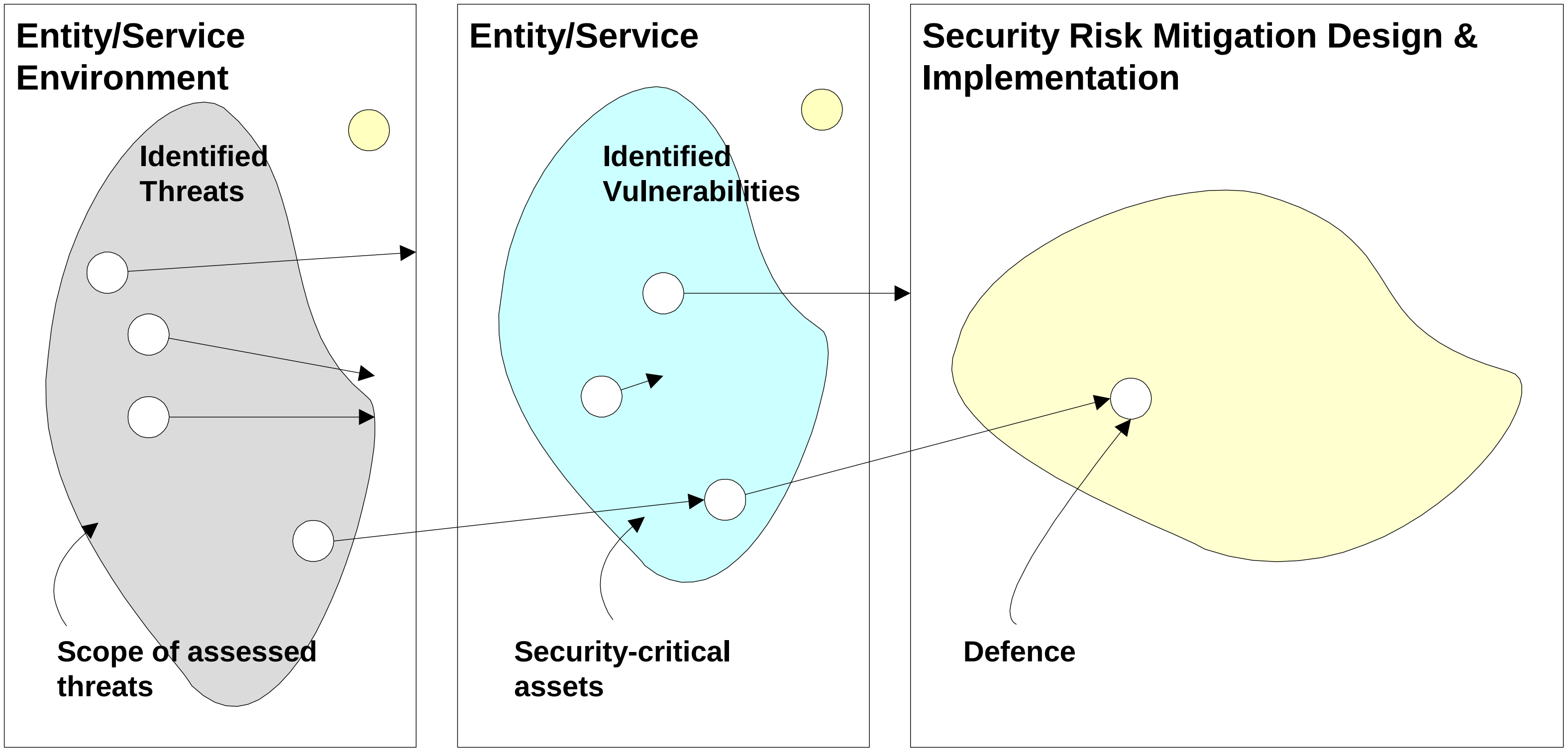
Practical Software and Systems Measurement



Practical Software and Systems Measurement



Practical Software and Systems Measurement



Entity/Service Environment

Identified Threats

Scope of assessed threats

Entity/Service

Identified Vulnerabilities

Security-critical assets

Security Risk Mitigation Design & Implementation

Defence

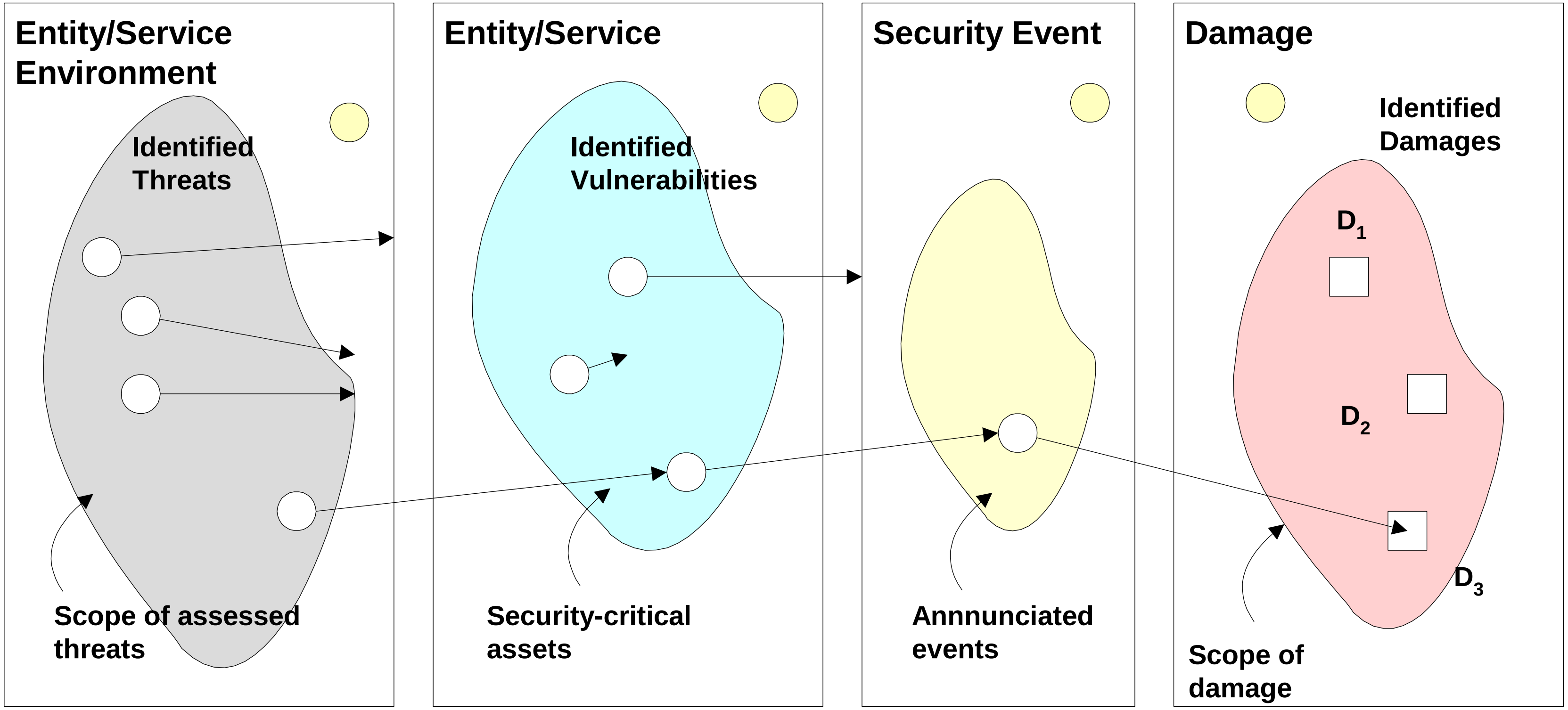
Threat: capability, intent
Threat type

Vulnerability
Vulnerability type
Vulnerability attack likelihood and severity

Risk Mitigation

🟡 - unidentified threat, vulnerability etc

Practical Software and Systems Measurement



Entity/Service Environment

Identified Threats

Scope of assessed threats

Entity/Service

Identified Vulnerabilities

Security-critical assets

Security Event

Annnunciated events

Damage

Identified Damages

D_1

D_2

D_3

Scope of damage

Threat: capability, intent
Threat type

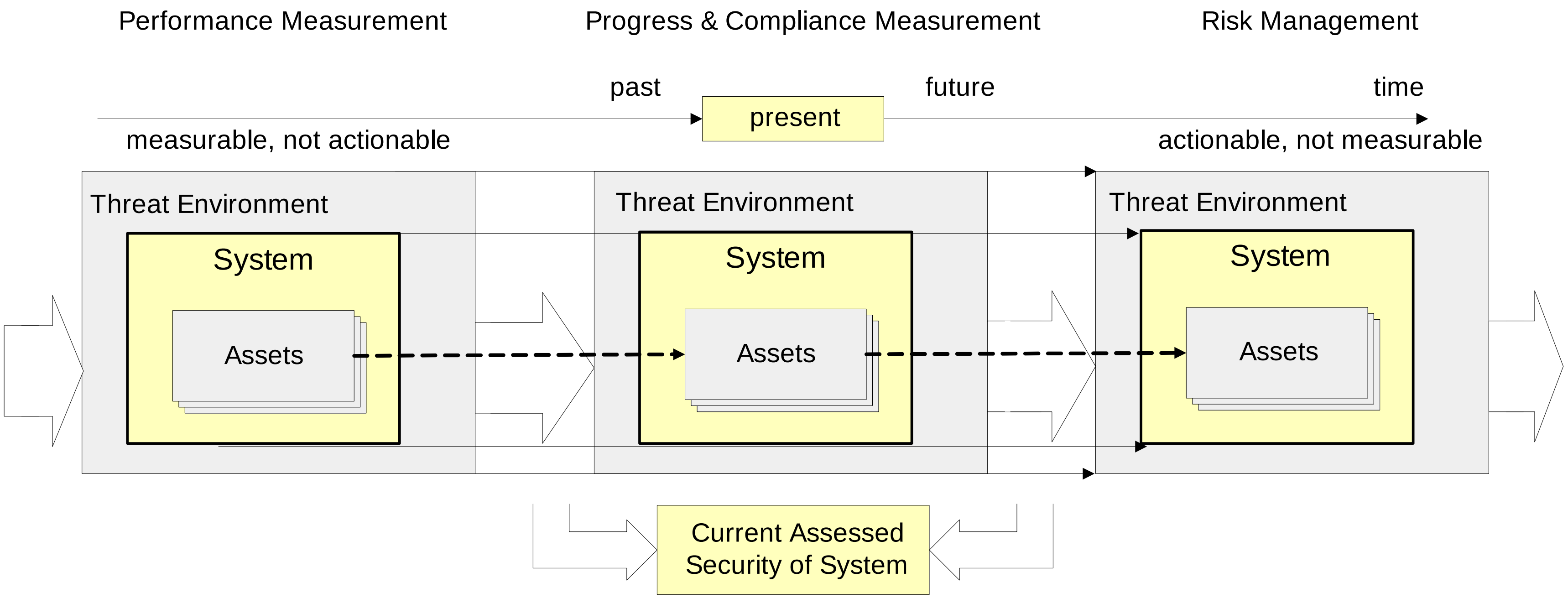
Vulnerability
Vulnerability type
Vulnerability attack likelihood and severity

Security incident
Incident type
Incident likelihood

Damage severity
Damage likelihood

○ **- unidentified threat, vulnerability etc**

Time-Based View of Measurement



Performance Measurement

Progress & Compliance Measurement

Risk Management

past

present

future

time

measurable, not actionable

actionable, not measurable

Threat Environment

System

Assets

Threat Environment

System

Assets

Threat Environment

System

Assets

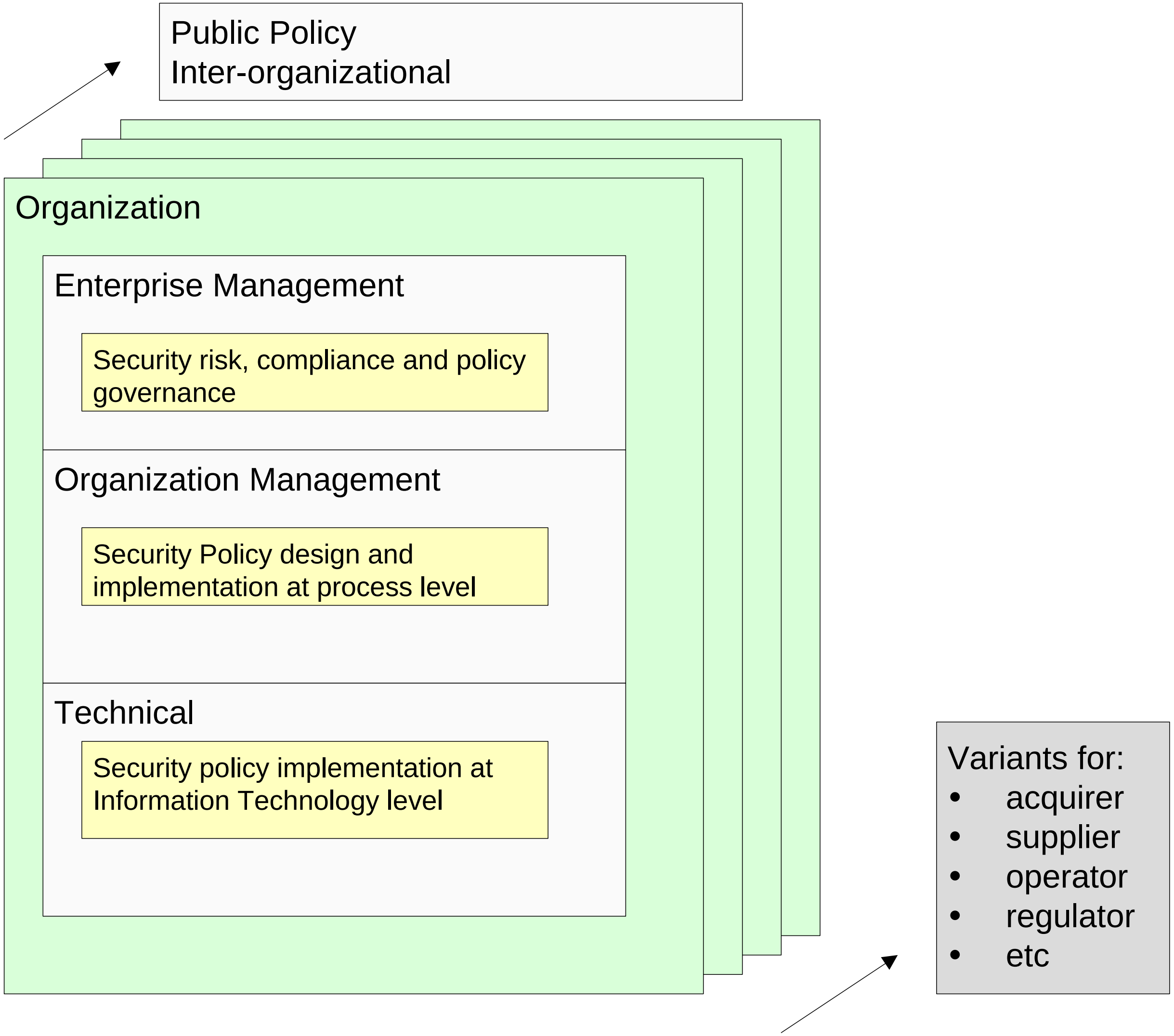
Current Assessed Security of System

Measures of achieved progress in security performance compared with goals

Measures of currrent activity and performance compared with plans

Predictors of security performance based on past & current performance & plans

Practical Software and Systems Measurement



Public Policy
Inter-organizational

Organization

Enterprise Management

Security risk, compliance and policy governance

Organization Management

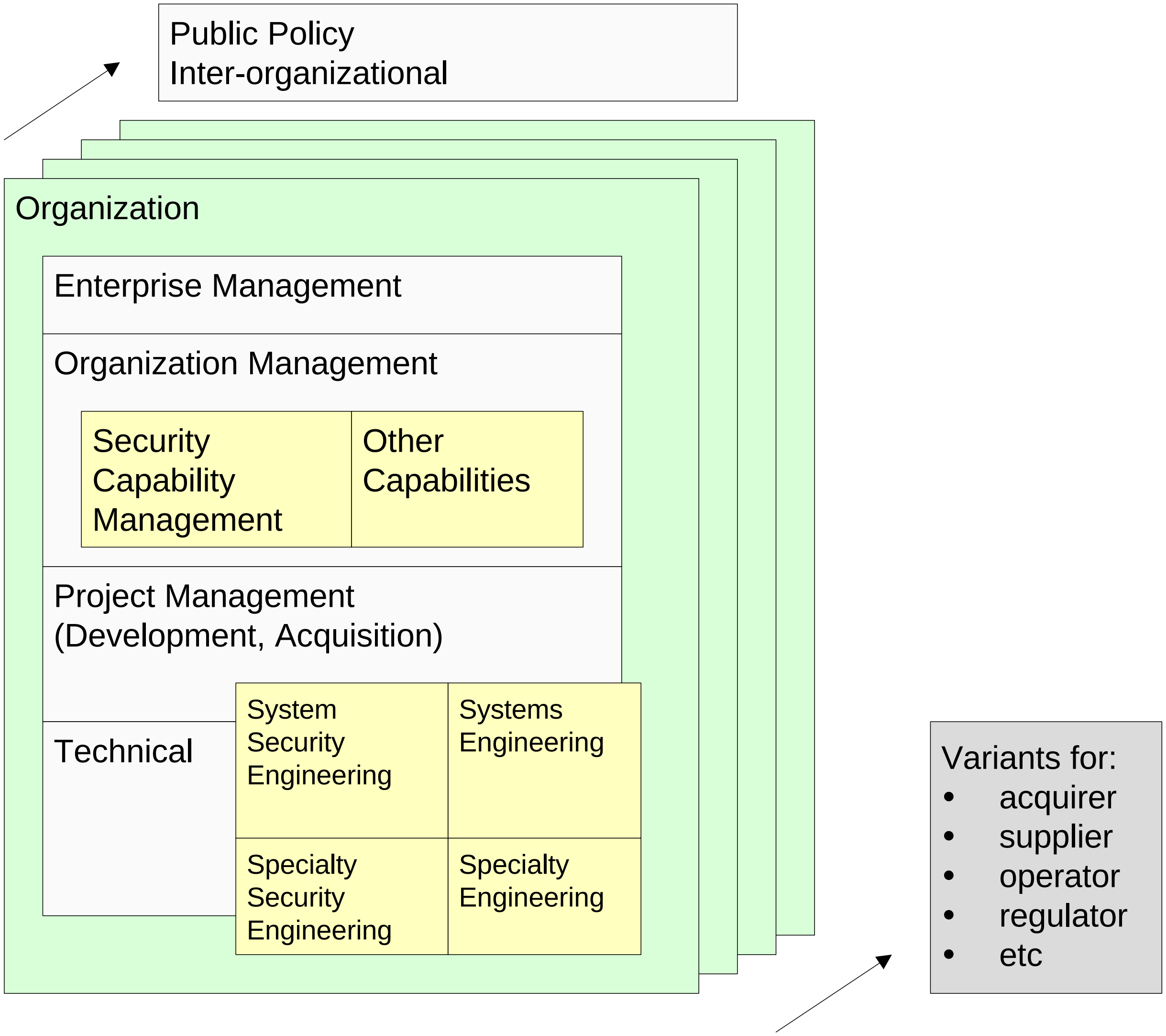
Security Policy design and implementation at process level

Technical

Security policy implementation at Information Technology level

Variants for:
- acquirer
- supplier
- operator
- regulator
- etc

Practical Software and Systems Measurement



Public Policy
Inter-organizational

Organization

Enterprise Management

Organization Management

Security Capability Management

Other Capabilities

Project Management
(Development, Acquisition)

Technical

System Security Engineering

Systems Engineering

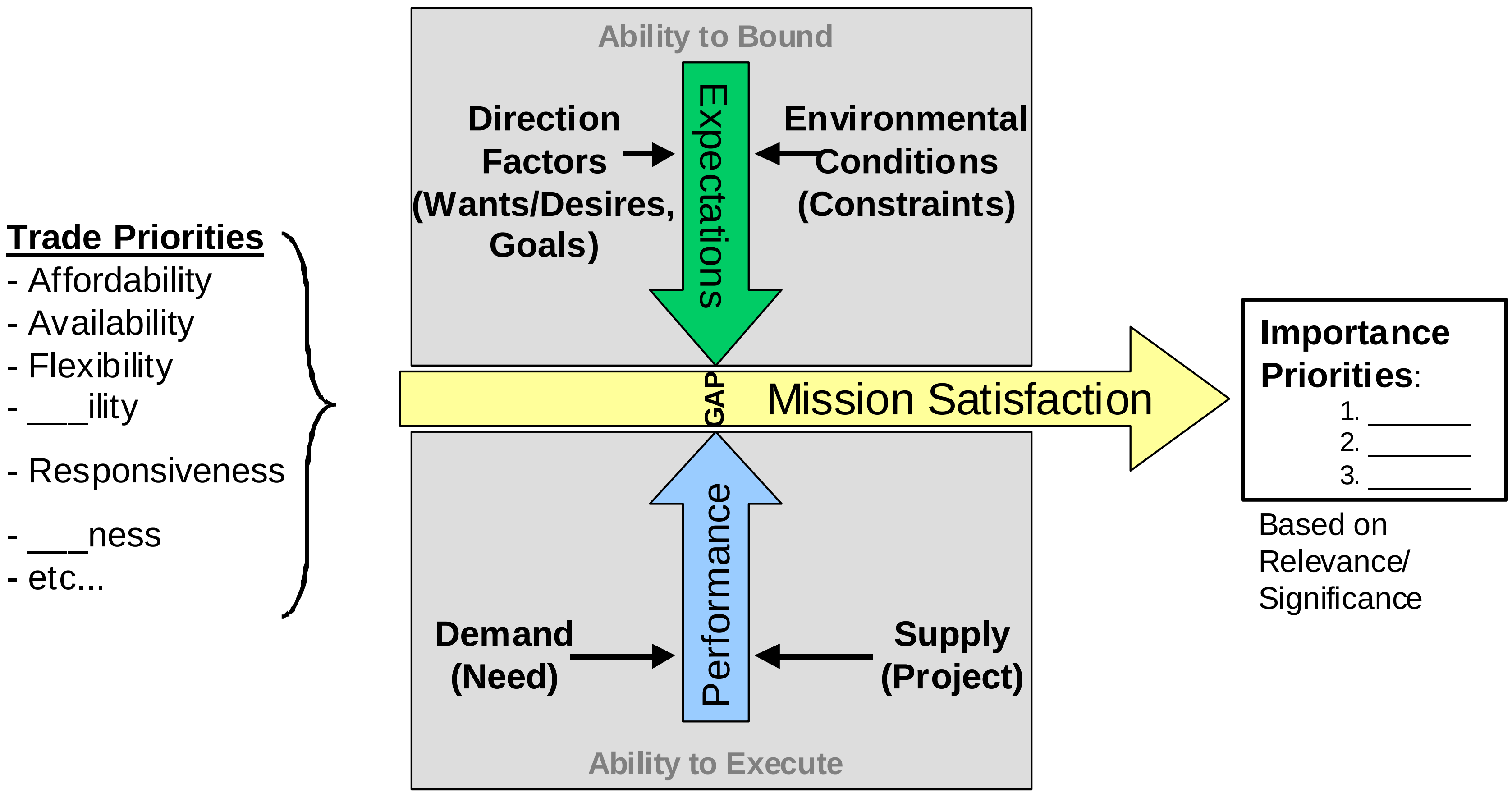
Specialty Security Engineering

Specialty Engineering

Variants for:

- acquirer
- supplier
- operator
- regulator
- etc

Practical Software and Systems Measurement



Trade Priorities

- Affordability
- Availability
- Flexibility
- ___ility
- Responsiveness
- ___ness
- etc...

Ability to Bound

Direction Factors (Wants/Desires, Goals)

Expectations

Environmental Conditions (Constraints)

GAP

Mission Satisfaction

Demand (Need)

Performance

Supply (Project)

Ability to Execute

Importance Priorities:

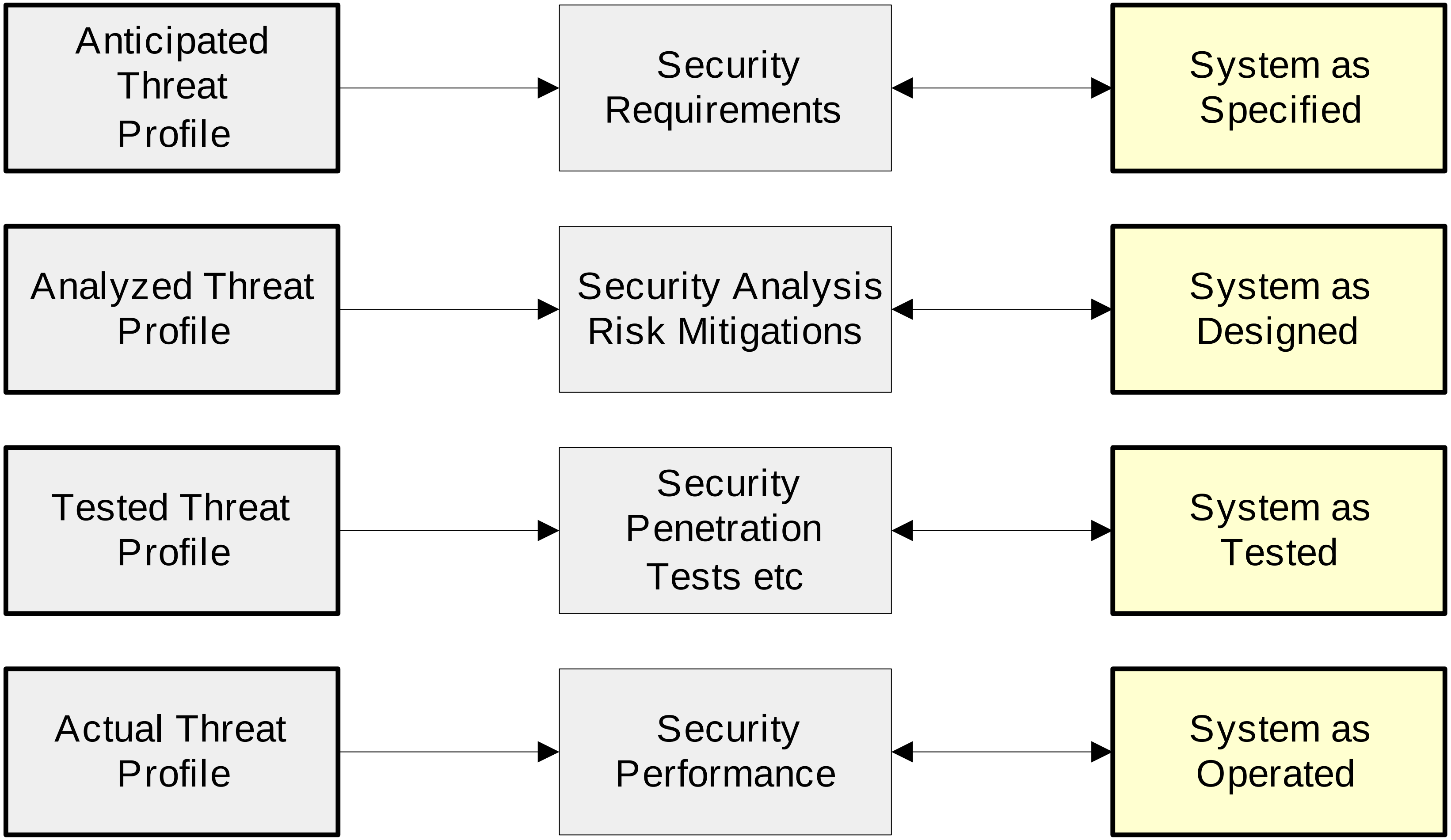
1. _______
2. _______
3. _______

Based on Relevance/ Significance

All four quadrants are expressed as situation, task, asset

Need:	**feasibly achievable expectation**
Project:	**executable work package to satisfy a need**

Assess security against what?



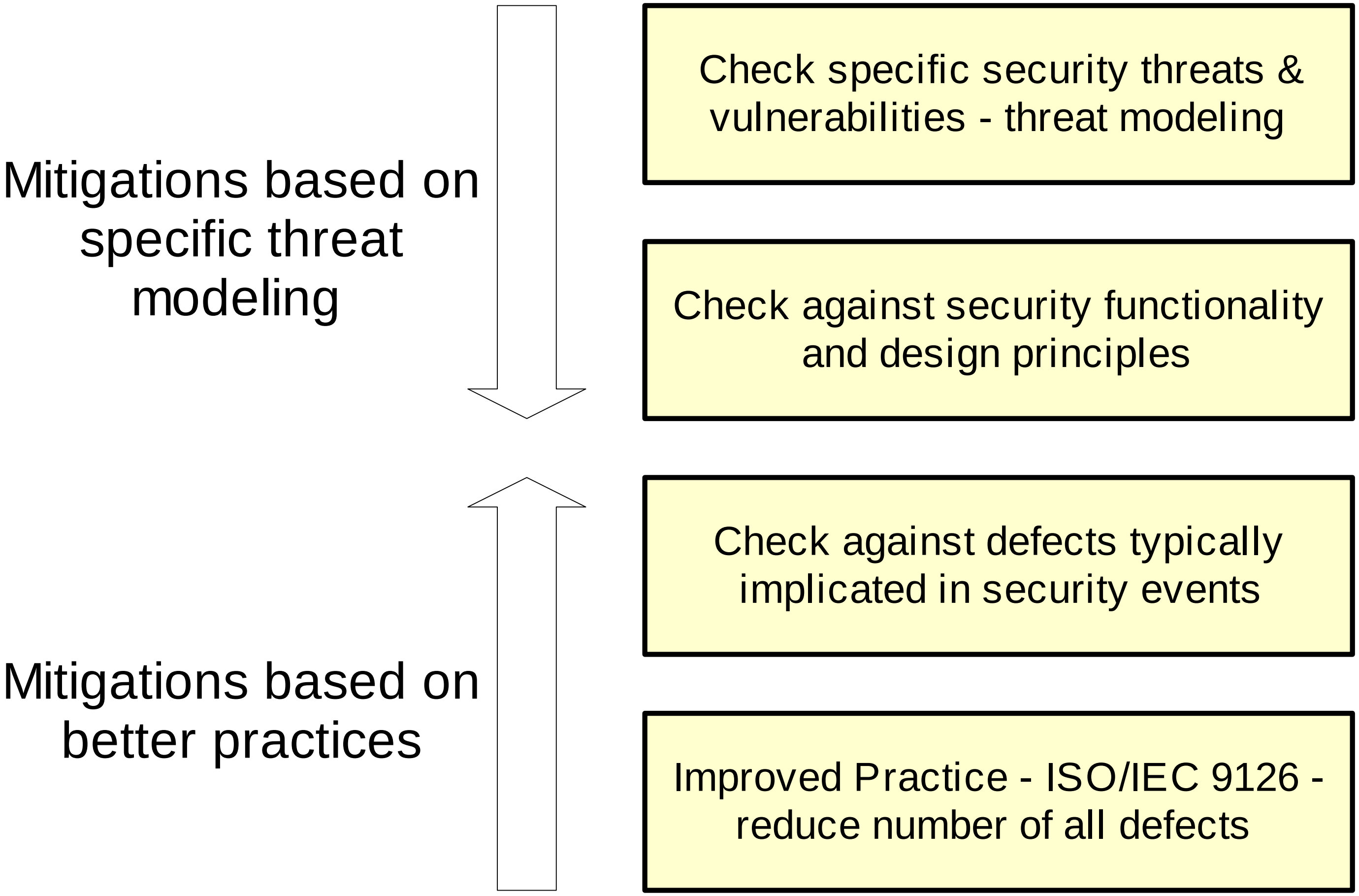
Anticipated Threat Profile → Security Requirements ↔ System as Specified

Analyzed Threat Profile → Security Analysis Risk Mitigations ↔ System as Designed

Tested Threat Profile → Security Penetration Tests etc ↔ System as Tested

Actual Threat Profile → Security Performance ↔ System as Operated

Assurance



Mitigations based on specific threat modeling

Mitigations based on better practices

Check specific security threats & vulnerabilities - threat modeling

Check against security functionality and design principles

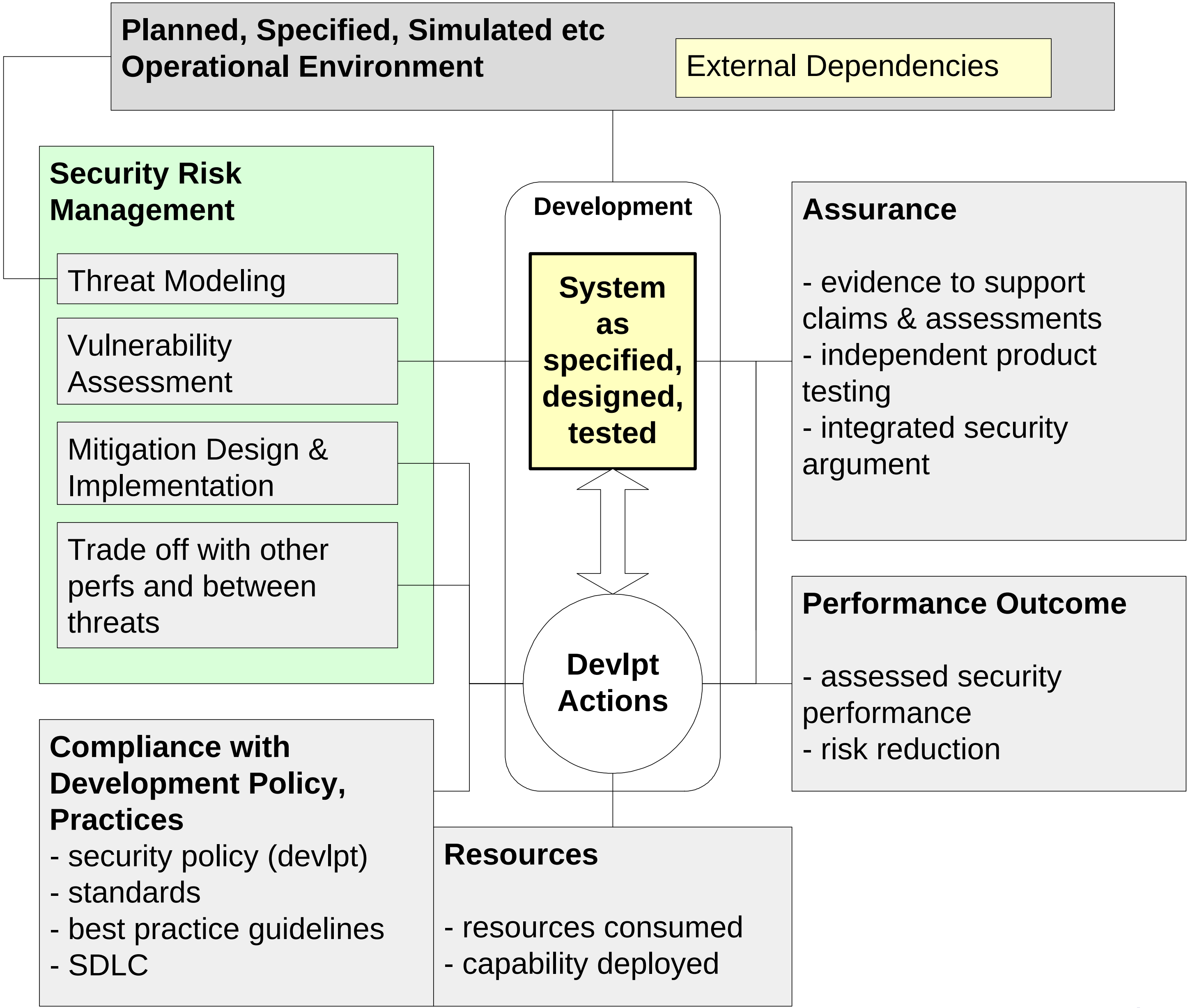
Check against defects typically implicated in security events

Improved Practice - ISO/IEC 9126 - reduce number of all defects

What Does it Mean to Measure Security?

1. Expression of desired security performance (threat definitions)
2. Assessment of achieved security performance (retrospective, events)
3. Assessment of risk of undesired security events (prospective)
4. Assessment of costs of risk reduction efforts retrospectively (cost accounting), prospectively (estimating)
5. Trade-offs of security improvement/risk acceptance with other performances
6. Security technology, engineering, operations capability: how good are we, or they?
7. Compliance: to what extent are we following best practice, the relevant standard, regulatory requirements
8. Assurance: how confident are we in the above?

Practical Software and Systems Measurement



Planned, Specified, Simulated etc Operational Environment

External Dependencies

Security Risk Management

Threat Modeling

Vulnerability Assessment

Mitigation Design & Implementation

Trade off with other perfs and between threats

Development

System as specified, designed, tested

Devlpt Actions

Assurance

- evidence to support claims & assessments
- independent product testing
- integrated security argument

Performance Outcome

- assessed security performance
- risk reduction

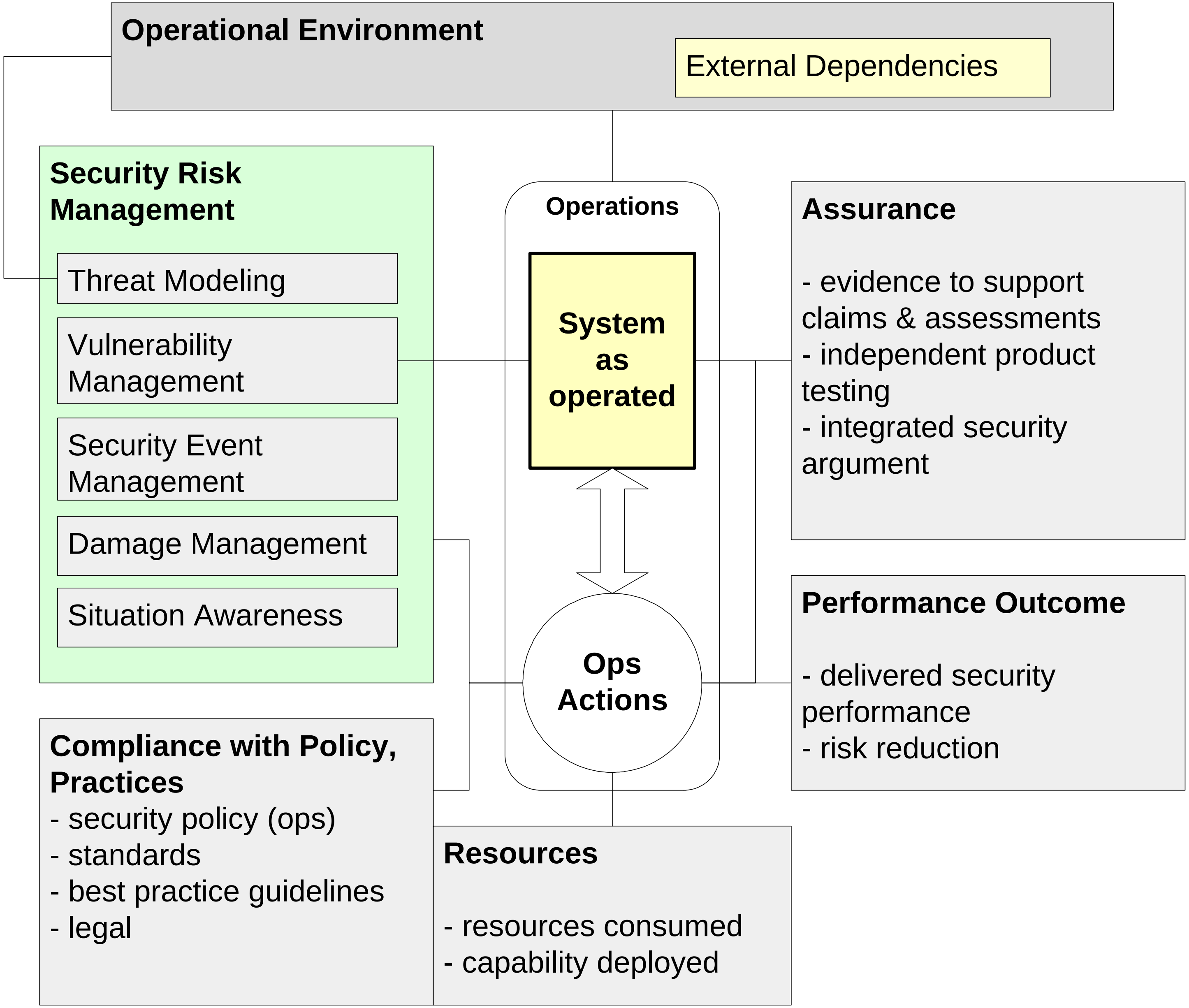
Compliance with Development Policy, Practices

- security policy (devlpt)
- standards
- best practice guidelines
- SDLC

Resources

- resources consumed
- capability deployed

Practical Software and Systems Measurement



Operational Environment

External Dependencies

Security Risk Management

- Threat Modeling
- Vulnerability Management
- Security Event Management
- Damage Management
- Situation Awareness

Operations

System as operated

Ops Actions

Assurance

- evidence to support claims & assessments
- independent product testing
- integrated security argument

Performance Outcome

- delivered security performance
- risk reduction

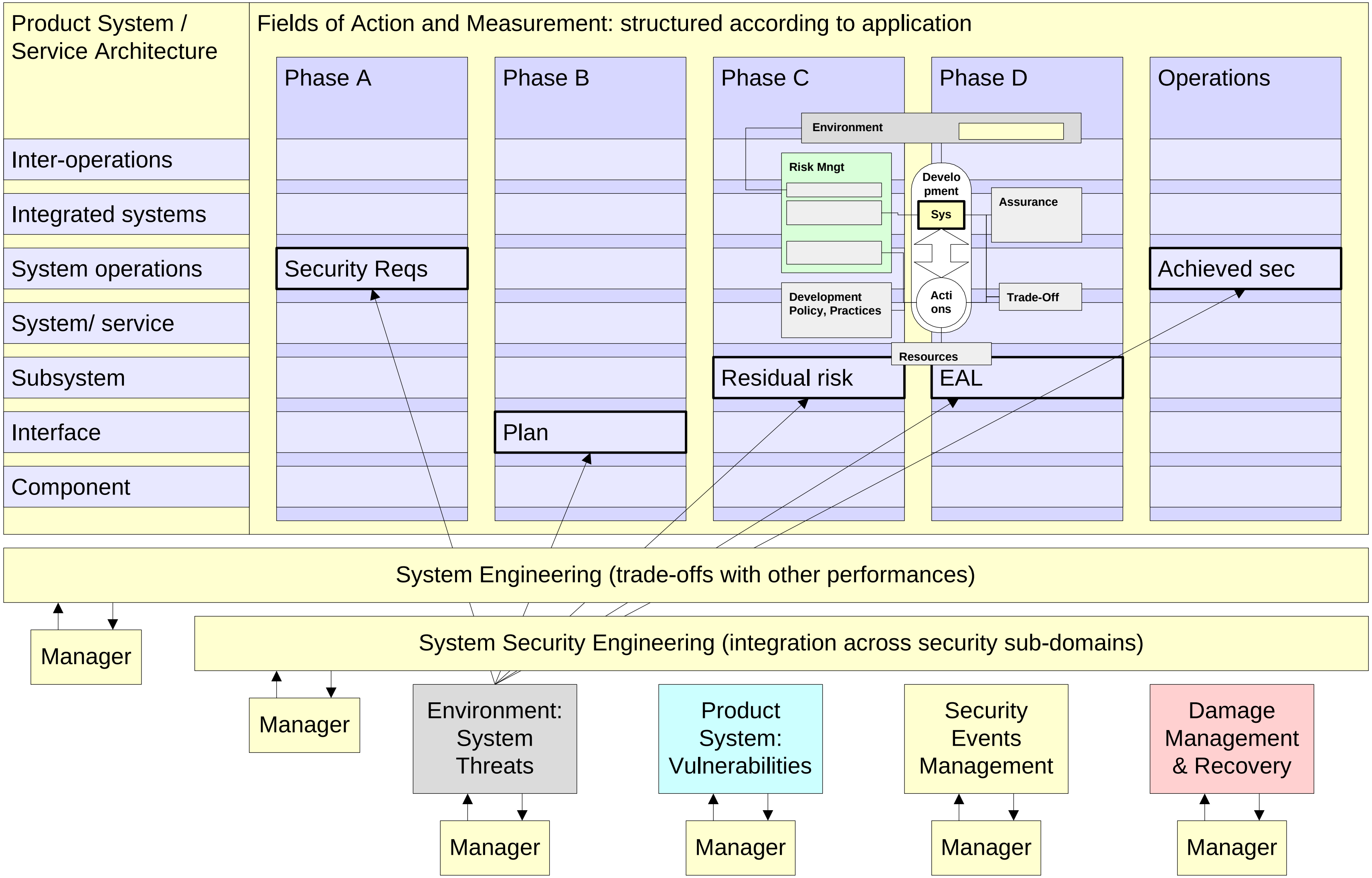
Compliance with Policy, Practices

- security policy (ops)
- standards
- best practice guidelines
- legal

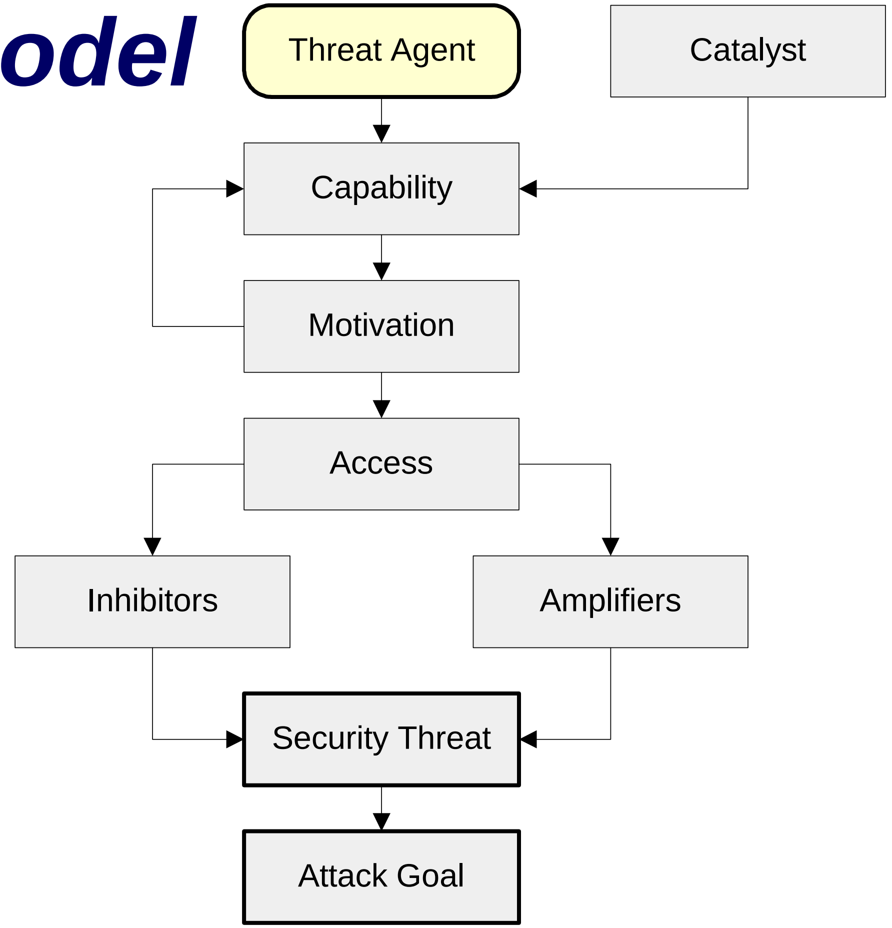
Resources

- resources consumed
- capability deployed

Practical Software and Systems Measurement


Product System / Service Architecture
Fields of Action and Measurement: structured according to application
Phase A
Phase B
Phase C
Phase D
Operations
Inter-operations
Integrated systems
System operations
System/ service
Subsystem
Interface
Component
Environment
Risk Mngt
Develo pment
Sys
Acti ons
Assurance
Trade-Off
Development Policy, Practices
Resources
Security Reqs
Achieved sec
Residual risk
EAL
Plan
System Engineering (trade-offs with other performances)
Manager
System Security Engineering (integration across security sub-domains)
Manager
Environment: System Threats
Product System: Vulnerabilities
Security Events Management
Damage Management & Recovery
Manager
Manager
Manager
Manager

Threat Agent Model



Adapted from:

Jones A. Ashenden D., Risk Management for Computer Security: protecting your network and computer assets, Elsevier, Oxford, 2005

Topic 2 Information Needs

How can we measure the benefit of security investment?

Key Indicators: what do we need to know, as a minimum, to manage security operations and engineering?

Information Needs – First Level

Are we compliant with legal and other requirements?

Are the residual security risks of a defined entity acceptably low, for defined security threats? (ALARP)

What is the Return on Security Investment (ROSI) ?

Both these questions involve:

- ***assessing the integrated security performance of an entity (systems plus processes), retrospectively & prospectively***

- ***the total costs incurred (development and operations) in providing security improvements***

At the next level of decomposition, we can ask the following questions:

Information Needs – Second Level

1. What is the capability/competence of the resources deployed on security?

   (this should address operations, acquisition/procurement, and development - how would this be objectively evaluated/appraised, and how can it be linked, as appropriate, to safety?)

2. Are security actions based on known best practice and in compliance with applicable standards and legal requirements?

   (from a US industry perspective, this should also address security requirements derived from compliance with Sarbanes-Oxley)

3. How are security and safety risks being managed?

   (and specifically, how does measurably improved security contribute to managing safety risk and privacy risks?)

Information Needs – Second Level

4. *What is the assurance evidence that defines our degree of confidence in likely future security performance?*

   (what of this could be used as indicators for future security performance? How should the PSM "Security Measurement" White Paper v1.0 30-Nov-04 be revised to target specific user needs?)

5. *What is the achieved performance of our systems in terms of managing threats, vulnerabilities, responding to events and recovering from & controlling damage?*

   (what level of decomposition is needed to address software assurance, information assurance, cybersecurity, etc.?)

Topic 3 Development of Practical Advice

1. *security measurement process*
2. *measurement information specifications*

Security Operations

- Operational Policy compliance
- Risk management
- Situation awareness
- Performance outcomes
- ROSI
- Innovation

Security Engineering

- ***Development Policy compliance***
- ***SDLC***
- ***Risk management***
- ***Situation awareness***
- ***Performance outcomes – assurance***
- ***ROSI***
- ***Innovation***

Practical Software and Systems Measurement

Information Category	Measurable Concept	Examples	Measurement Reference
Schedule and Progress	Work Unit Status	Mitigation Status	Security Risk Tracker
		Status of planned security process tasks	Project Plan
Resources and Cost	Security Capability Deployed	Competency of teams	Professional Society models
	Capability Maturity	Maturity of security practices	Audit against CMMI/ iCMM extensions
	Resources Consumed in Operations and development	Costs	Project Plan
		Schedule	Project Plan
Product Size, Stability and Scope	Scope - Security (secure system)	Security Requirements	Requirements Tracker
		Security-Critical Functions	System design and threat environment. Scope provides basis for estimating and monitoring progress
		Security-Critical Components	
		Security-Critical Interfaces	
		Security-Critical Modes	
		Security Enclaves	
		Security Change Workload	Project Plan
	Scope - Security-critical Assets	Value	Priority; level of protection required

Practical Software and Systems Measurement

Product Size, Stability and Scope			
	Scope - Security-critical Assets		
		Damage Costs	Damage scenarios
		Security Risk Tolerance	Assurance required
Environment Properties	Security Risk: Threat Agents	Threat Level [19]	Standard models
		ROI for Attacker	Attacker perceived Gain & Attack Cost
	External Dependency	Externalized Risk	Security risk borne by external agencies
	Insurance	Insured Risk	Financial risk transferred to insurer, at cost
Product Quality	Defects	Defects potentially security-related Latent defects	Categorized by SDLC phase
	Security: Attack Trees	Count of trees and status Count of Attack Paths in each tree and status	
	Security Risk: Vulnerabilities	Likelihood of attack/ exploit	Assessment Penetration Testing
		Likelihood of successful attack	

Practical Software and Systems Measurement

Product Quality			
	Security Risk: Damages/ Impacts	Impact Cost	Damage Assessments
	Security Risk: Security Events	Count of, categorized Undetected events	Monitoring Systems (e.g. IDSs)
	Security Risk: Responses	Response success rate	Monitoring Systems
	Assurance - Security: Test/ Analysis/ Inspections	CC EALs	Common Criteria independent tests
		SW scanning tools e.g. OUNCE Labs Vulnerability density	Checks implicit in tools
		Integrated Security Assurance Case	
Process Performance	Compliance: Legal	Regulatory certification	Legal requirements
	Compliance: Industry/ standards	Secure SW development – checklists of common vulnerabilities	Industry recommendations (e.g. CERT)
	Compliance: Best practice	Checklists (see Appendix 5)	DISA Checklists, Security Engineering
	Compliance: Security Policy	CISWG [4]	Adopted Security Policy
	Situation Awareness	Detected potential threats	Identified threats
	Performance Outcome: Events/ Incidents	Number of intrusions, incidents by category, ‘near misses’	Historical performance

Practical Software and Systems Measurement

Process Performance			
	Performance Outcome: Damages	Damage costs, to operator and other parties	Recovery cost monitoring systems
	Performance Outcome: Residual Risk	Residual security risk	Difficult to directly measure, but as assessed
	Performance Outcome: Effectiveness	Return on investment ROSI Response Time	
	Performance Outcome: Security Options	Security options	
	Customer Trust	Trust in organization / system as expressed by customers, users	User perception relative to the past

Topic 4 Next Steps: what are the priority tasks, collaboration, trials etc ?

- *Trials*
- *Engaging with security engineering communities*
- *Engaging with other programs:*
    - *DoD metrics*
    - *NIST*
    - *Cybersecurity*
    - *iCMM/CMMI etc*
    - *SEI*