

TEL2813/IS2621

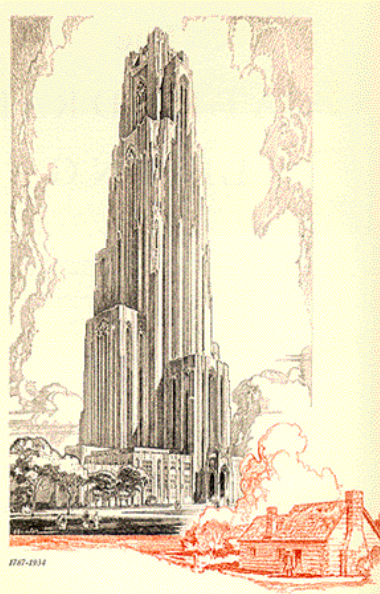
Security Management

James Joshi

Associate Professor

Lecture 7

March 19, 2015



Managing Secure Development : Models/Methodologies
Supply Chain Security



Some Terms: Process

- Process
 - A sequence of steps performed for a given purpose [IEEE]
- Secure Process
 - Set of activities performed to develop, maintain, and deliver a secure system/software solution
 - Activities could be concurrent or iterative



Process Models

- **Process model**
 - provides a reference set of best practices
 - process improvement and
 - process assessment.
 - defines the characteristics of processes.
 - Usually have an architecture or a structure.
- Most process models also have a *capability* or *maturity* dimension, that can be used for
 - assessment and
 - evaluation purposes.



Process Models

- Process Models

- have been produced to create
 - common measures of organizational processes throughout the software development lifecycle (SDLC).
- identify many technical and management practices
- primarily address good system/software engineering practices to manage system/software development

Cannot guarantee system/software developed is bug free



Assessments

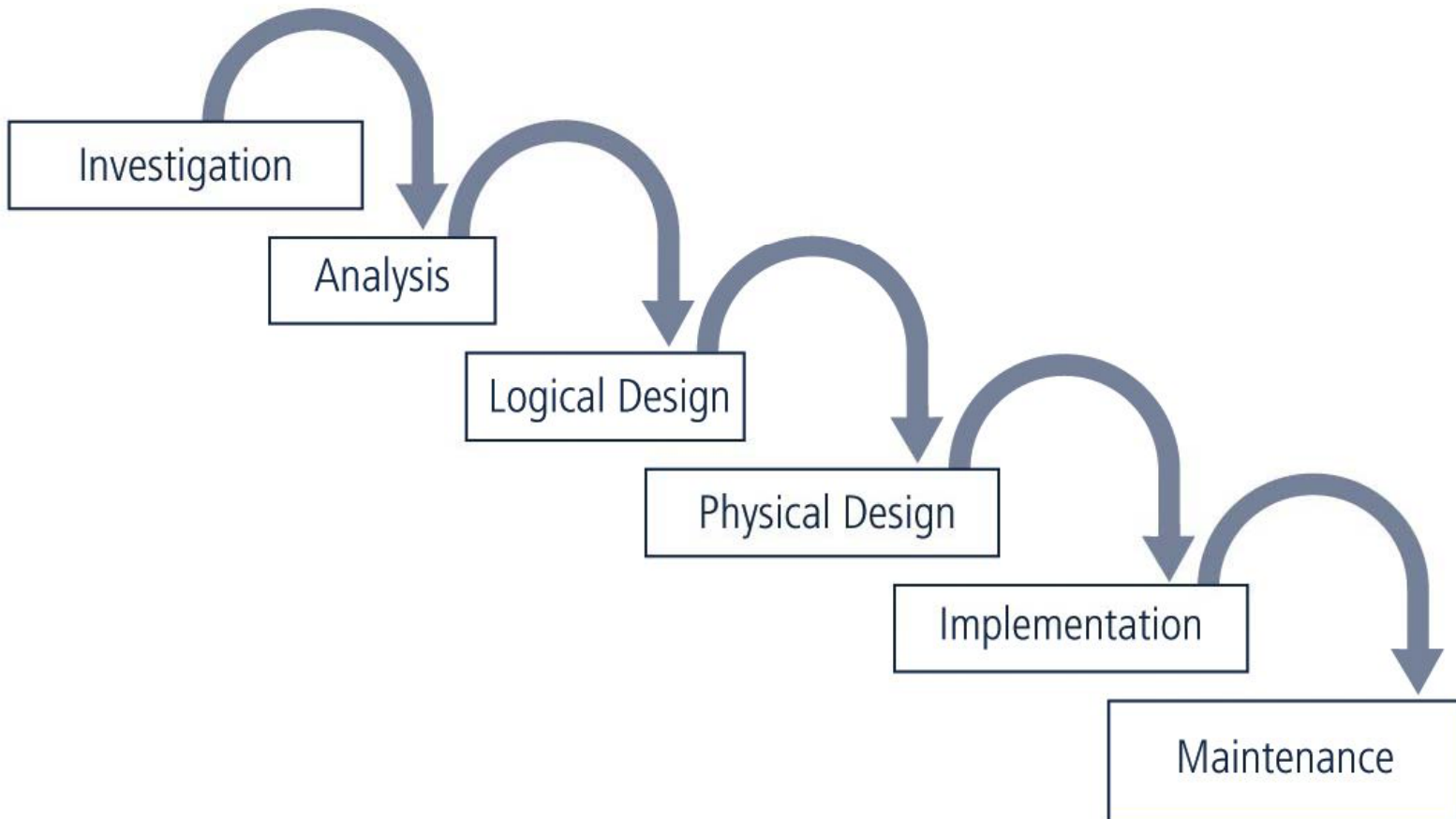
- **Assessments, evaluations, appraisals**
 - Imply comparison of a process being practiced to a reference process model or standard,
 - used to understand process capability in order to improve processes,
 - help determine if the processes being practiced are
 - adequately specified, designed, integrated, and implemented sufficiently to support the needs



S/S Development Life Cycle (SDLC)

- Following four SDLC focus areas for secure S/S development.
 - Security Engineering Activities
 - Security Assurance
 - Security Organizational and Project Management Activities
 - Security Risk Identification and Management Activities

System DLC





Capability Maturity Models (CMM)

- CMM

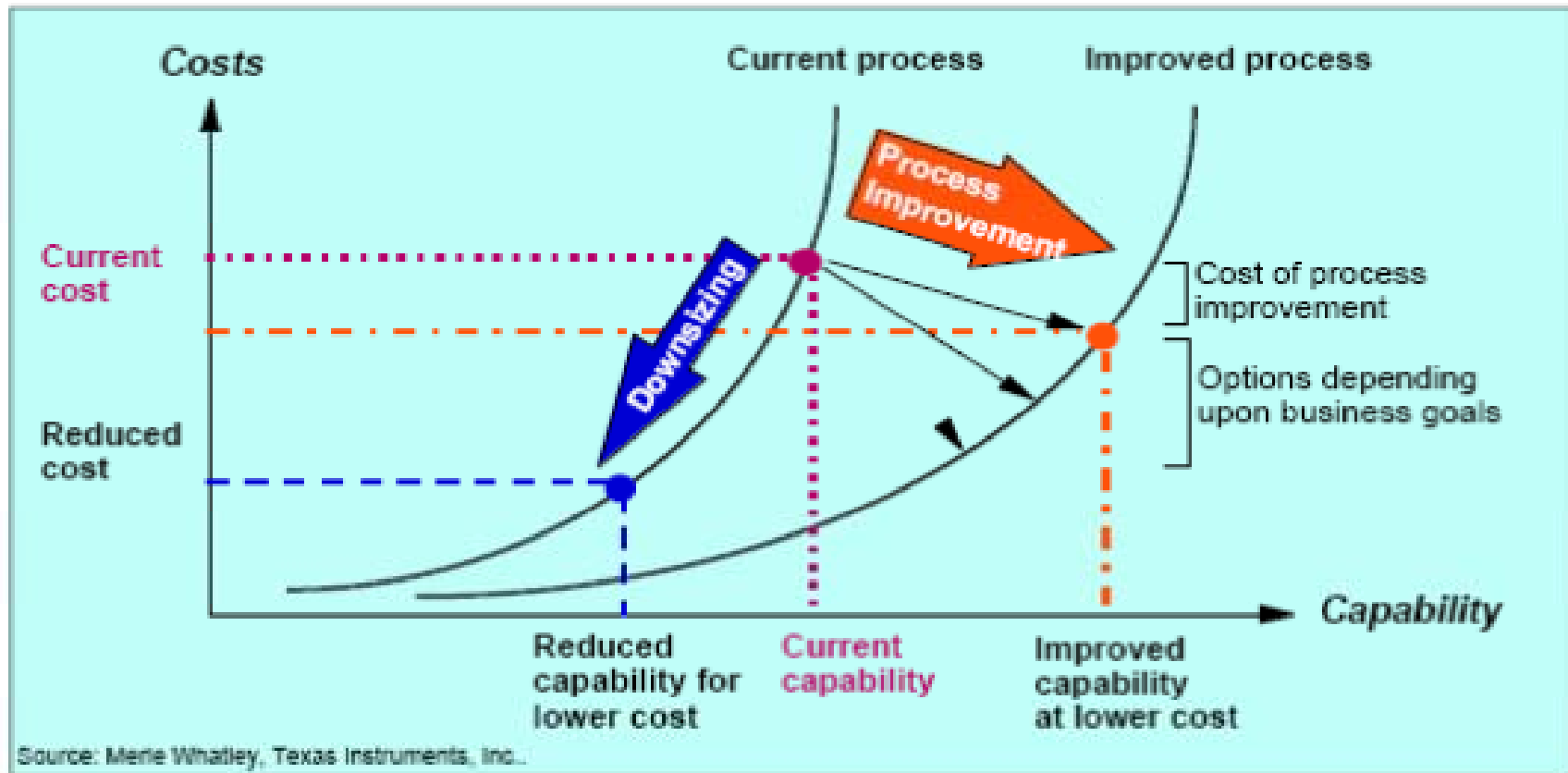
- *Defines process characteristics*
- Provides reference model of mature practices
- Helps identify the potential areas of improvement
- Provides goal-level definition for and key attributes for specific processes
- No operational guidance



CMM

- Three CMMs
 - Capability Maturity Model Integration® (CMMI®),
 - The integrated Capability Maturity Model (iCMM),
 - The Systems Security Engineering Capability Maturity Model (SSE-CMM)
 - Specifically developed for security

Why CMM?



Source: http://www.secat.com/download/locked_pdf/SSEovrw_lkd.pdf



CMMI

- CMM Integration (CMMI) provides
 - the latest best practices for product and service development, maintenance, and acquisition,
 - including mechanisms to help organizations improve their processes and
 - criteria for evaluating process capability/maturity.
- As of Dec 2005, the SEI reports
 - 1106 organizations and 4771 projects have reported results from CMMI-based appraisals
- its predecessor, the software CMM (SW-CMM)
 - Since 80s – Dec, 2005
 - 3049 Organizations + 16,540 projects

CMMI Categories

Process Management

Organizational Process Focus

Organization Process Definition

Organizational Training

Organizational Process Performance

Organizational Innovation and Deployment

Project Management

Project Planning

Project Monitoring and Control

Supplier Agreement Management

Integrated Project Management

Risk Management

Integrated Teaming

Integrated Supplier Management

Quantitative Project Management

Engineering

Requirements Development

Requirements Management

Technical Solution

Product Integration

Verification

Validation

Support

Configuration Management

Process and Product Quality Assurance

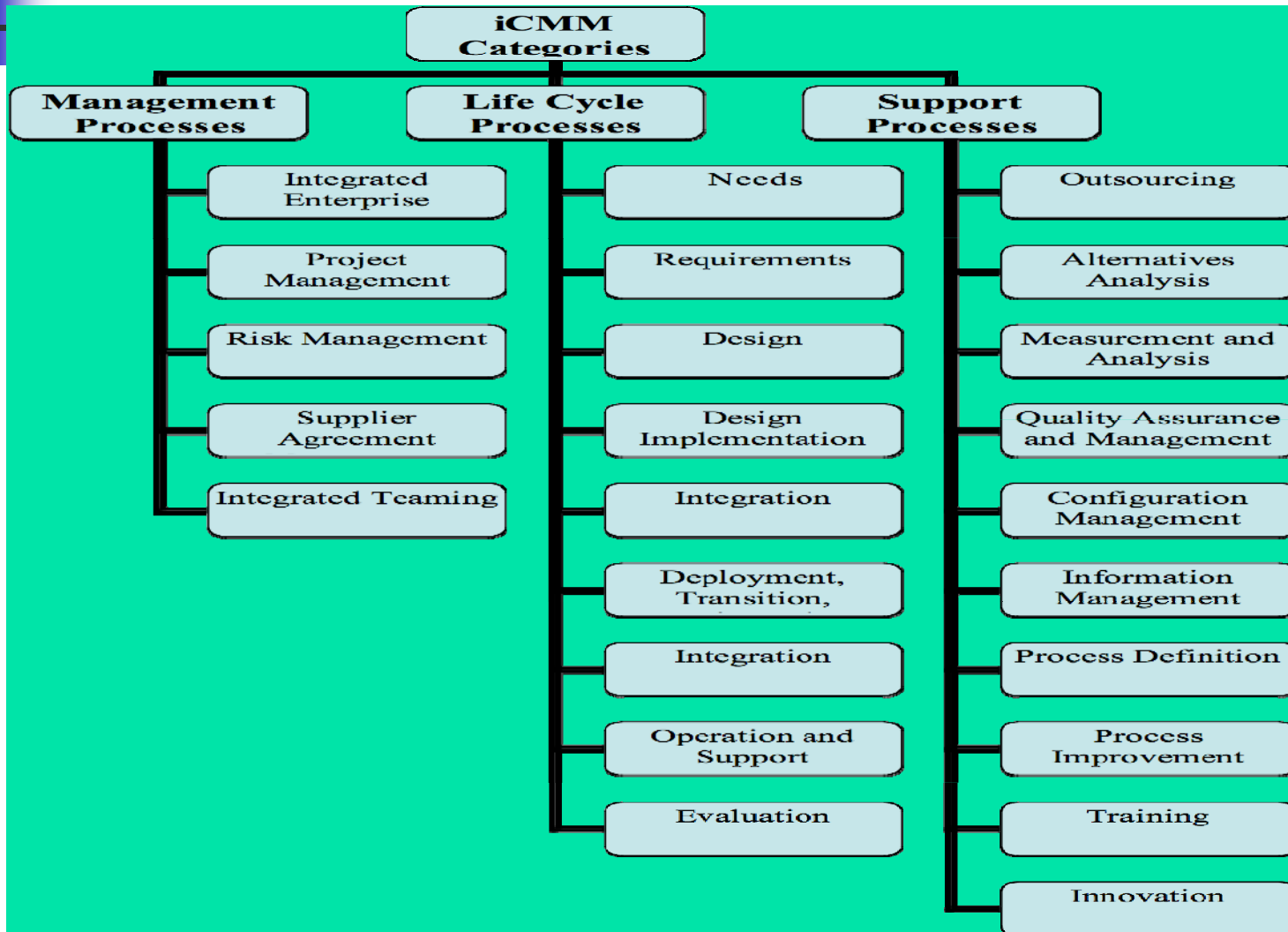
Measurement and Analysis

Organizational Environment for Integration

Decision Analysis and Resolution

Causal Analysis and Resolution

Integrated CMM





Trusted CMM

- Trusted CMM
 - In early 1990 as Trusted Software Methodology (TSM)
 - TSM defines trust levels
 - *Low* emphasizes resistance to unintentional vulnerabilities
 - *High* adding processes to counter malicious developers
 - TSM was later harmonized with CMM
 - Not much in use



Systems Security Engineering CMM

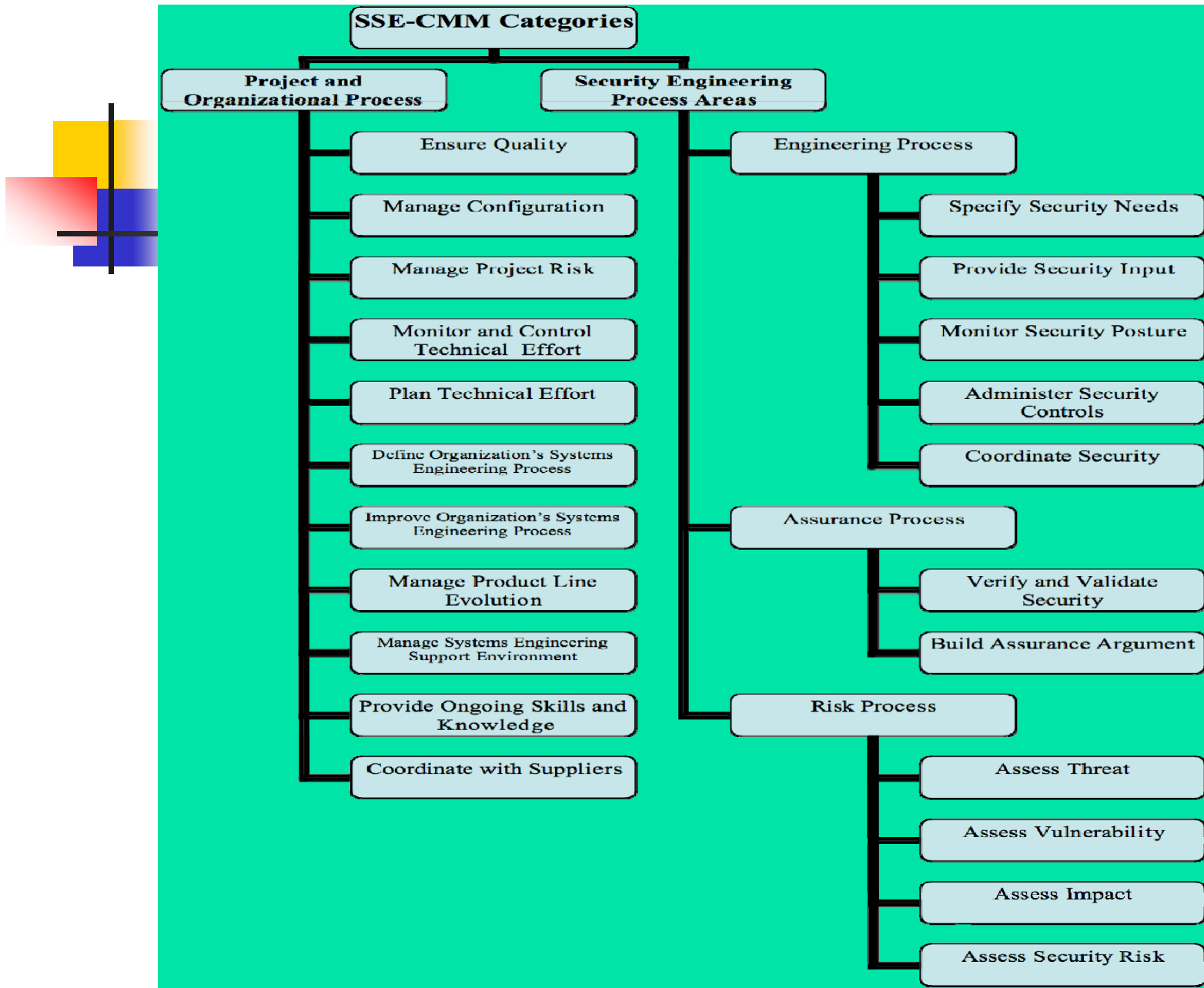
- The SSE-CMM

- is a process model that can be used to improve and assess
 - the security engineering capability of an organization.
- provides a comprehensive framework for
 - evaluating security engineering practices against the generally accepted security engineering principles.
- provides a way to measure and improve performance in the application of security engineering principles.



SSE-CMM

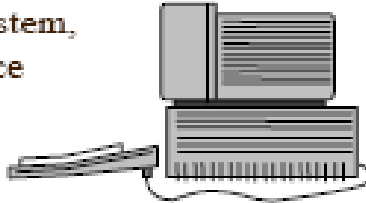
- Purpose for SSE-CMM
 - Fulfills a lack a comprehensive framework for evaluating security engineering practices against the principles.
- The SSE-CMM also
 - describes the essential characteristics of an organization's security engineering processes
- The SSE-CMM is now ISO/IEC 21827 standard (version 3 is available)





Security Engineering Process

Product, System,
or Service



Engineering
Process

Assurance
Process

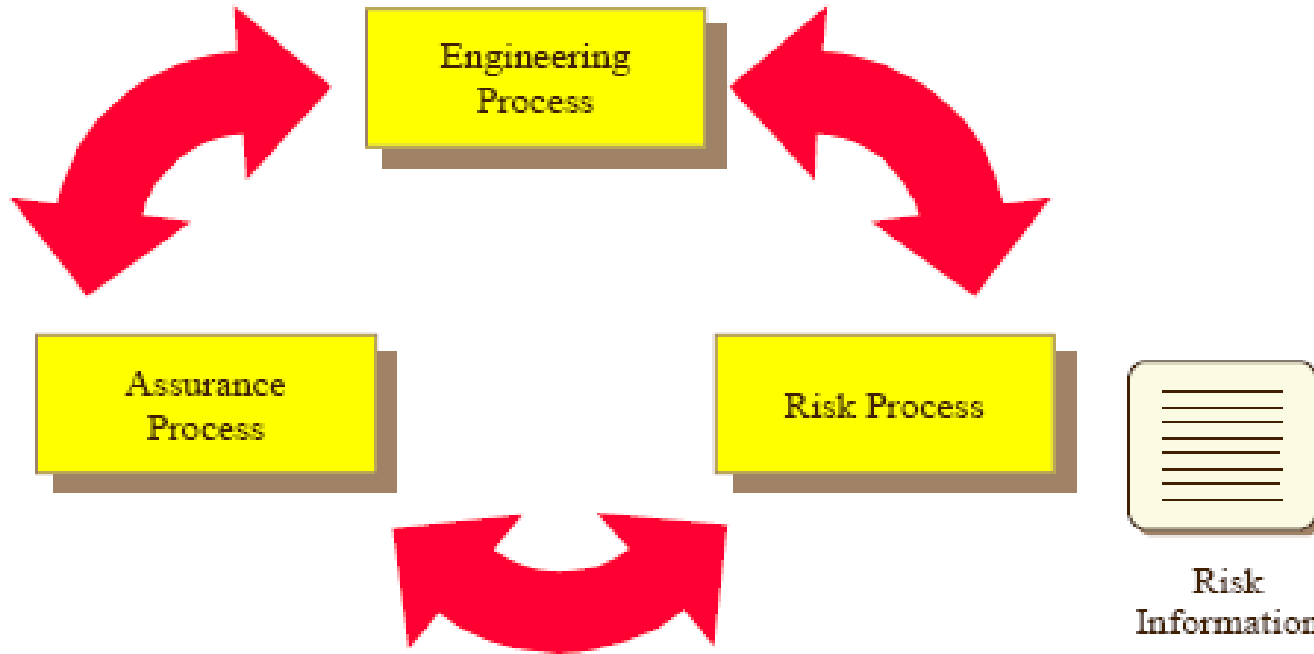
Risk Process



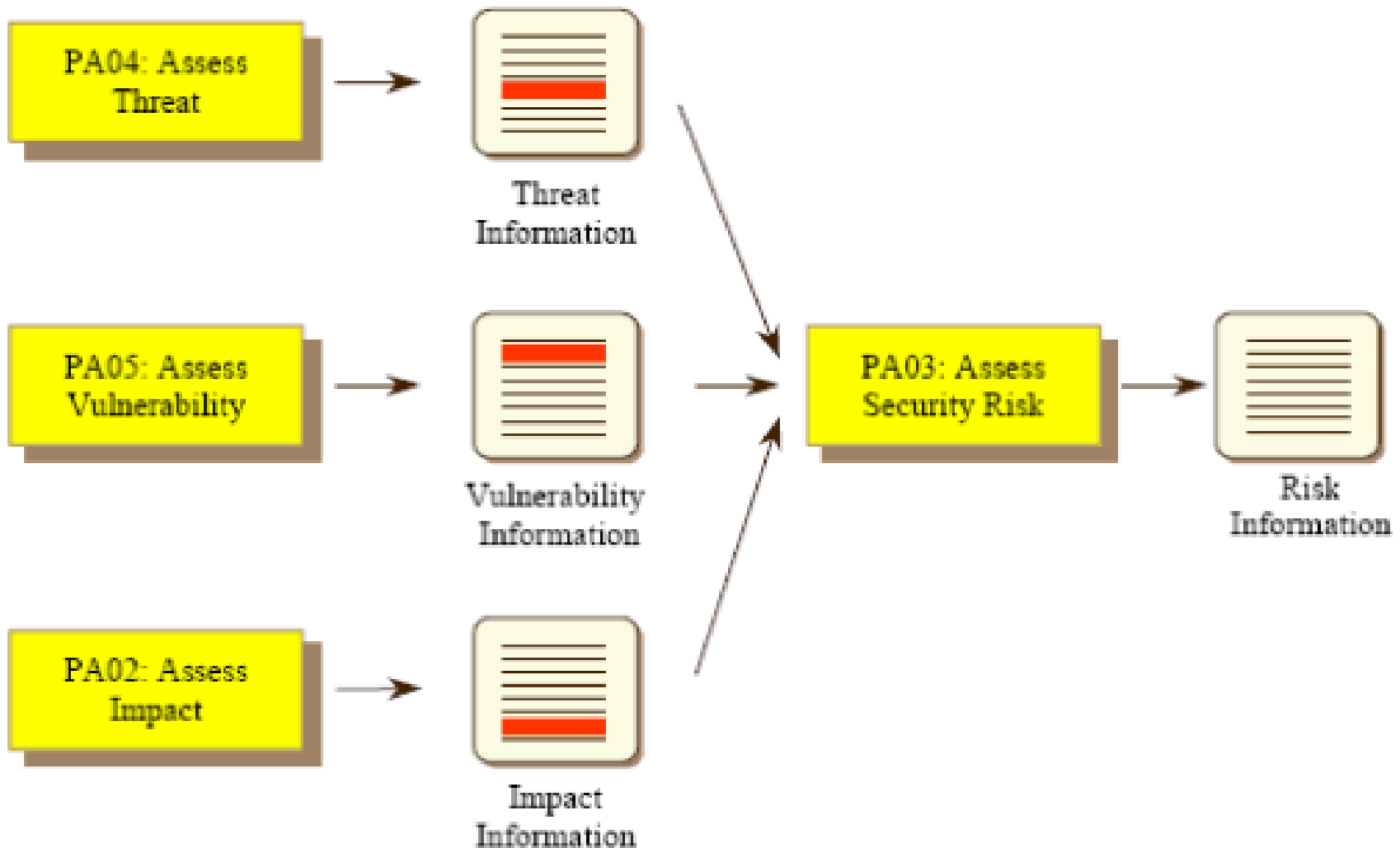
Assurance
Argument



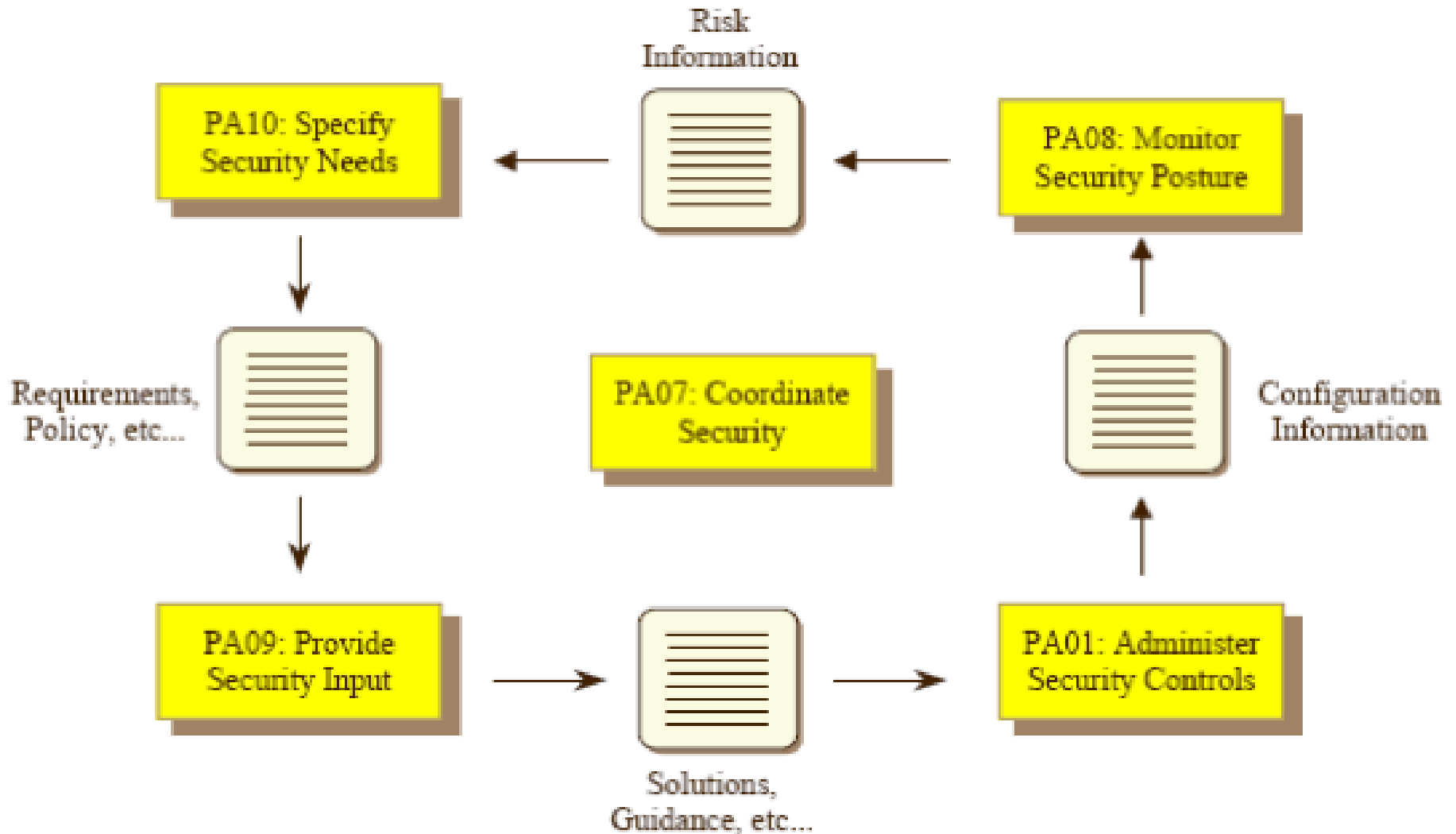
Risk
Information



Security Risk Process

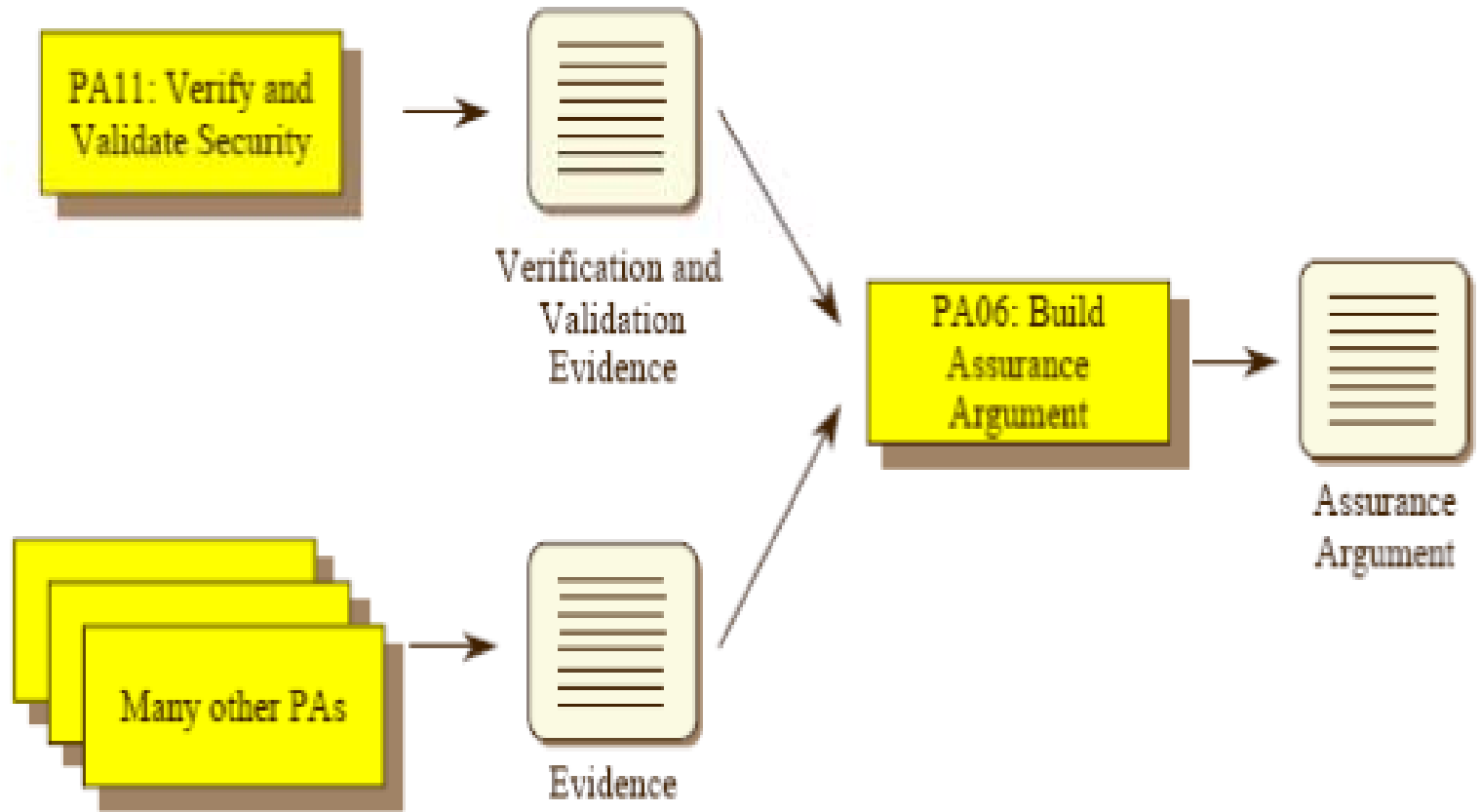


Security is part of Engineering



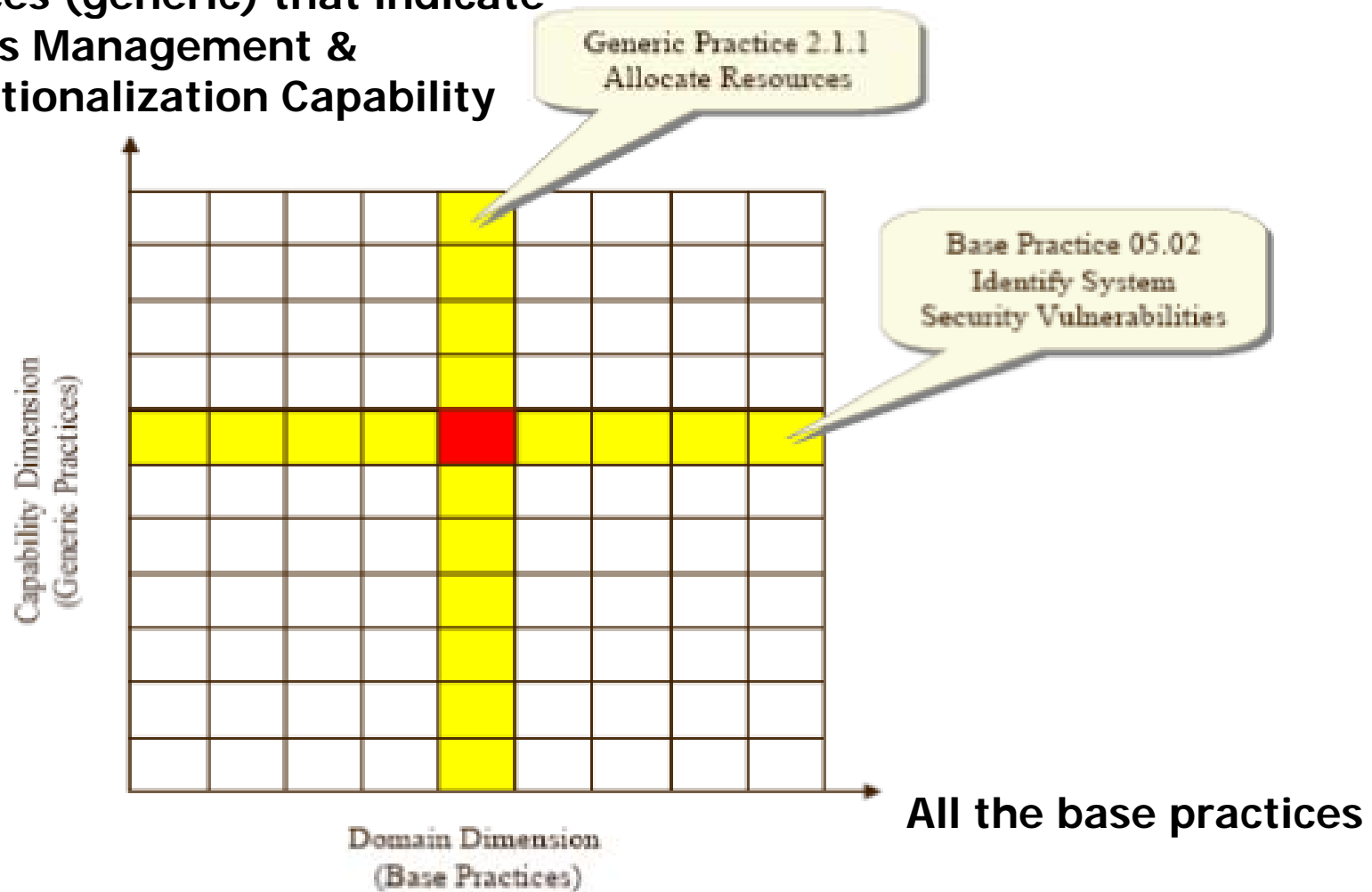


Assurance



SSE-CMM Dimensions

Practices (generic) that indicate
Process Management &
Institutionalization Capability





SSE-CMM

- 129 base practices Organized into 22 process areas
 - 61 of these, organized in 11 process areas, cover all major areas of security engineering
 - Remaining relates to project and organization domains
- Base practice
 - Applies across the life cycle of the enterprise
 - Does not overlap with other base practices
 - Represents a “best practice” of the security community
 - Does not simply reflect a state of the art technique
 - Is applicable using multiple methods in multiple business context
 - Does not specify a particular method or tool



Process Area

- Assembles related activities in one area for ease of use
- Relates to valuable security engineering services
- Applies across the life cycle of the enterprise
- Can be implemented in multiple organization and product contexts
- Can be improved as a distinct process
- Can be improved by a group with similar interests in the process
- Includes all base practices that are required to meet the goals of the process area



Process Areas

Process Areas related to Security Engineering process areas

- PA01 Administer Security Controls
- PA02 Assess Impact
- PA03 Assess Security Risk
- PA04 Assess Threat
- PA05 Assess Vulnerability
- PA06 Build Assurance Argument
- PA07 Coordinate Security
- PA08 Monitor Security Posture
- PA09 Provide Security Input
- PA10 Specify Security Needs
- PA11 Verify and Validate Security

Process Areas related to project and Organizational practices

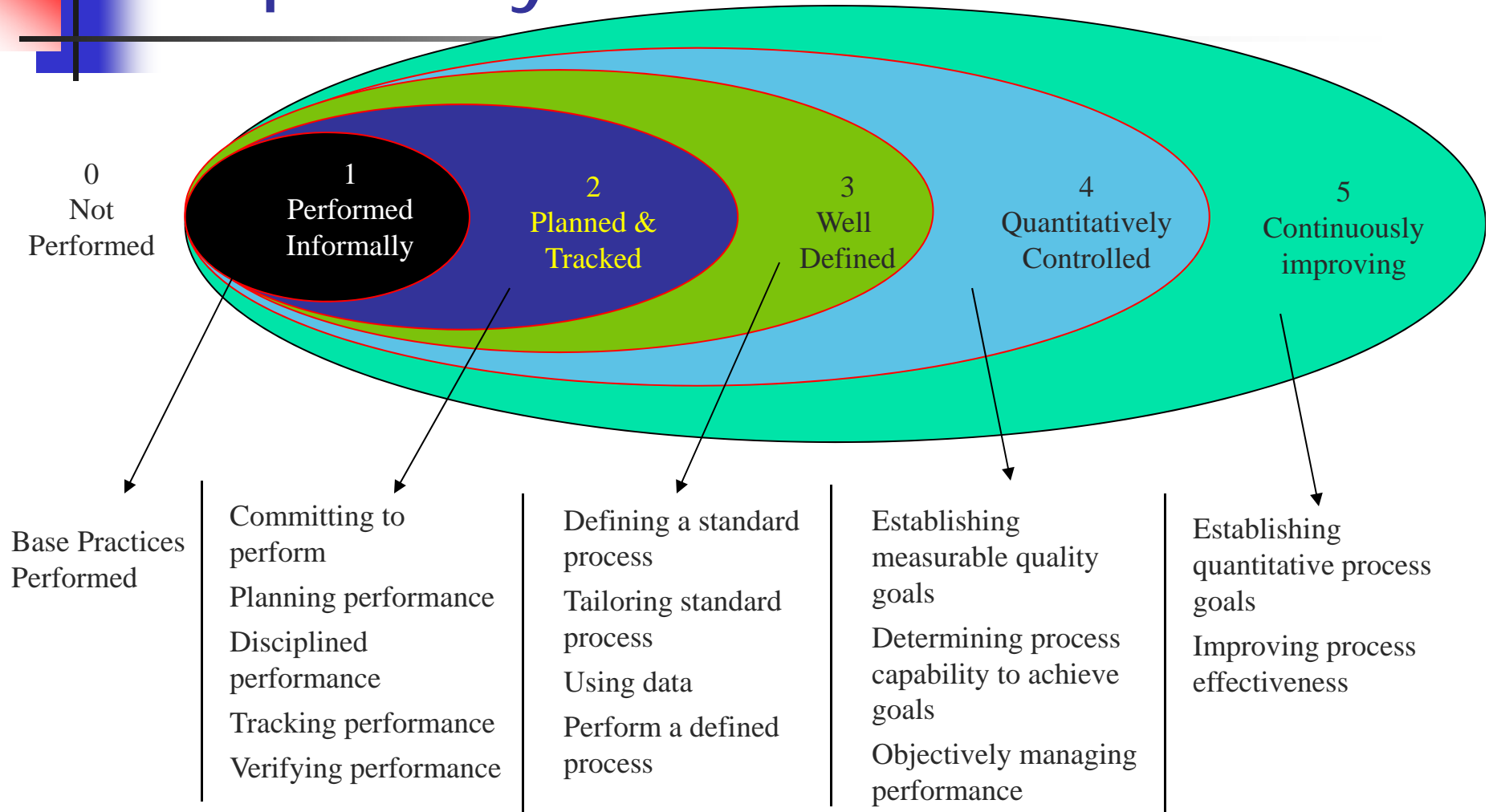
- PA12 – Ensure Quality
- PA13 – Manage Configuration
- PA14 – Manage Project Risk
- PA15 – Monitor and Control Technical Effort
- PA16 – Plan Technical Effort
- PA17 – Define Organization's Systems Engineering Process
- PA18 – Improve Organization's Systems Engineering Process
- PA19 – Manage Product Line Evolution
- PA20 – Manage Systems Engineering Support Environment
- PA21 – Provide Ongoing Skills and Knowledge
- PA22 – Coordinate with Suppliers



Generic Process Areas

- Activities that apply to all processes
- They are used during
 - Measurement and institutionalization
- Capability levels
 - Organize common features
 - Ordered according to maturity

Capability Levels





Using SSE-CMM

- Can be used in one of the three ways
 - Process improvement
 - Facilitates understanding of the level of security engineering process capability
 - Capability evaluation
 - Allows a consumer organization to understand the security engineering process capability of a provider
 - Assurance
 - Increases the confidence that product/system/service is trustworthy



Capability Evaluation

- No need to use any particular appraisal method
 - SSE-CMM Appraisal method (SSAM) as been developed (if appraisal is needed)
- SSAM purpose
 - Obtain the baseline or benchmark of actual practice related to security engineering within the organization or project
 - Create or support momentum for improvement within multiple levels of the organizational structure



SSAM Overview

- Planning phase
 - Establish appraisal framework
- Preparation phase
 - Prepare team for onsite phase through information gathering (questionnaire)
 - Preliminary data analysis indicate what to look for / ask for
- Onsite phase
 - Data gathering and validation with the practitioner
 - interviews
- Post-appraisal
 - Present final data analysis to the sponsor

Capability Evaluation

Level 5																							
Level 4																							
Level 3																							
Level 2																							
Level 1																							
Capability Levels	Process Areas	PA01	PA02	PA03	PA04	PA05	PA06	PA07	PA08	PA09	PA10	PA11	PA12	PA13	PA14	PA15	PA16	PA17	PA18	PA19	PA20	PA21	PA22
		Security Engineering Process Areas											Project and Organizational Process Areas										



Assurance

- A mature organization is significantly more likely to create a product or system with appropriate assurance
- Process evidence can be used to support claims for the trustworthiness of those products/systems
- It is conceivable that
 - An immature organization could produce high assurance product.



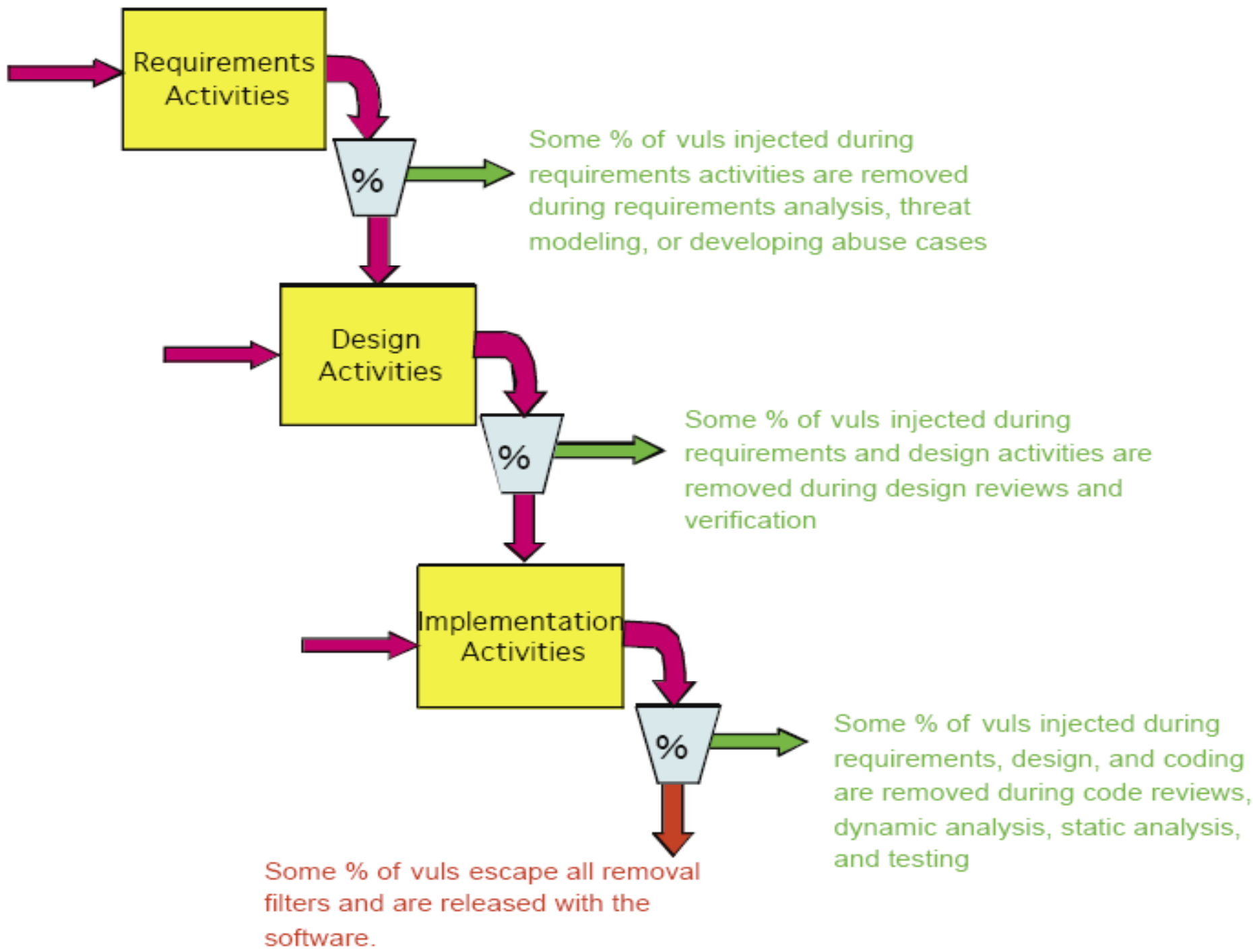
CMMI/iCMM/SSE-CMM

- Because of the integration of process disciplines and coverage of enterprise issues,
 - the CMMI and the iCMM are used by more organizations than the SSE-CMM;
- CMMI and iCMM have gaps in their coverage of safety and security.
- FAA and the DoD have sponsored a joint effort to identify best safety and security practices for use in combination with the iCMM and the CMMI.



Team Software Process for Secure SW/Dev

- TSP
 - provides a framework, a set of processes, and disciplined methods for applying software engineering principles at the team and individual level
- TSP for Secure Software Development (TSP-Secure)
 - focus more directly on the security of software applications.





Correctness by Construction

- CbC Methodology from Praxis Critical Systems
 - Process for developing high integrity software
 - Has been successfully used to develop safety-critical systems
 - Removes defects at the earliest stages
 - the process almost always uses formal methods to specify behavioral, security and safety properties of the software.



Correctness by Construction

- The seven key principles of Correctness-by-Construction are:
 - Expect requirements to change.
 - Know why you're testing (debug + verification)
 - Eliminate errors before testing
 - Write software that is easy to verify
 - Develop incrementally
 - Some aspects of software development are just plain hard.
 - Software is not useful by itself.

Correctness by Construction

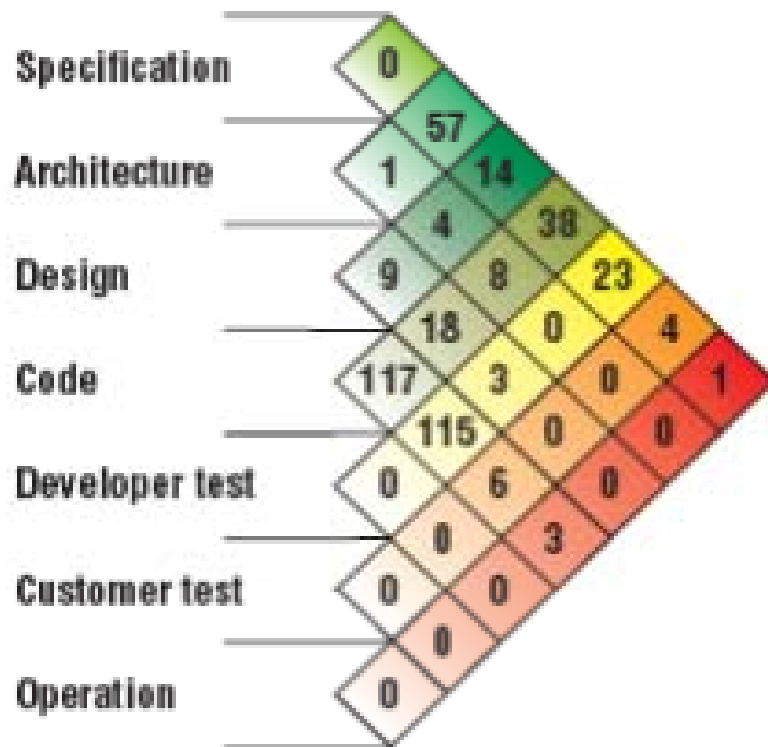


Table 1

Distribution of effort.

Activity	Effort (%)
Requirements	2
Specification and architecture	25
Code	14
Test	34
Fault fixing	6
Project management	10
Training	3
Design authority	3
Development- and target-environment	3



Agile Methods

- Agile manifesto
 - “We are **uncovering better** ways of developing software by **doing it** and **helping others** do it. Through this work we have come to value:
 - *Individuals and interactions* over processes and tools
 - *Working software* over comprehensive documentation
 - *Customer collaboration* over contract negotiation
 - *Responding to change* over following a plan
 - That is, while there is value in the items on the right, we value the items on the left more.”

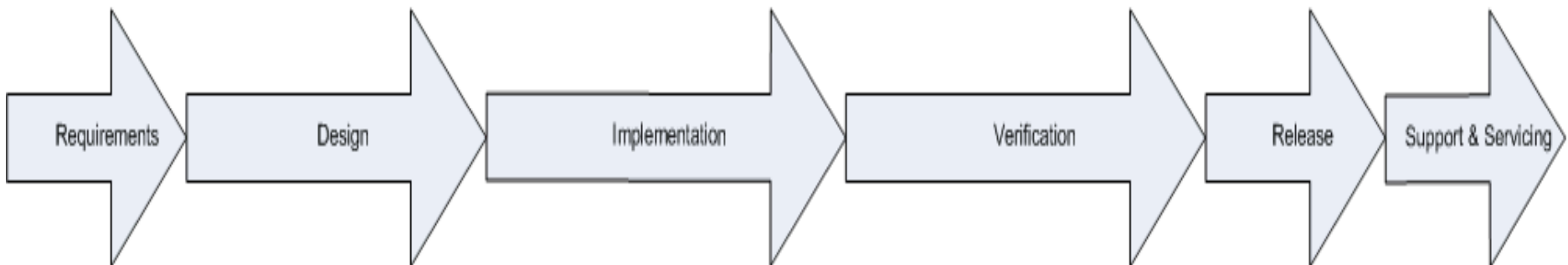


Agile Processes

- Among many variations
 - Adaptive software development (ASP)
 - Extreme programming (XP)
 - Crystal
 - Rational Unified Process (RUP)

Microsoft Trustworthy Computing SDLC

- Generally accepted SDL process at MS
 - (actually spiral not “waterfall” as it indicates)





SDL Overview

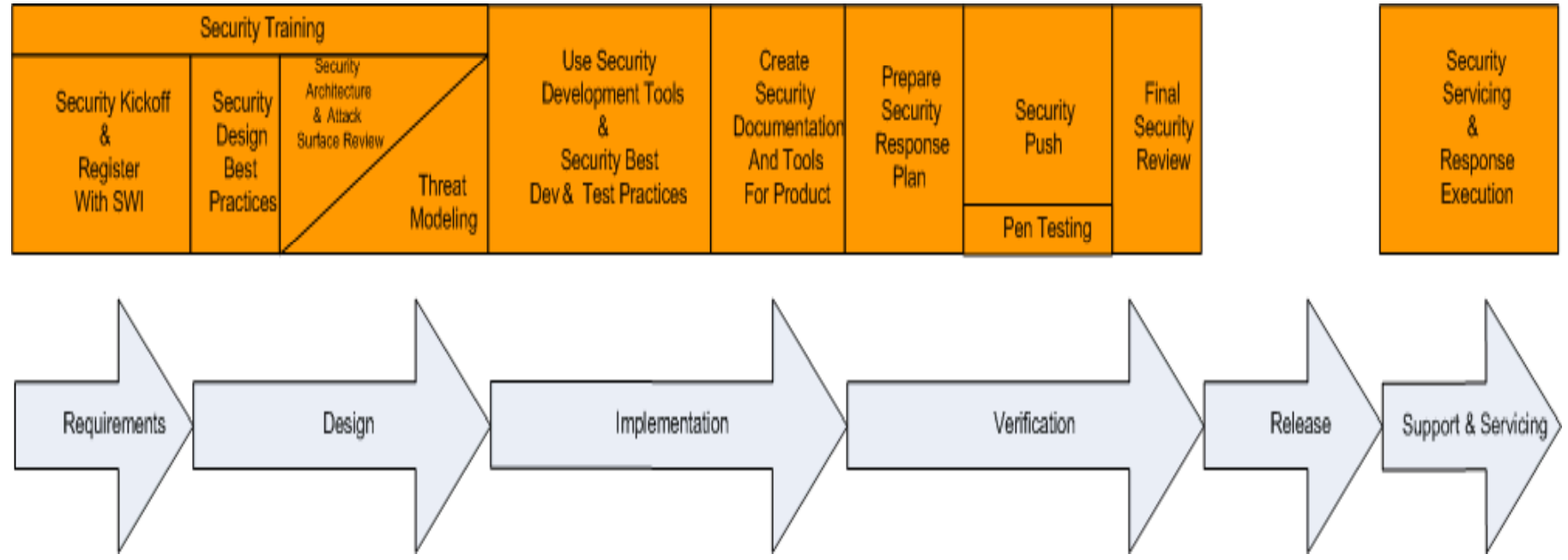
- MS's SD³ + C paradigm
 - Secure by Design
 - Secure by Default
 - Secure by Deployment
 - Communications
 - software developers should be prepared for the discovery of product vulnerabilities and should communicate openly and responsibly

The SDL is updated as shown next



SDL at MS

- Add the SD³ + C praradigm





Design Phase

- Define Security architecture and design guidelines
 - Identify tcb; use layering etc.
- Document the elements of the software attack surface
 - Find out default security
- Conduct threat modeling
- Define supplemental ship criteria



Implementation phase

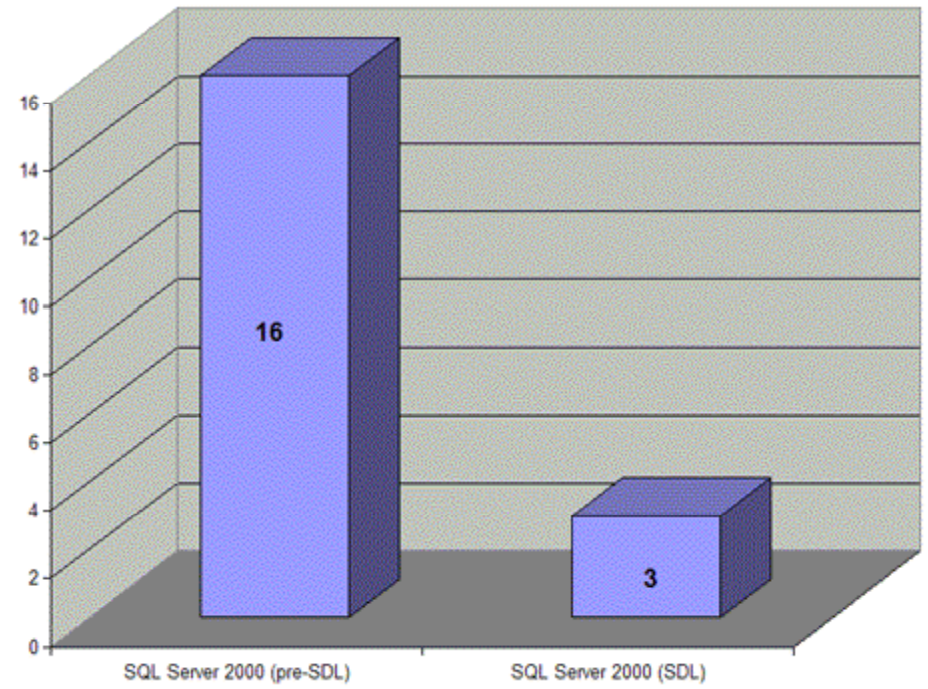
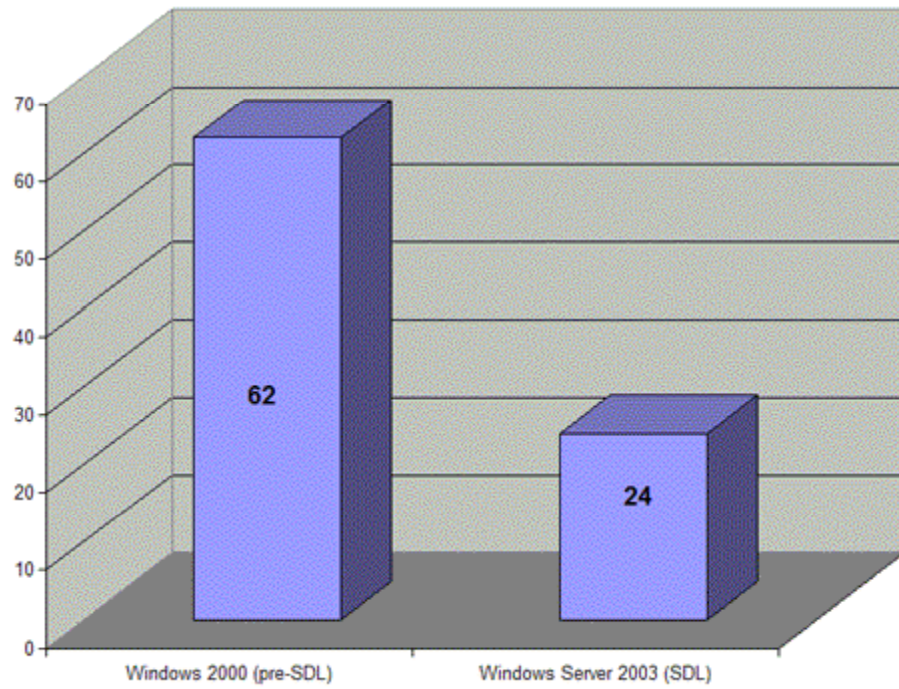
- Apply coding and testing standards
- Apply security testing tools including fuzzing tools
- Apply static analysis code scanning tools
- Conduct code reviews



Verification Phase

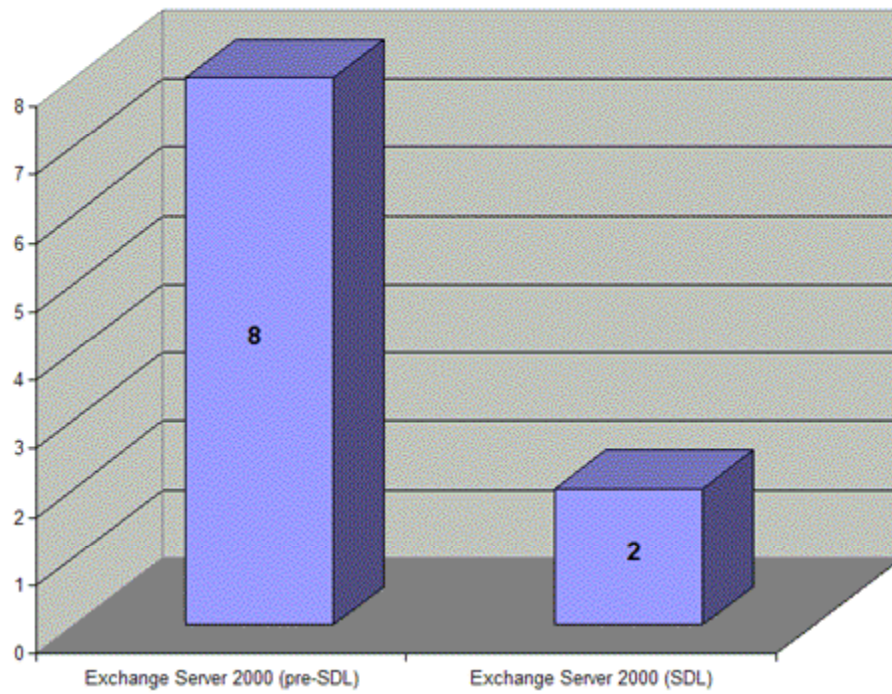
- “Security push” for Windows server 2003
 - Includes code review beyond those in implementation phase and
 - Focused testing
- Two reasons for “security push”
 - Products had reached the verification phase
 - Opportunity to review both code that was developed or updated during the implementation phase and “legacy code” that was not modified

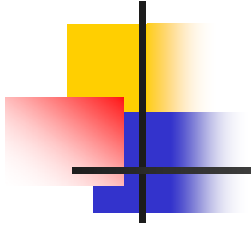
Results





Results





Supply Chain Security

ICT Supply Chain

Complex, Global, Distributed, Interconnected Networks

- Organizations, processes, products, services and infrastructure
- Today's: Significant Complexity Diversity and Scale
- System integrators
 - distinct role of assembling information systems, system components, and information services



Example:

Target breach – HVAC company

Global supply chain is the "the next playground for hackers,"
(International Maritime Bureau (IMB))

Gartner Says IT Supply Chain Integrity Will Be Identified as a Top Three Security-Related Concern by Global 2000 IT Leaders by 2017

Supply Chain Risk

- ICT supply chain risks include
 - insertion of counterfeits, tampering, theft, and insertion of malicious software.
- Risks through exploits of vulnerabilities
 - Reduced functionality: poor or counterfeit components
 - Unwanted functionality: malware inserted, poor quality

ICT Supply Chain Risk

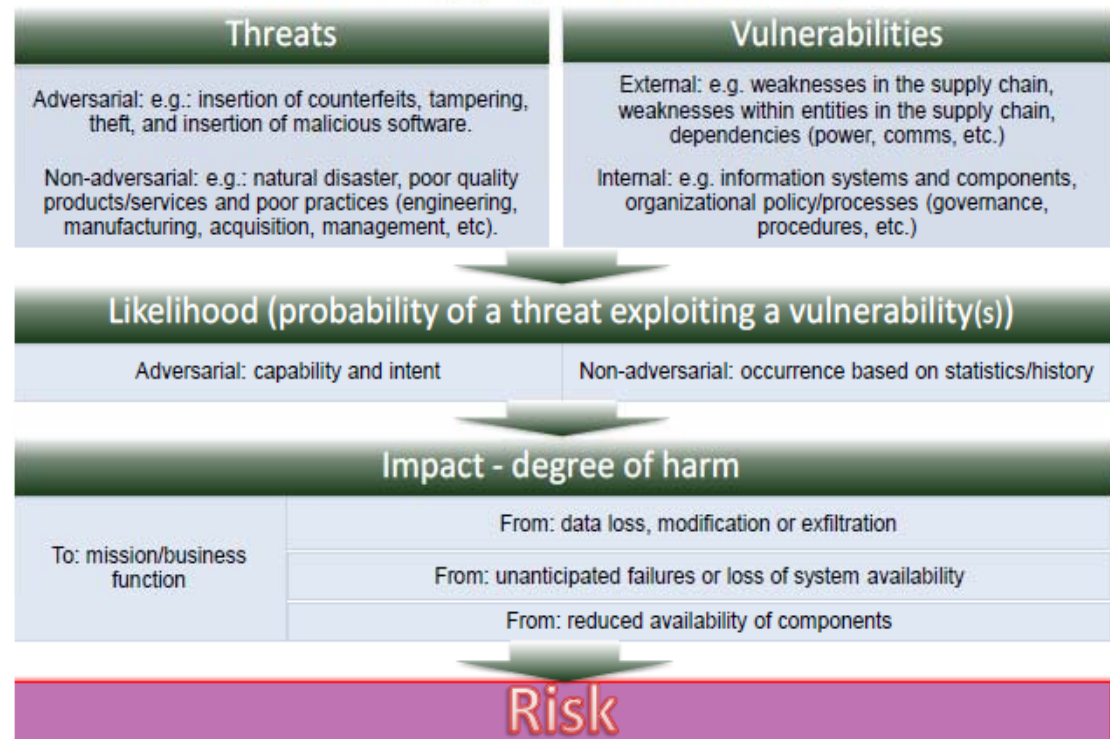


Figure 1-1. ICT Supply Chain Risk

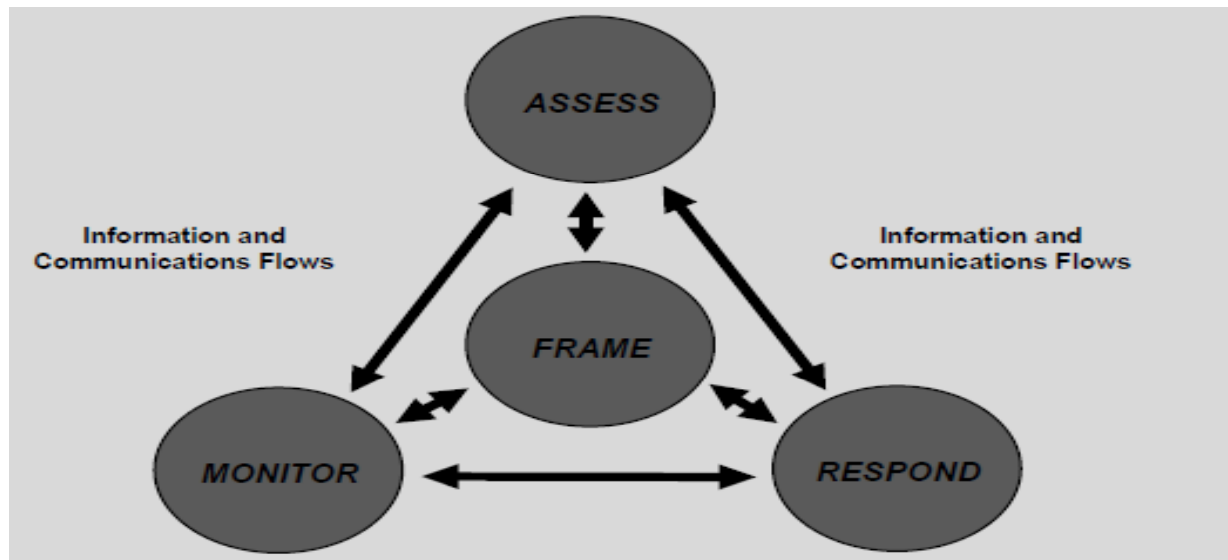


SC and Globalization

- Adversary may include:
 - **Individuals, Orgs, Nation-states**
 - Directly or indirectly affect management and operations of companies; E.g.,
 - foreign nation states may force (i) a manufacturer to hand over spec of sensitive US system (ii) insert malware
- Need to protect information that
 - describes the ICT supply chain (e.g., information about the paths of ICT products and services, both logical and physical),
 - traverses the ICT supply chain (e.g., intellectual property contained in ICT products and services), and
 - information about the parties participating in the ICT supply chain (anyone who touches an ICT product or service throughout its life cycle).

Integrate SC with RM

- *Frame risk* – establish the context for risk-based decisions and the current state of the system or ICT supply chain environment;
- *Assess risk* – review and interpret threat, vulnerability, and related information;
- *Respond to risk once determined* – select, tailor, and implement mitigation controls; and,
- *Monitor risk* on an ongoing basis, including changes to an information system or ICT supply chain environment,



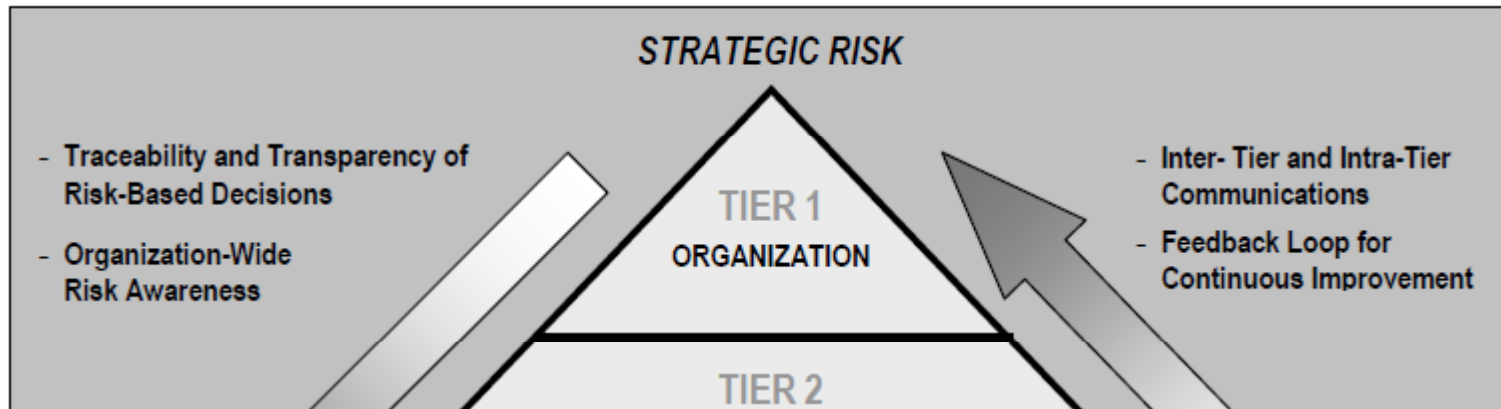


Table 2-1: Supply Chain Risk Management Stakeholders

Tiers	Tier Name	Generic Stakeholder	Activities
1	Organization	Executive Leadership (CEO, CIO, COO, CFO, CISO, CTO, etc.) - Risk executive	Corporate Strategy, Policy, goals and strategies
Tiers	Tier Name	Generic Stakeholder	Activities
2	Mission	Business Management (includes program management (PM), research and development (R&D), Engineering [SDLC oversight], Acquisitions / Procurement, Cost Accounting, - "ility" management [reliability, safety, quality], etc.)	Actionable Policies and procedures, Guidance and constraints
3	Operation	Systems Management (architect, developers, QA/QC, test, contracting personnel (approving selection, payment and approach for obtaining, maintenance engineering, disposal personnel, etc.)	Policy implementation Requirements, constraints implementations

ICT SCRM Activities in Risk Management Process

	Frame	Assess	Respond	Monitor
Enterprise	<ul style="list-style-type: none"> Develop ICT SCRM Policy Conduct Baseline Criticality Determination Integrate ICT SCRM considerations into enterprise risk management 	<ul style="list-style-type: none"> Integrate ICT SCRM considerations into enterprise risk management 	<ul style="list-style-type: none"> Make enterprise risk decisions to avoid, mitigate, share, or transfer risk Select, tailor, and implement appropriate enterprise ICT SCRM controls Document controls in Enterprise ICT SCRM Plan 	<ul style="list-style-type: none"> Integrate ICT SCRM into agency Continuous Monitoring program Monitor and evaluate enterprise-level constraints and risks for change and impact Monitor effectiveness of enterprise-level risk response
Mission/Business Process	<ul style="list-style-type: none"> Define ICT SCRM Mission/business requirements Incorporate these requirements into mission/ business processes and enterprise architecture Establish ICT SCRM Risk Assessment Methodology Establish FIPS 199 impact levels Conduct Mission Function Baseline Criticality Determination Determine ICT SCRM risk assessment methodology 	<ul style="list-style-type: none"> Conduct Risk Assessment including Criticality Analysis for mission threads Determine current risk posture 	<ul style="list-style-type: none"> Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk Select, tailor, and implement appropriate mission/ business-level controls Document controls in Mission-level ICT SCRM Plan 	<ul style="list-style-type: none"> Identify which mission functions need to be monitored for ICT supply chain change and assessed for impact Integrate ICT SCRM into Continuous Monitoring processes and systems Monitor and evaluate mission-level risks and constraints for change and impact Monitor effectiveness of mission level risk response
System	<ul style="list-style-type: none"> Define system-level ICT SCRM requirements 	<ul style="list-style-type: none"> Conduct ICT SCRM Risk Assessment including Criticality Analysis for individual systems Determine current risk posture 	<ul style="list-style-type: none"> Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk Select, tailor, and implement appropriate system-level controls Document ICT SCRM controls in System Security Plan 	<ul style="list-style-type: none"> Monitor and evaluate system-level requirements and risks for change and impact Monitor effectiveness of system-level risk response

Figure 2-3. ICT SCRM Activities in Risk Management Process

SCRM Risk Assessment Process

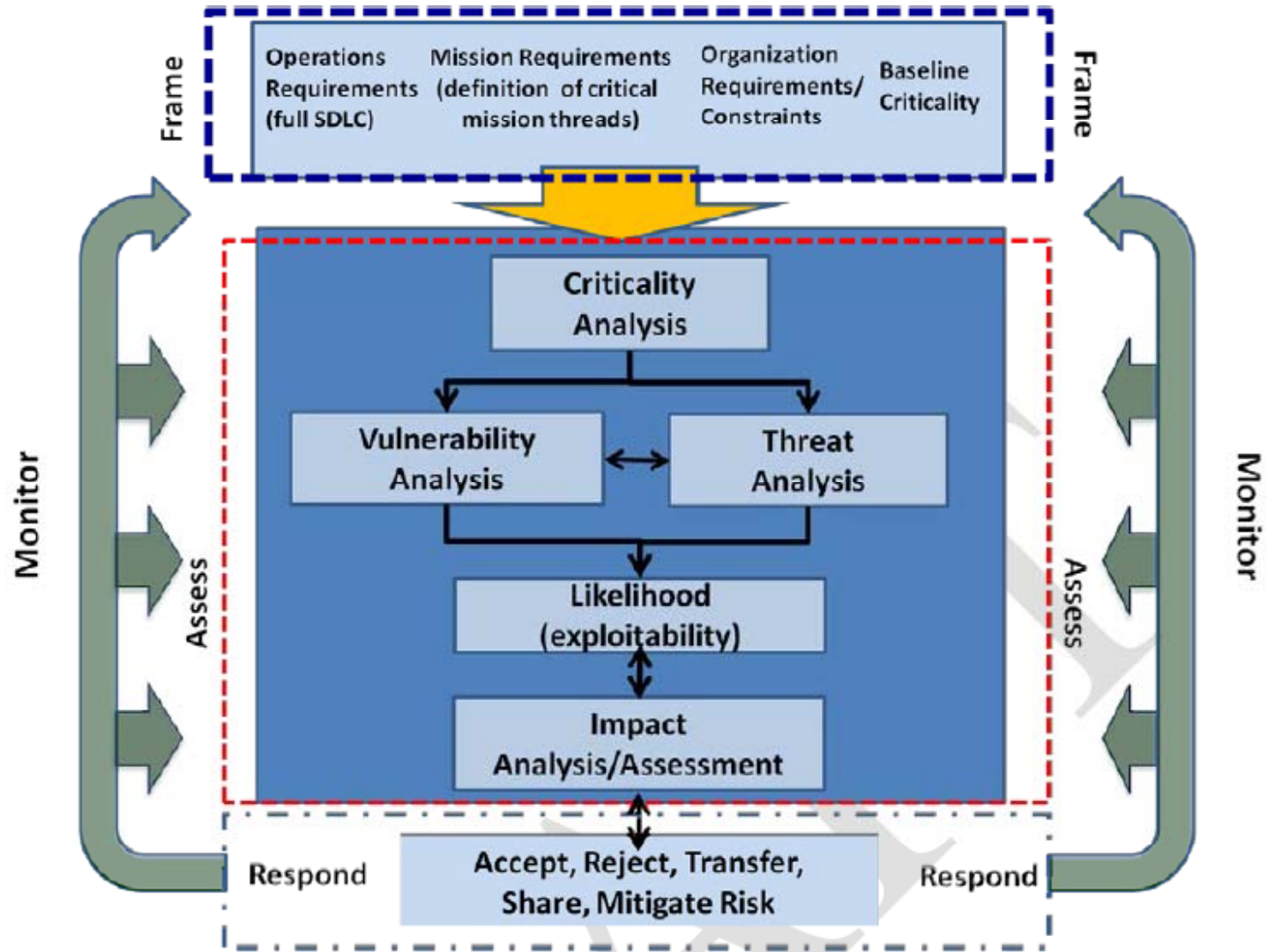
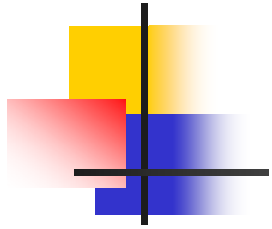
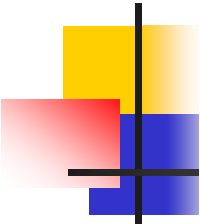


Figure 2-4. ICT SCRM Risk Assessment



Frame Step

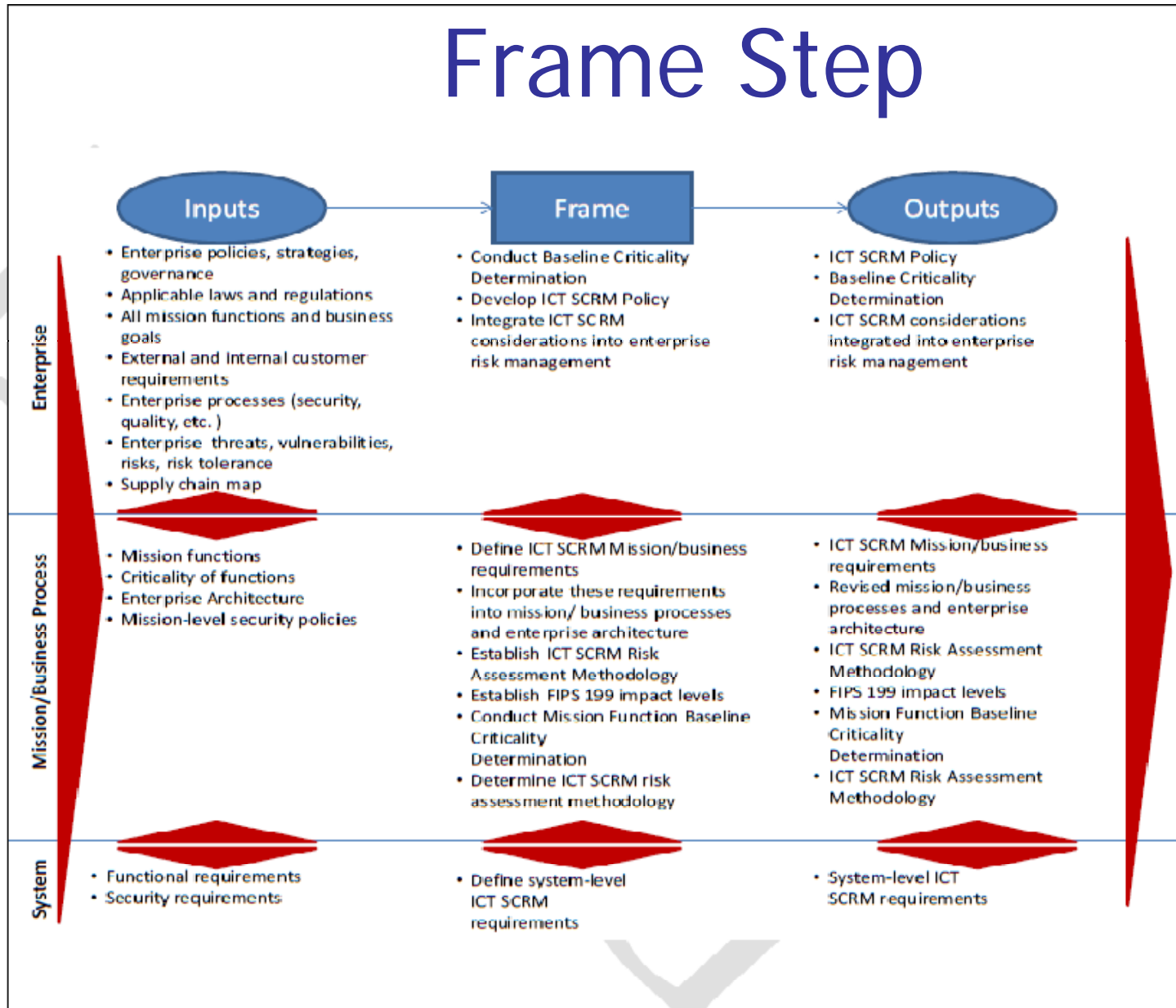


Figure 2-5. ICT SCRM in the Frame Step



Threat Agents

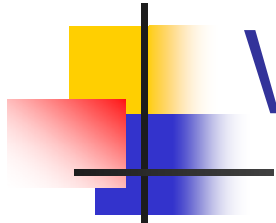
Threat Agent	Scenario	Examples
Counterfeiters	Counterfeits	Criminal groups seek to acquire and sell counterfeit ICT components for monetary gain. Specifically, organized crime groups seek disposed units, purchase overstock items, and acquire blueprints to obtain ICT components that they can sell through various gray market resellers to acquirers. ¹¹
Insiders	Intellectual property loss	Disgruntled insiders sell or transfer intellectual property to competitors or foreign intelligence agencies for a variety of reasons including monetary gain. Intellectual property includes software code, blueprints, or documentation. ¹²
Foreign Intelligence Services	Malicious code insertion (see Appendix F Scenario 3)	Foreign intelligence services seek to penetrate ICT supply chain and implant unwanted functionality (by inserting new or modifying existing functionality) to be used when the system is operational to gather information or subvert system or mission operations.
Terrorists	Unauthorized access	Terrorists seek to penetrate ICT supply chain and may implant unwanted functionality (by inserting new or modifying existing functionality) or subvert system or mission operations.
Industrial Espionage	Industrial Espionage (see Appendix F Scenario 2)	Industrial spies seek to penetrate ICT supply chain to gather information or subvert system or mission operations.



Threat Considerations

Table 2-5. Supply Chain Threat Considerations

Tier	Threat Consideration	Methods
Tier 1	<ul style="list-style-type: none"> • Organization's business and mission • Strategic supplier relationships • Geographical considerations related to the extent of the organization's ICT supply chain 	<ul style="list-style-type: none"> • Establish common starting points for identifying ICT supply chain threat. • Establish procedures for countering organization-wide threats such as natural disasters.
Tier 2	<ul style="list-style-type: none"> • Mission functions • Geographic locations • Types of suppliers (COTS, external service providers, or custom, etc.) • Technologies used enterprise-wide 	<ul style="list-style-type: none"> • Identify additional sources of threat information specific to organizational mission functions. • Identify potential threat sources based on the locations and suppliers identified through examining the agency supply chain map.
		<ul style="list-style-type: none"> • Scope identified threat sources to the specific mission functions, using the supply chain maps. • Establish mission-specific preparatory procedures for countering threat adversaries/natural disasters.
Tier 3	<ul style="list-style-type: none"> • SDLC 	<ul style="list-style-type: none"> • Consider the phase in the system development life cycle to determine the level of detail with which threats should be considered. • Identify and refine threat sources based on the potential for threat insertion within individual SDLC processes.



Vulnerability

Table 2-6. Supply Chain Vulnerabilities Considerations

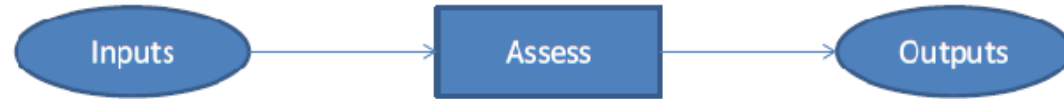
Tier	Vulnerability Consideration	Methods
Tier 1	<ul style="list-style-type: none"> • Organization's business and mission • Supplier relationships (e.g., system integrators, COTS, external services) • Geographical considerations related to the extent of the organization's ICT supply chain <ul style="list-style-type: none"> • Enterprise / Security Architecture • Criticality Baseline 	<ul style="list-style-type: none"> • Examine agency Supply Chain Maps and/or historical data to identify especially vulnerable locations or organizations. • Analyze agency mission for susceptibility to potential supply chain vulnerabilities. • Examine system integrator and supplier relationships for susceptibility to potential supply chain vulnerabilities. • Review enterprise architecture and criticality baseline to identify areas of weakness requiring more robust ICT supply chain considerations.
Tier 2	<ul style="list-style-type: none"> • Mission functions • Geographic locations • Types of suppliers (COTS, custom, etc.) • Technologies used 	<ul style="list-style-type: none"> • Refine analysis from Tier 1 based on specific mission functions and applicable threat and supply chain information. • Consider using CVEs to characterize and categorize vulnerabilities. • Consider using scoring guidance to prioritize vulnerabilities for remediation.
Tier 3	<ul style="list-style-type: none"> • Individual technologies, solutions, and suppliers should be considered 	<ul style="list-style-type: none"> • Use CVEs where available to characterize and categorize vulnerabilities • Identify weaknesses



Consequences of SC threats

- Examples of SC Consequences and Impact:
 - An earthquake in Malaysia reduced the number of commodity DRAMs to 60% of the world's supply, creating a shortage for hardware maintenance and new design.
 - Accidental procurement of a counterfeit part resulted in premature component failure, therefore impacting organization's mission performance.

Assess Step



Enterprise

- ICT SCRM Policy
- Baseline Criticality Determination

- Integrate ICT SCRM considerations into enterprise risk management

- ICT SCRM considerations integrated into enterprise risk management

Mission/Business Process

- ICT SCRM Mission/business requirements
- Revised mission/business processes and enterprise architecture
- ICT SCRM Risk Assessment Methodology
- FIPS 199 impact levels
- Mission Function Baseline Criticality Determination
- ICT SCRM Risk Assessment Methodology

- Conduct Risk Assessment including Criticality Analysis for mission threads
- Determine current risk posture

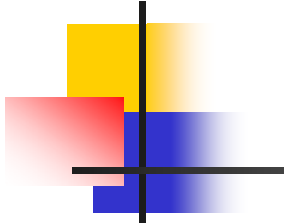
- Mission function criticality
- Mission risks
- ICT supply chain risk assessment for mission threads

System

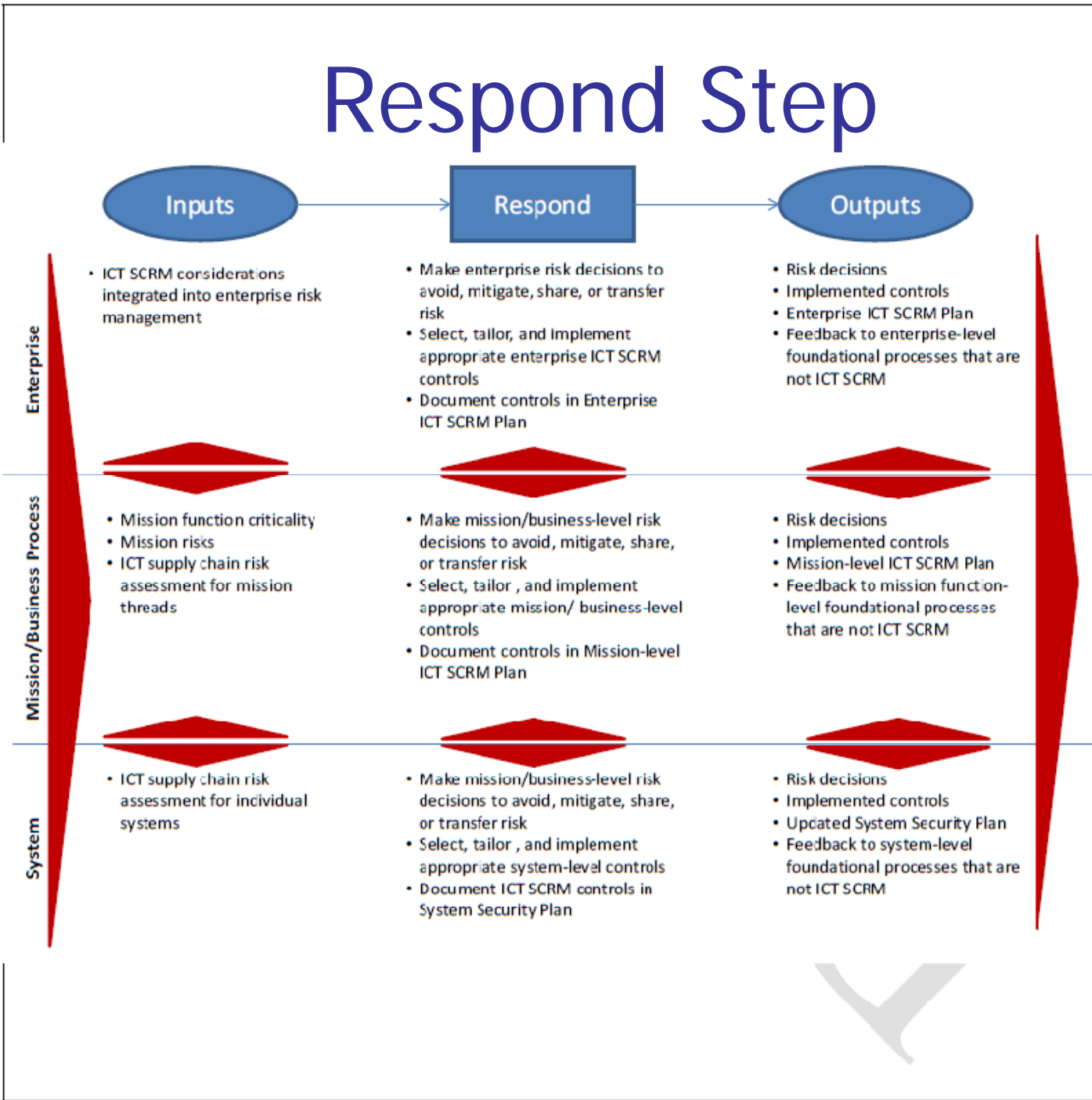
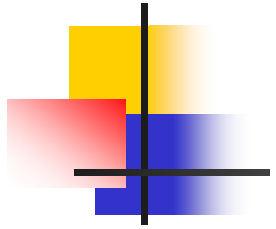
- System-level ICT SCRM requirements

- Conduct ICT SCRM Risk Assessment including Criticality Analysis for individual systems
- Determine current risk posture

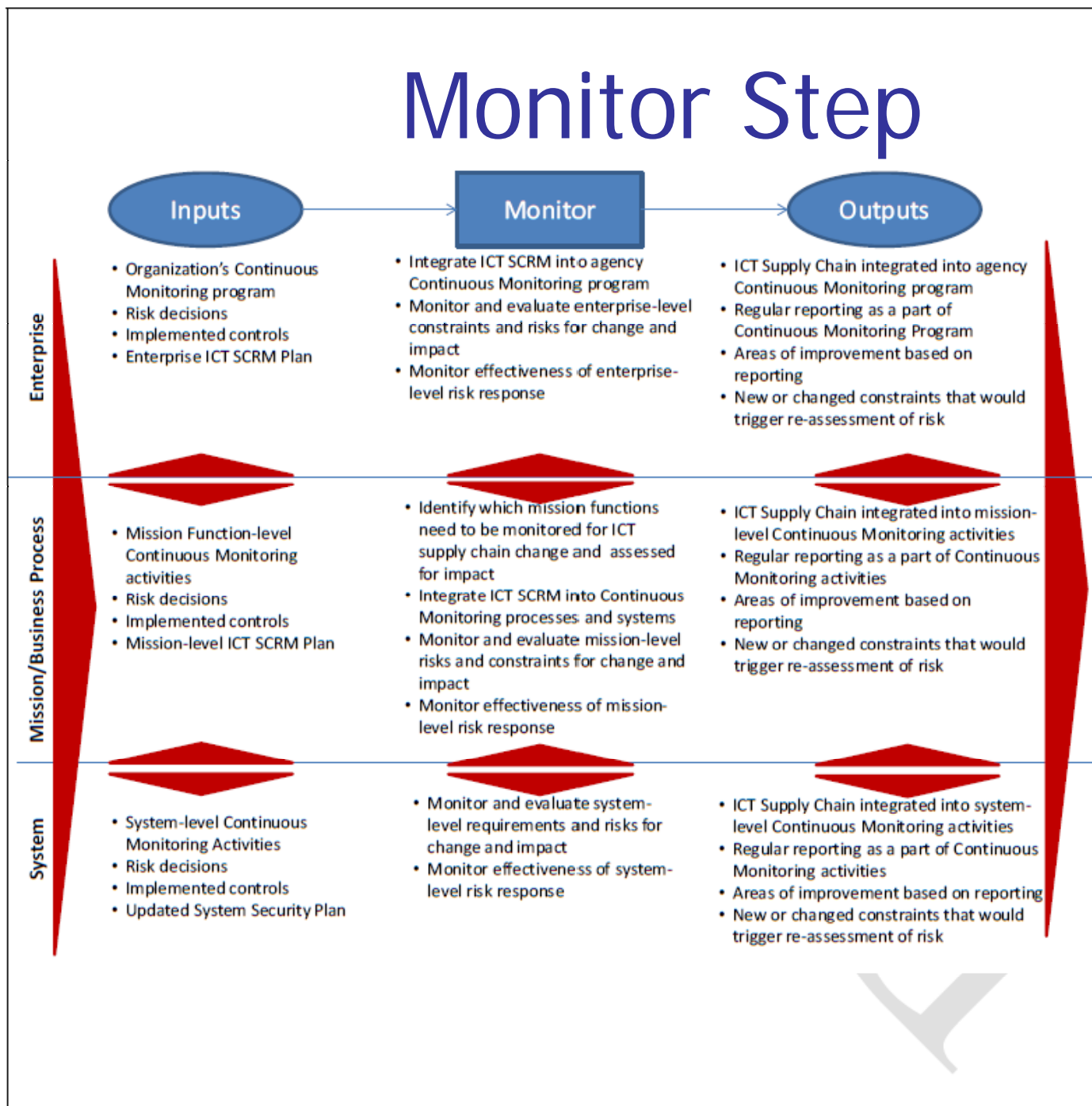
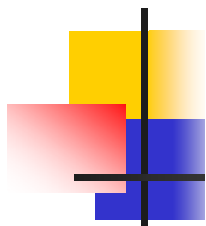
- ICT supply chain risk assessment for individual systems



Respond Step



Monitor Step





SC Environment

- System Integrators
 - organizations that provide customized services to an acquirer - custom development, test, and operations and maintenance; may include many suppliers
- Suppliers
 - organizations providing commercial off-the-shelf (COTS) to an acquirer

External Providers of InfoSys Services

- Outsourcing IT services –
- Visibility and control of functionality and security controls are critical