



# **Mature and Secure: Creating a CMMI<sup>®</sup> and ISO/IEC 21827 Compliant Process Improvement Program**

Herndon, VA  
March 29, 2006

# Security needs are continuously evolving, which makes security implementation increasingly challenging

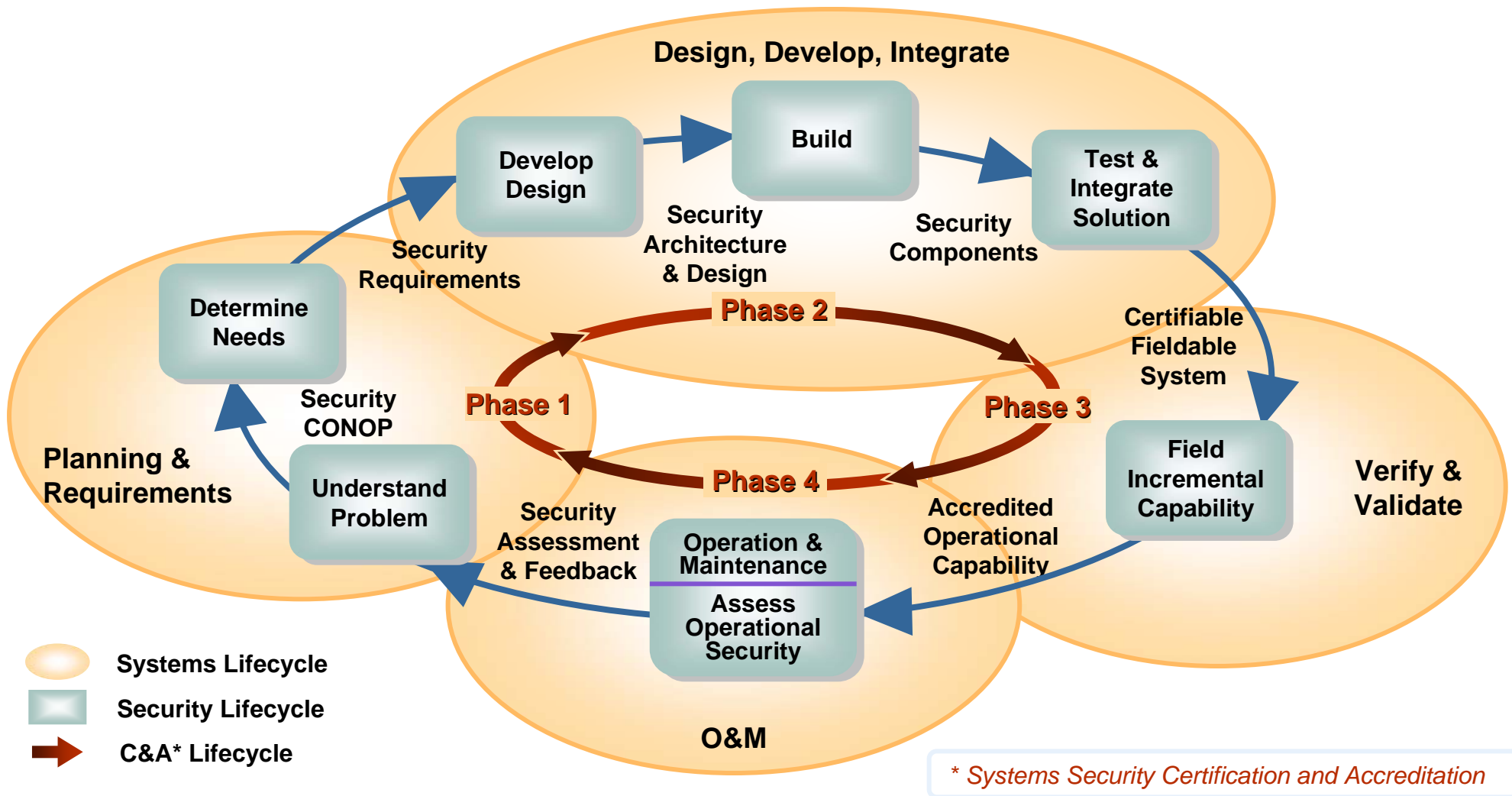
- ▶ Global interconnection
- ▶ Massive complexity
- ▶ Release of beta versions of software
- ▶ Evolutionary development



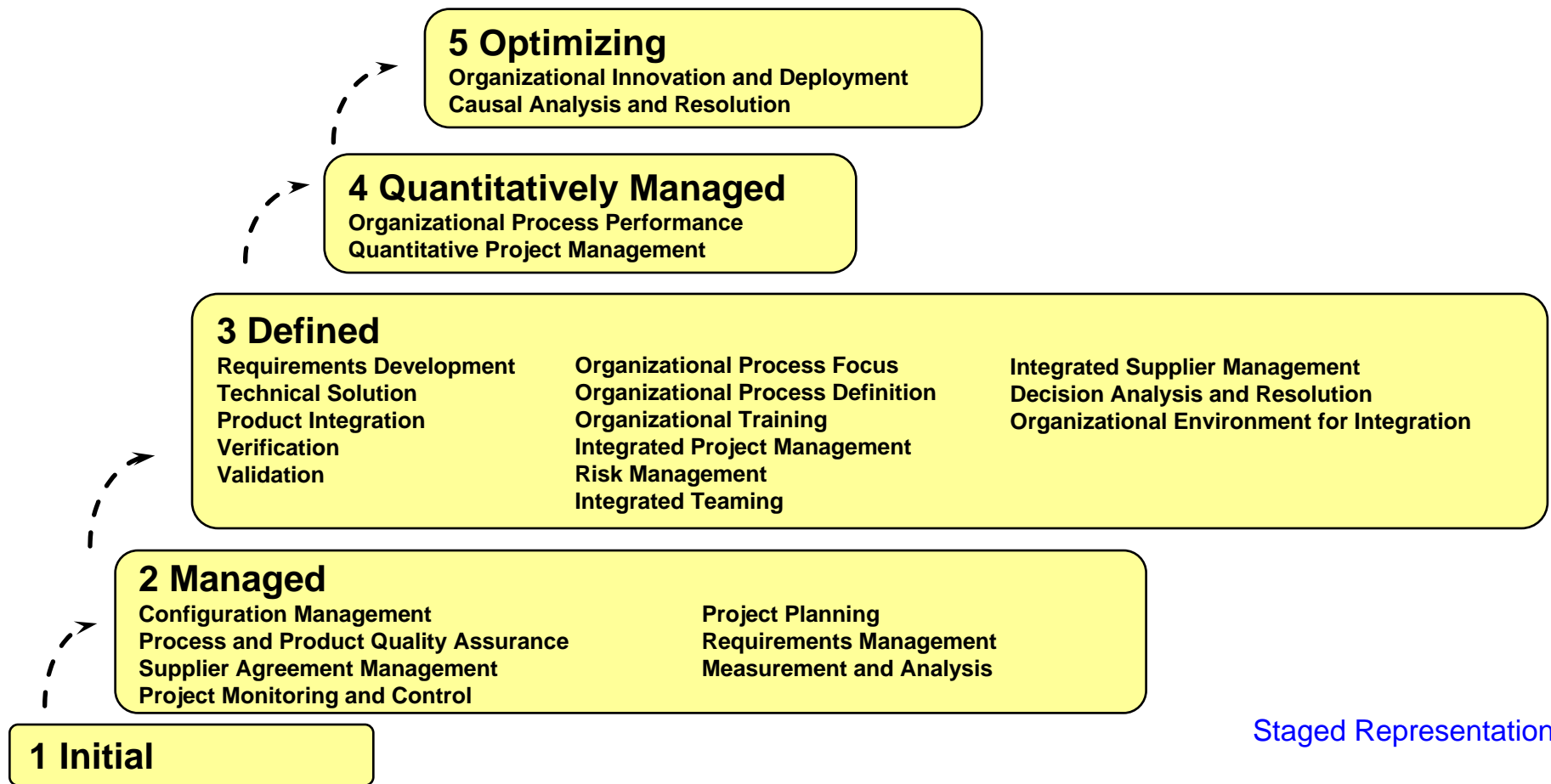
# Business drivers help shape the integration of security into our systems/software efforts

- ▶ **Headline News**
  - Microsoft: "Code Red" Worm
  - Air Force: "Hacker Steals Air Force Officer's Personal Information"
- ▶ **Legislation**
  - e-Gov Act
  - OMB A-11 Exhibit 300 Section II. B
  - FISMA
- ▶ **Market recognition**
  - Assurance that security is appropriately addressed
  - Security implementation should be transparent
  - Well-defined, repeatable processes will allow duplication of successful efforts
  - Understanding our strengths and weaknesses will allow us to become more efficient in our delivery

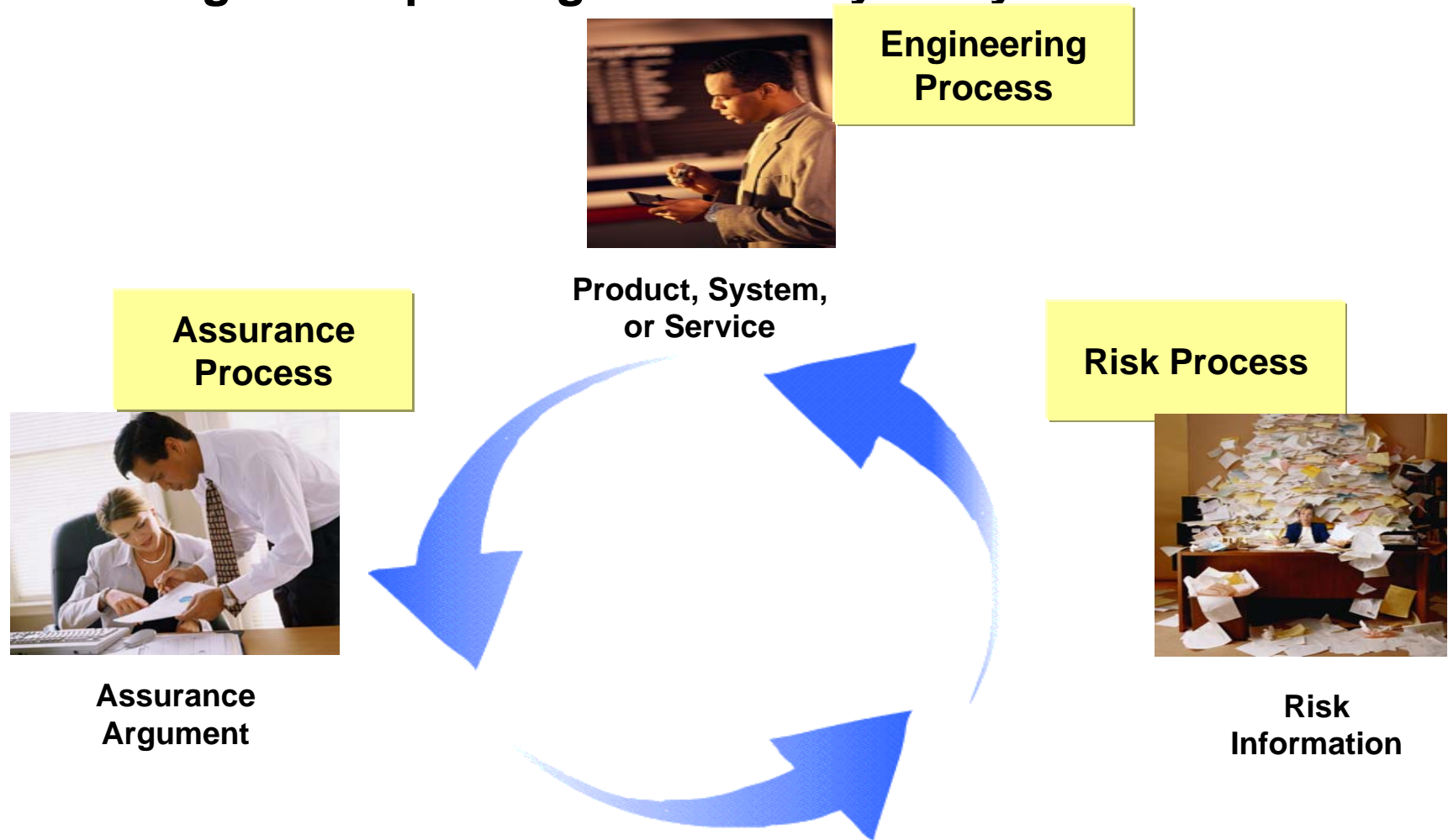
# Integrating security engineering into the systems engineering lifecycle enables successful information assurance implementation



# The CMMI is an existing business requirement that provides guidance for defining, implementing and improving the systems lifecycle

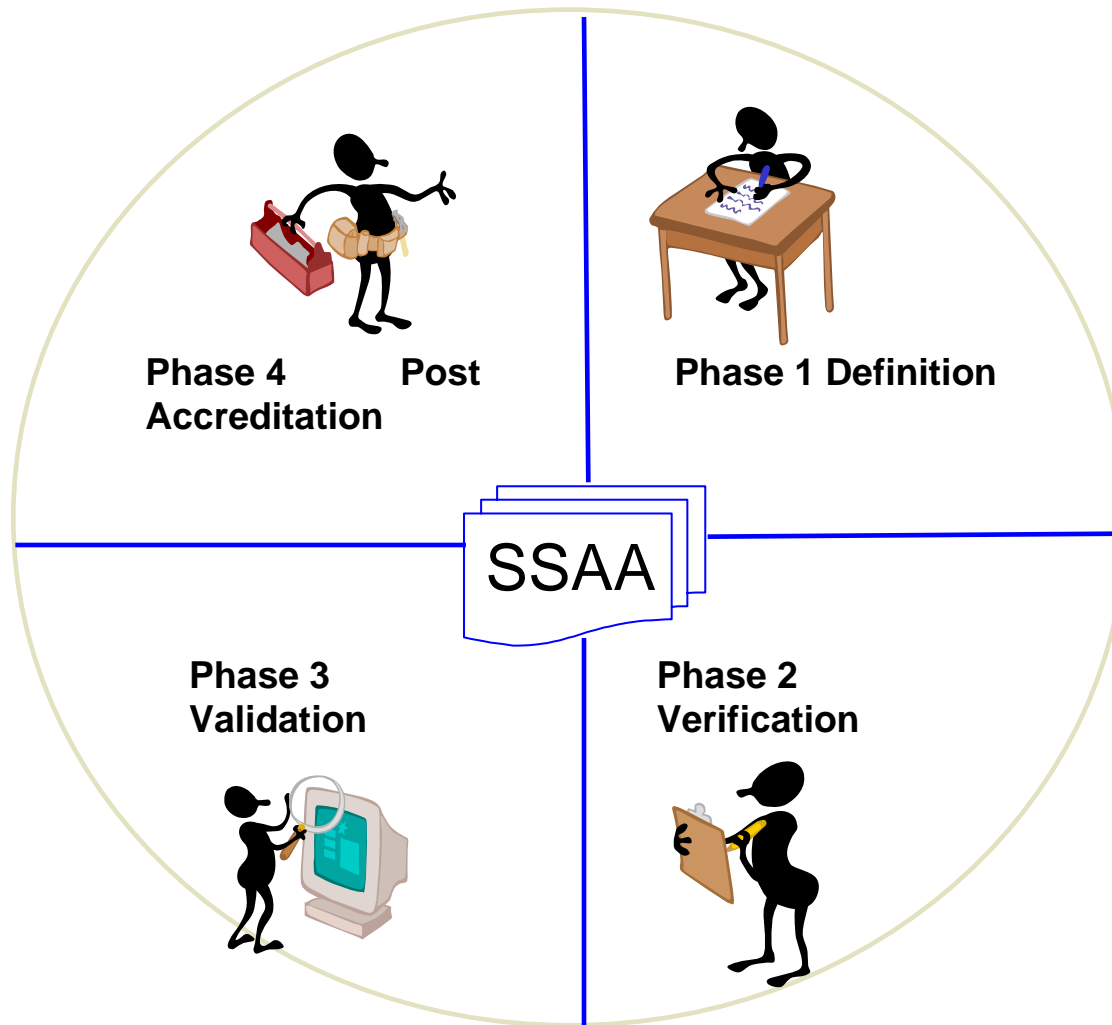


# The ISO 21827 SSE-CMM\* provides guidance for defining, implementing and improving the security lifecycle

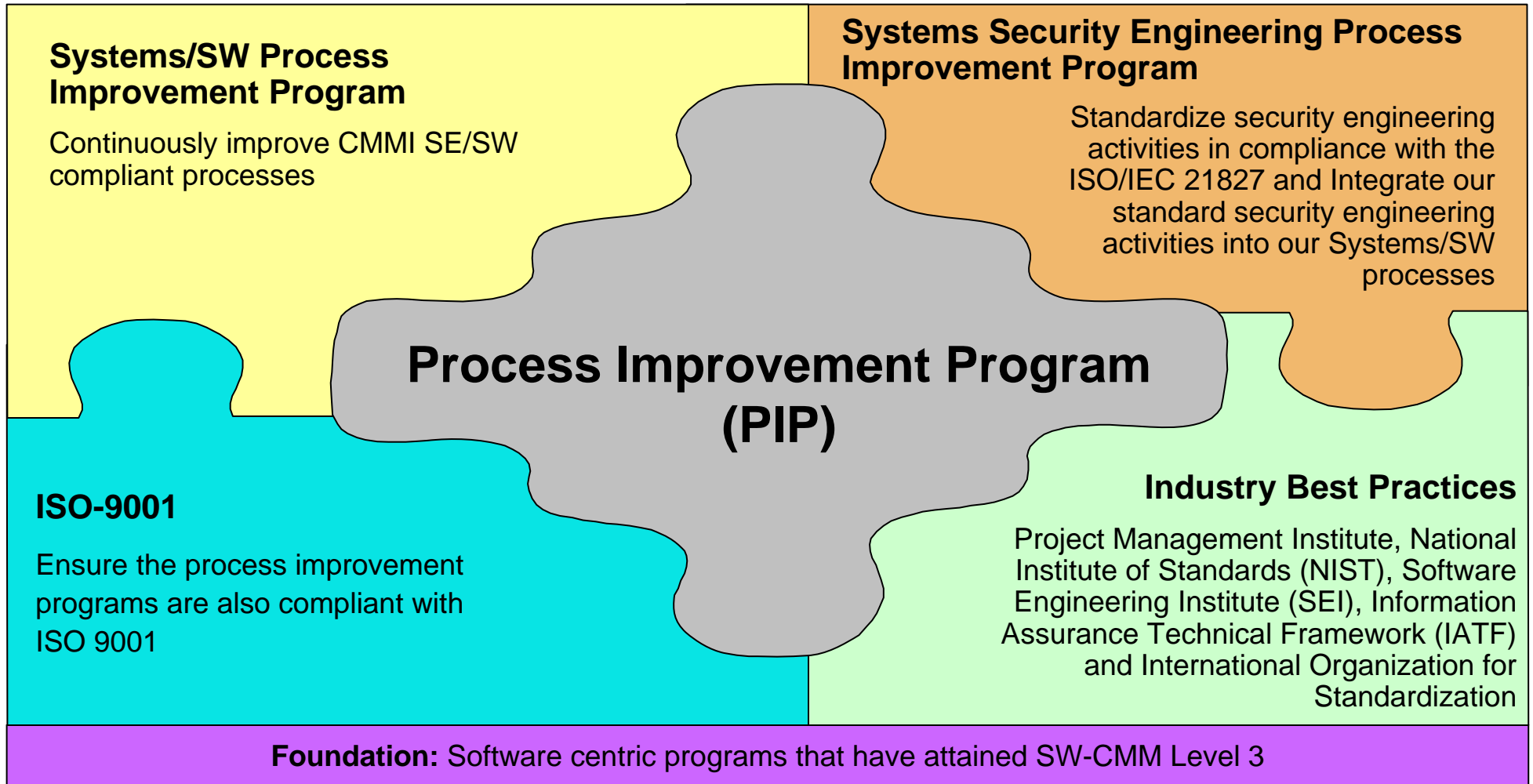


\* Systems Security Engineering Capability Maturity Model

# DITSCAP/NIST SP 800-37 define the certification and accreditation lifecycle



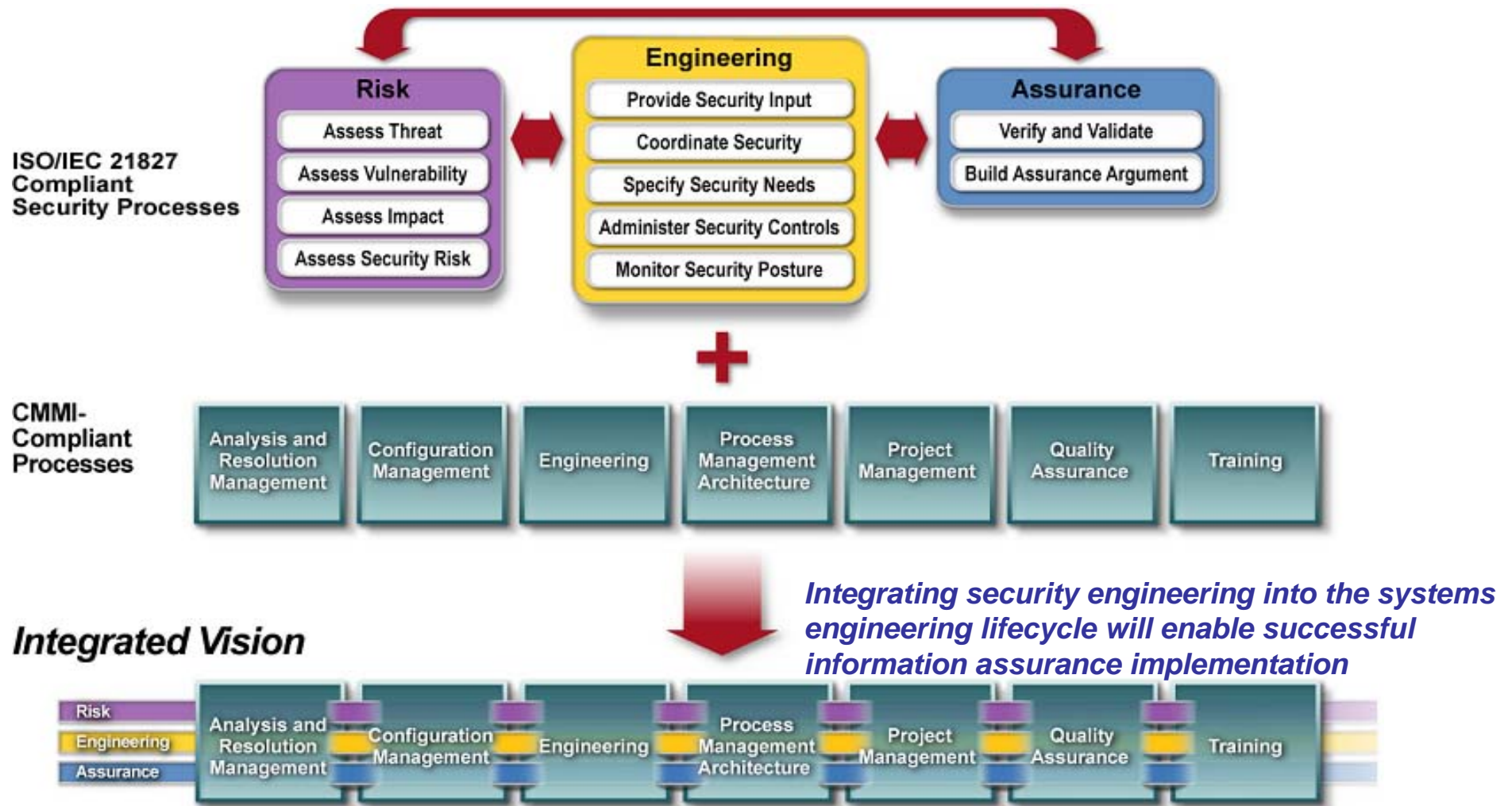
# Organizational Standard Processes leverage industry standards that support diverse clients



**CMMI = Capability Maturity Model Integration**  
**ISO = International Organization for Standardization**



# Our CMMI approach integrated security engineering processes with our systems/software processes



# Profile of Staged and Continuous Models

Maturity Levels	
Level 5	
Level 4	
Level 3	█
Level 2	█
Level 1	█
Process Areas	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22
	Security Engineering Process Areas      Project and Organizational Process Areas

## ▶ Staged Model

- ALL process areas must be at the same level before the organization can advance to the next level of maturity

Capability Levels	
Level 5	
Level 4	
Level 3	█
Level 2	█
Level 1	█
Process Areas	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22
	Security Engineering Process Areas      Project and Organizational Process Areas

## ▶ Continuous Model

- Organization can apply focus and assets against those process areas considered most essential to the business and mission. Capability level can vary from one PA to another.

# Sample Profile for a Security Product Developer

- ▶ For a security product developer, the process areas related to product development activities might target a higher level of maturity.

Capability Levels																						
Level 5																						
Level 4																						
Level 3																						
Level 2																						
Level 1																						
Process Areas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
		Security Engineering Process Areas										Project and Organizational Process Areas										

# Sample Profile for a Systems Integrator

- ▶ In this case, the highest level of maturity is required in those process areas that contribute most significantly to fulfilling the customers expectations.

Capability Levels																						
Level 5																						
Level 4			█			█									█	█						
Level 3	█		█		█	█				█	█		█	█	█	█	█		█		█	
Level 2	█	█	█		█	█	█	█	█	█	█	█	█	█	█	█		█	█	█		
Level 1	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█		█	█	█	█	
Process Areas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
		Security Engineering Process Areas										Project and Organizational Process Areas										

# CMMI processes provided the foundation for implementation of security practices

CMMI	ISO/IEC 21827 SSE-CMM
Org Process Focus (L3) Org Process Definition (L3) Org Process Performance (L4) Org Innovation and Deployment (L5)	Define Organization's Systems Security Engineering Process Improve Organization's Systems Security Engineering Process Manage Systems Engineering Support Environment Manage Product Line Evolution
Organizational Training (L3)	Provide Ongoing Skills and Knowledge
Project Planning (L2) Project Monitoring and Control (L2) Supplier Agreement Management (L2) Integrated Project Management (L3) Risk Management (L3) Quantitative Project Management (L4)	Plan Technical Effort Monitor and Control Technical Effort Coordinate with Suppliers <a href="#">Coordinate Security</a> Manage Project Risk <a href="#">Build Assurance Argument</a>
Requirements Management (L2) Requirements Development (L3) Technical Solution (L3) Product Integration (L3) Verification (L3) Validation (L3)	<a href="#">Specify Security Needs</a> <a href="#">Provide Security Input</a> <a href="#">Verify and Validate Security</a> <a href="#">Administer Security Controls</a> <a href="#">Assess Impact</a> <a href="#">Assess Security Risk</a> <a href="#">Assess Threat</a> <a href="#">Assess Vulnerability</a> <a href="#">Monitor Security Posture</a>
Configuration Management (L2)	Manage Configurations
Process & Product Quality Assurance (L2)	Ensure Quality
Measurement and Analysis (L2) Decision Analysis and Resolution (L3) Causal Analysis and Resolution (L5)	

## An integrated team advocates process implementation

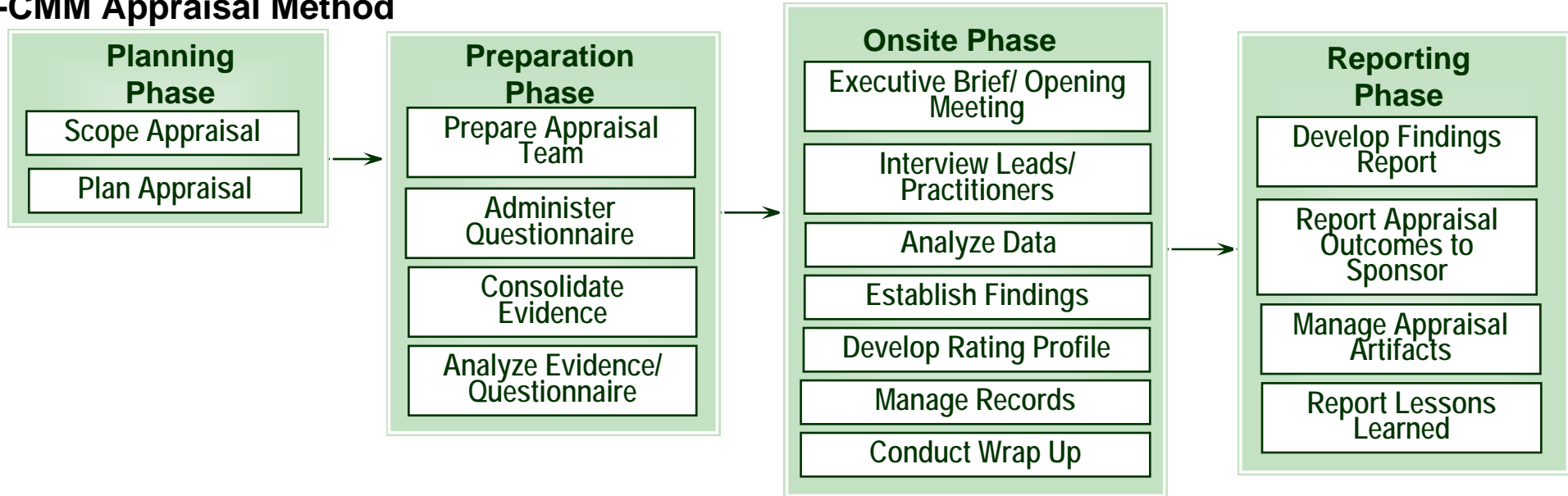
- ▶ Appraisers
  - Role: Provide CMMI model and OSP subject matter expertise
- ▶ Process Engineers
  - Role: Mentor and assist project personnel in implementing project processes
- ▶ Security Process Engineers
  - Role: Provide SME support and guidance for security process implementation

## Example metrics to determine if you are effectively incorporating security early in the SDLC

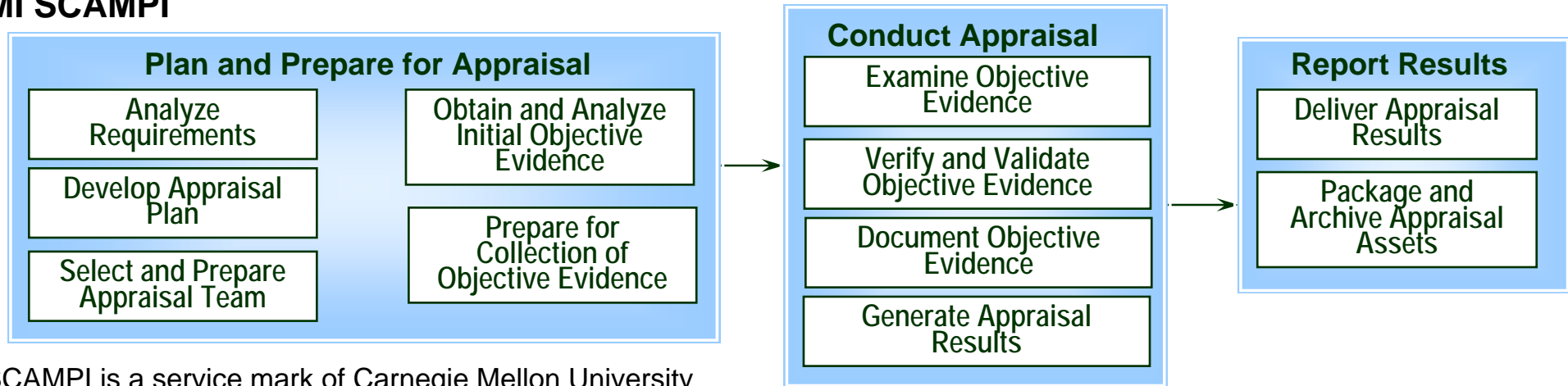
- ▶ Are we identifying IA requirements early in the lifecycle?
  - #/% of authorized changes that impact security, during each phase of SDLC
  - #/% of security requirements (per design specification) implemented
  - #/% of vulnerabilities discovered during testing that require mitigation
  - Cost of implementing/ integrating new/additional requirements
  - % of Security/IA system functions performing as designed
- ▶ Do we have adequate FTEs allocated?
  - # of Security/IA FTEs allocated to current system development project
  - % of budget allocated to current phase for Security/IA activities
  - # of days required to gain concurrence from Security Stakeholders regarding security requirements

# The SCAMPI and ISO/IEC 21827 Appraisal Method have similar steps

## SSE-CMM Appraisal Method



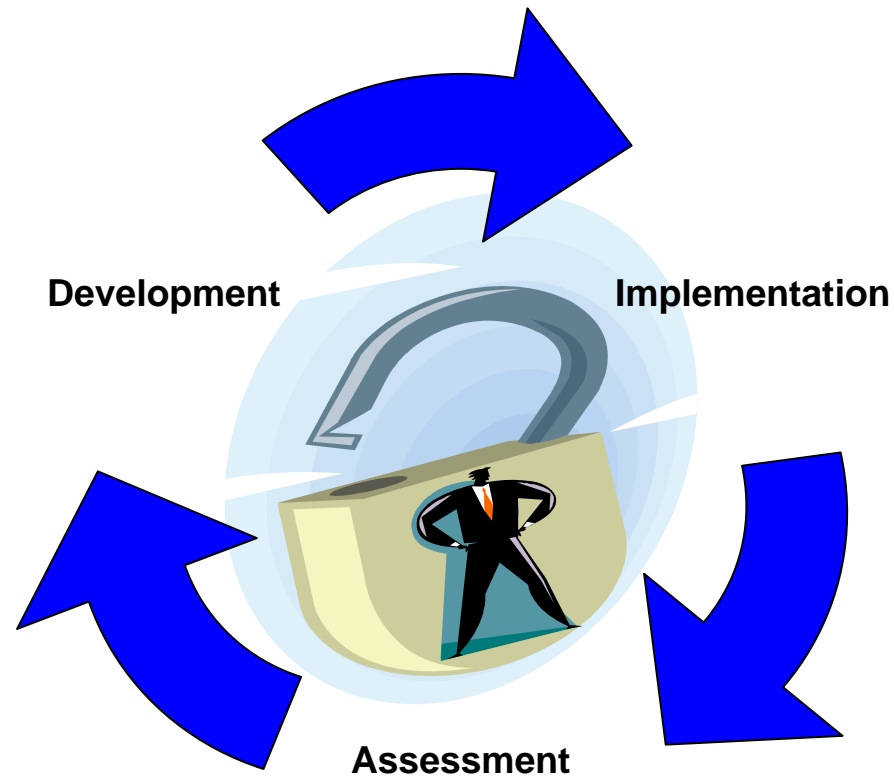
## CMMI SCAMPI



SM SCAMPI is a service mark of Carnegie Mellon University



# Integrating security into a Process Improvement Program results in increased assurance and transparency of security implementation



## For More Information

- ▶ ISO/IEC 21827
  - [www.sse-cmm.org](http://www.sse-cmm.org)
  - [www.issea.org](http://www.issea.org)
- ▶ CMMI
  - <http://www.sei.cmu.edu/cmmi/Information>
- ▶ Assurance
  - <http://iase.disa.mil/>
  - <http://iac.dtic.mil/iatac/>
  - <http://www.iatf.net>
  - <http://www.nist.gov>
  - <http://www.sei.cmu.edu/programs/nss/nss.html>

**Michele Moss**  
Associate

**Booz | Allen | Hamilton**

8283 Greensboro Drive  
McLean, VA 22102  
Tel (703) 377-1254  
moss\_michele@bah.com

## **Back up slides**

**DRAFT**

Booz | Allen | Hamilton


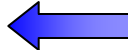
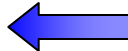
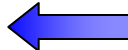
# History of ISO/IEC 21827

- ▶ 1993 NSA initiated funding for development of a CMM for security engineering
- ▶ 1995 Working groups established to develop the SSE-CMM
- ▶ 1996 SSE-CMM v1.0 published
- ▶ 1996-98 SSE-CMM piloted in 7 organizations
- ▶ 1999 SSE-CMM v2.0 published

The International System Security Engineering Association (ISSEA) was established as a non-profit professional membership organization to be a liaison with ISO for standardization, model maintenance, and appraiser certification

- ▶ 2002 SSE-CMM approved as ISO/IEC 21827
- ▶ 2004-05 ISSEA submitting application for approval as ISO/IEC 21827 Appraiser Certification Body under ISO/IEC 17024, *General Requirements For Bodies Operating Certification Schemes For Persons*

# The ISO 21827 facilitates achieving several of security engineering goals

- ▶ Tool for provider organizations to evaluate their security practices and focus improvements  **Process Improvement**
- ▶ Basis for evaluation of organizations (e.g., certifiers, evaluators) to establish organizational capability-based confidence in results  **Assurance**
- ▶ Mechanism to measure and monitor an organization's capability to deliver a specific security engineering capability  **Risk Management**
- ▶ Standard mechanism for customers to select appropriately qualified security engineering providers  **Capability Evaluation**

## There are 129 bases practices categorized into either Security Engineering Process Areas or Project and Organizational Process Areas

Security Engineering Process Areas	# of Base Practices	Project and Organizational Process Areas	# of Base Practices
1) Administer Security Controls	4	Ensure Quality	8
2) Assess Impact	6	Manage Configurations	5
3) Assess Security Risk	6	Manage Project Risk	6
4) Assess Threat	6	Monitor and Control Technical Effort	6
5) Assess Vulnerability	5	Plan Technical Effort	10
6) Build Assurance Argument	5	Define Organization's Security Engineering Process	4
7) Coordinate Security	4	Improve Organization's Security Engineering Process	4
8) Monitor Security Posture	7	Manage Product Line Evolution	5
9) Provide Security Input	6	Manage Systems Engineering Support Environment	7
10) Specify Security Needs	7	Provide Ongoing Skills and Knowledge	8
11) Verify and Validate Security	5	Coordinate with Suppliers	5

# Systems Security Certification & Accreditation

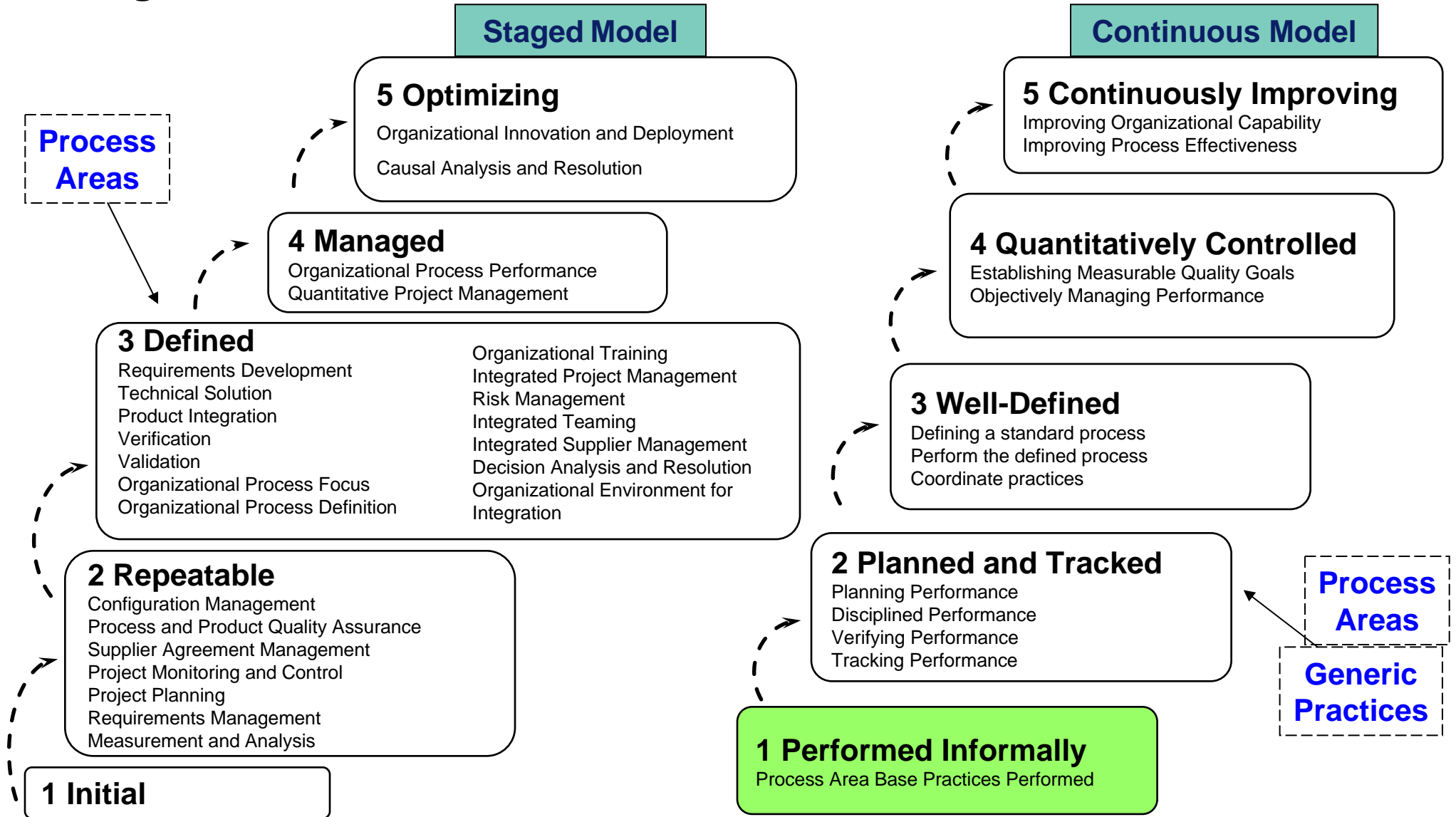
## ▶ Certification

- Provides a comprehensive **evaluation** of technical and non-technical security features of an information system
- Establishes the **extent to which** a particular design and implementation meets a set of specified security requirements
- Provides **proof** of compliance with security requirements
- **Leads** to accreditation

## ▶ Accreditation

- Formal **declaration** by the designated approving authority (DAA):
  - An information system is approved to operate in a particular security mode at an **acceptable level of risk**
  - Based on the implementation of an **approved set of** technical, managerial, and procedural **safeguards**
- Approval is granted to operate the system with the identified residual risk
- Upon accreditation, the DAA formally accepts full responsibility for the security of the system

# Staged vs. Continuous Models





## Staged and Continuous Model Comparison

Staged	Continuous
Less Flexible	More Flexible
Provides a definitive direction for improvement	Organizations can chart their own direction for improvement
Applies to only specific type of organization	Applies across all industries or types of organizations
All processes addressed at each level	