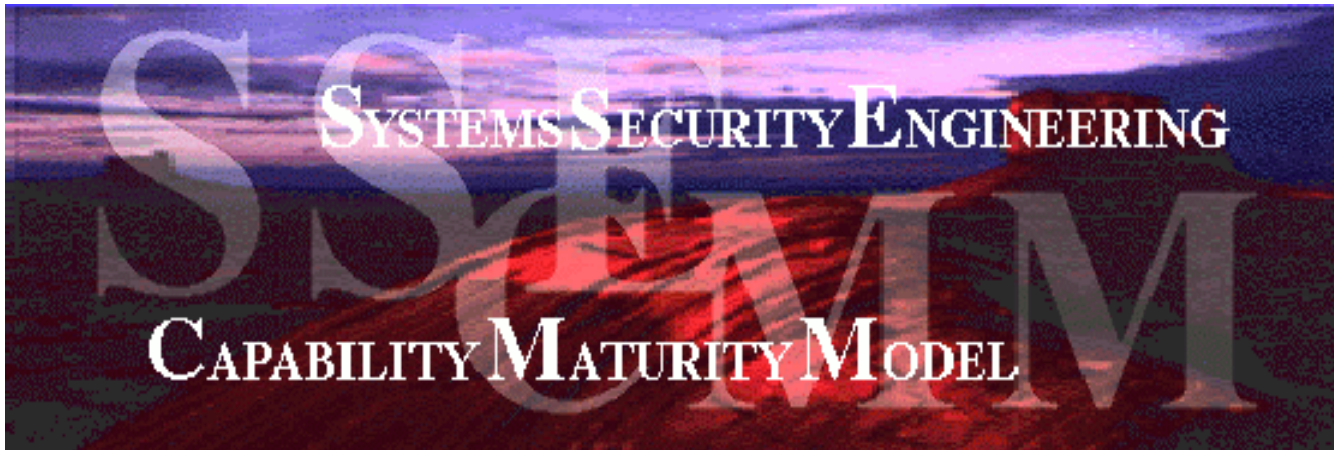


Secure and Mature: Combining a CMMI[®] SCAMPISM with an ISO/IEC 21827(SSE-CMM*) Appraisal



Karen M. Zimmie
Seattle, WA
March 8, 2004

© CMMI is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

SM SCAMPI is a service mark of Carnegie Mellon University.

* Systems Security Engineering Capability Maturity Model

Booz Allen Hamilton “Delivering Results that Endure”

International Corporate Capabilities

Founded in 1914
Privately Held
16,000+ Personnel
\$2.7 Billion Annual Sales
www.boozallen.com

Booz | Allen | Hamilton
90 years delivering results that endure

Process Consulting Capabilities

CMMI® Appraisals,
ISO 9000 Consulting,
Six Sigma, Function Points Analysis,
Work Style Preference Workshops,
Earned Value Management, Measurement Programs,
Security Processes, Rapid Assessment Method Audits
schaffer_jeff@bah.com butturff_kim@bah.com

SEISM Authorized Capabilities

Transition Partner
SCAMPISM Appraisals
Certified CMMI® Intro. Training
Process Consulting
voss_john_l@bah.com



Worldwide Technology Business Clients: Every Major USG Agency, Governments of 40 Nations, Most Prime Contractors

Worldwide Commercial Business Clients: Top 70% of Largest International Companies, 400 of *Fortune 500 Corporations*

© CMMI is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. SM SEI and SCAMPI are service marks of Carnegie Mellon University.

- ▶ 22 years information systems security experience
- ▶ B.S. Math & Computer Science
- ▶ SSE-CMM Author Group Leader
- ▶ SSE-CMM Lead Appraiser
- ▶ Participated in Systems Engineering CMM Workshops

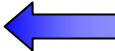
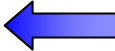
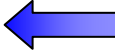
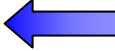
Karen M. Zimmie
Associate

Booz | Allen | Hamilton

900 Elkridge Landing Rd.
Linthicum, MD 21090
Tel (410) 684-6232
zimmie_karen@bah.com

Government and Industry collaborated to develop and promote the SSE-CMM with the goal of advancing security engineering as a mature and measurable discipline

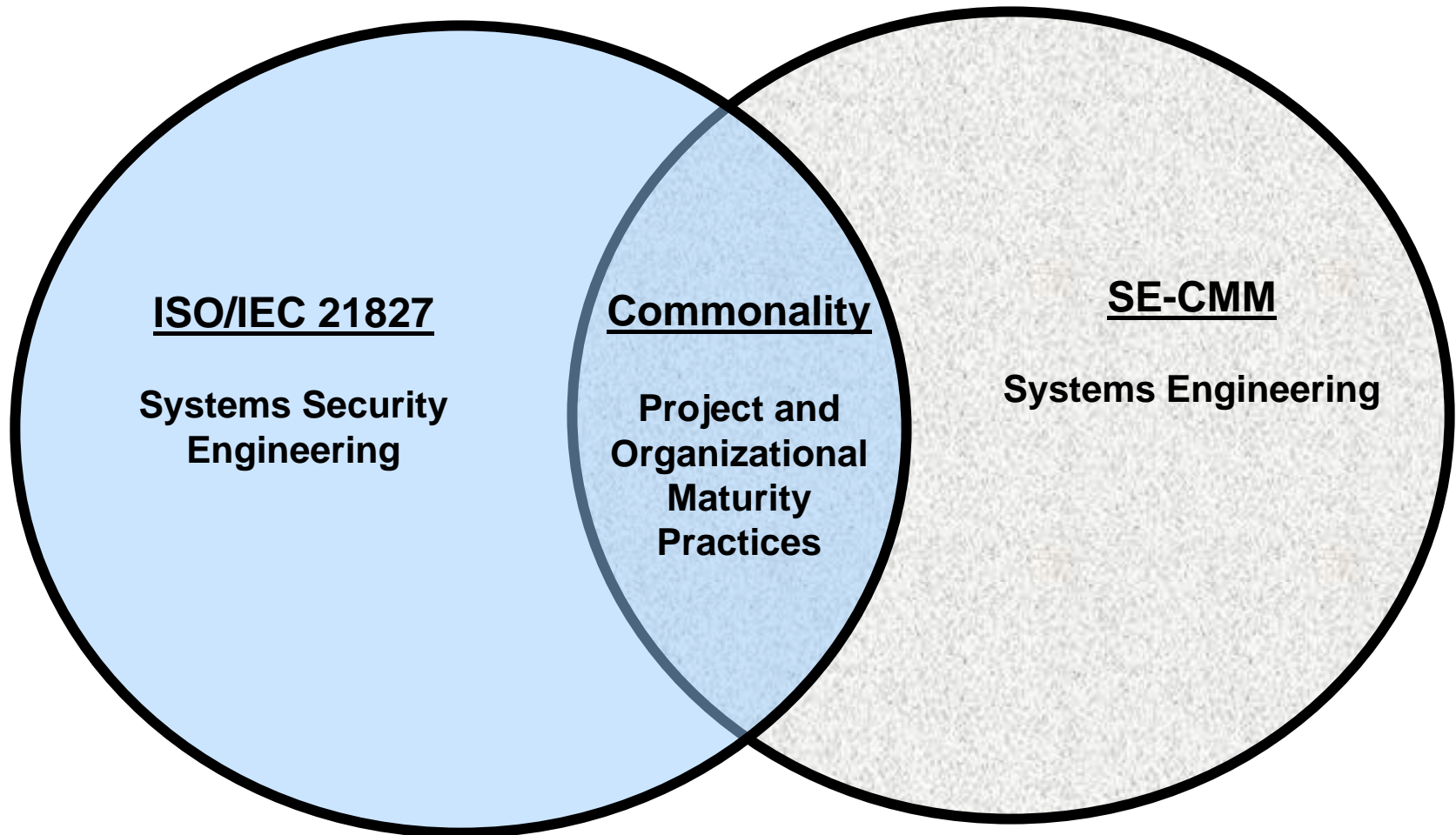
▶ The model provides a set of basic security engineering practices that can be used as a:

- Tool for provider organizations to evaluate their security practices and focus improvements  **Process Improvement**
- Standard mechanism for customers to select appropriately qualified security engineering providers  **Capability Evaluation**
- 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**

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*

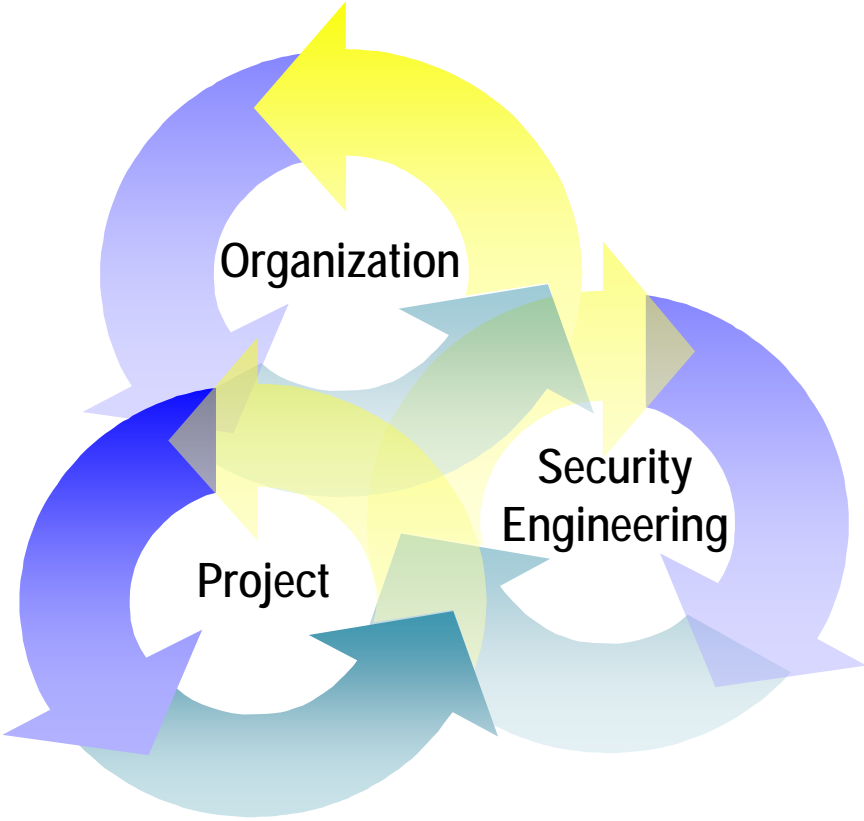
The model is based on the **Systems Engineering CMM (SE-CMM)**, adding security engineering practices to enable improvement of security specific practices



Systems Security Engineering can be described by the goals it seeks to achieve

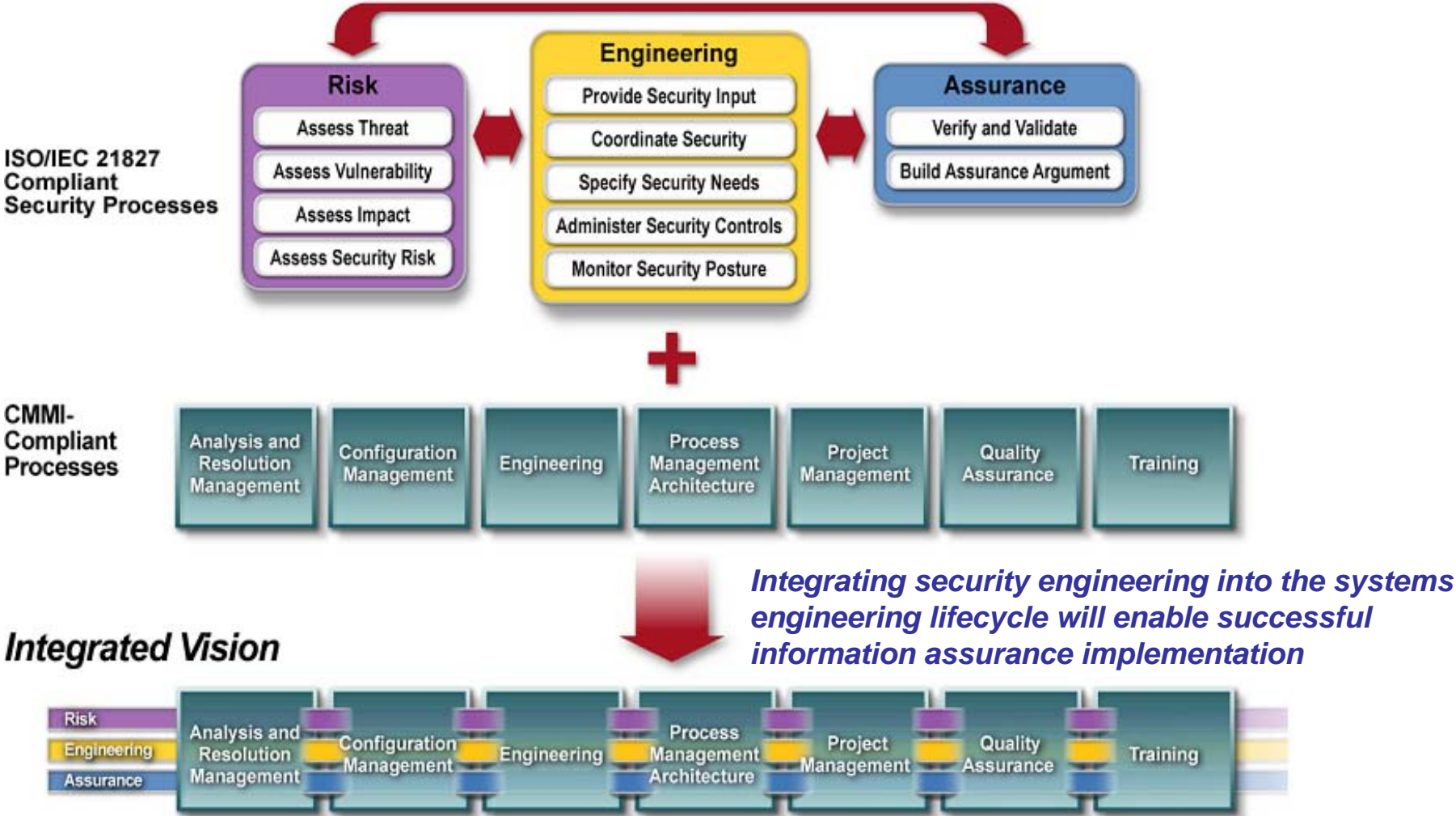
- ▶ Establish a set of security needs in accordance with the identified risks
- ▶ Translate needs to guidance and policy to be integrated into the activities of other disciplines involved in a project, and system configuration and operation descriptions
- ▶ Determine if operational impacts due to residual security vulnerabilities in a system or its operation are tolerable
- ▶ Establish confidence or assurance in the effectiveness and correctness of security mechanisms

ISO/IEC 21827 Process Areas and Capability Levels

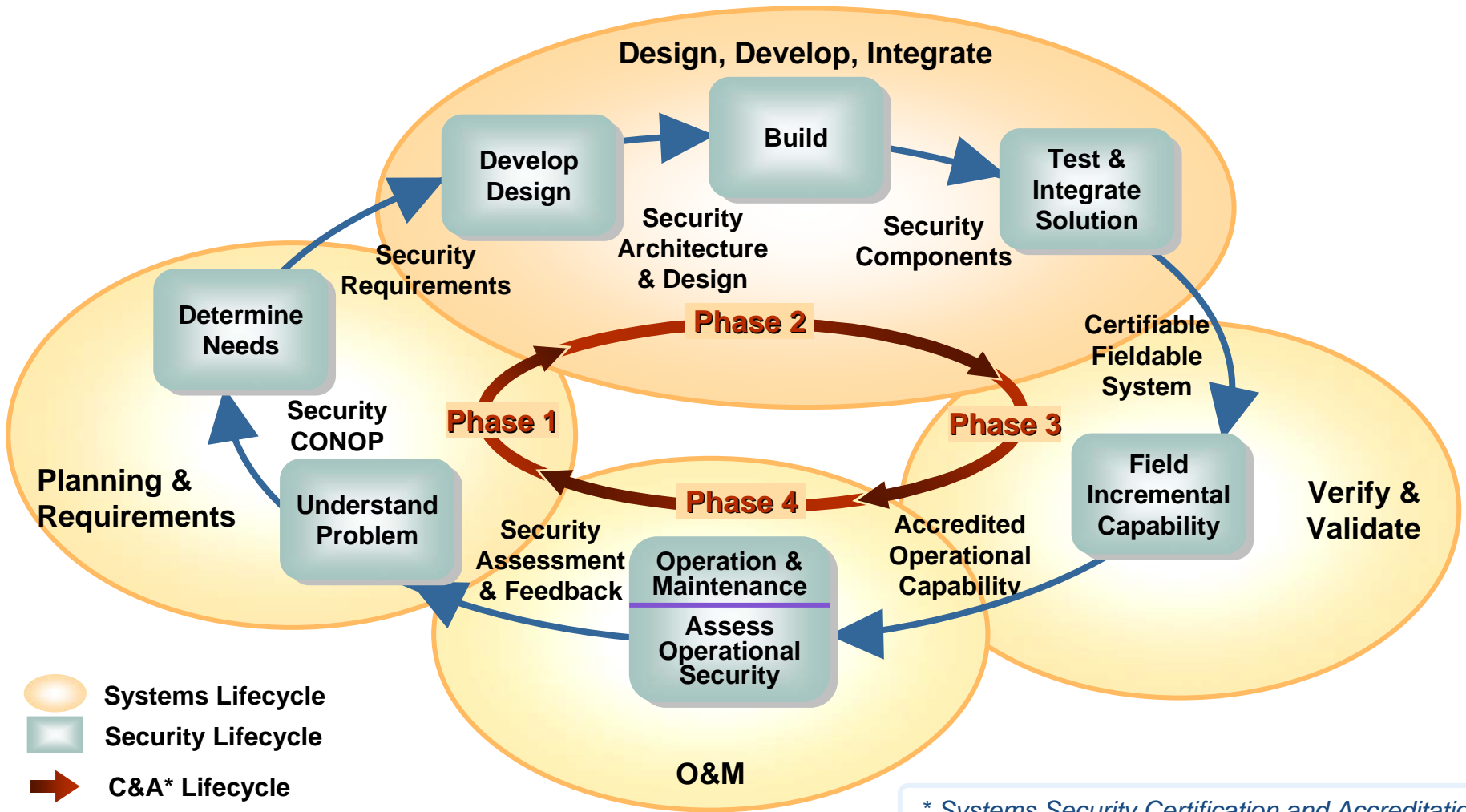


- 5 Continuously Improving**
Improving Organizational Capability
Improving Process Effectiveness
- 4 Quantitatively Controlled**
Establishing Measurable Quality Goals
Objectively Managing Performance
- 3 Well-Defined**
Defining a standard process
Perform the defined process
Coordinate practices
- 2 Planned and Tracked**
Planning Performance
Disciplined Performance
Verifying Performance
Tracking Performance
- 1 Performed Informally**
Process Area Base Practices
are Performed

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



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



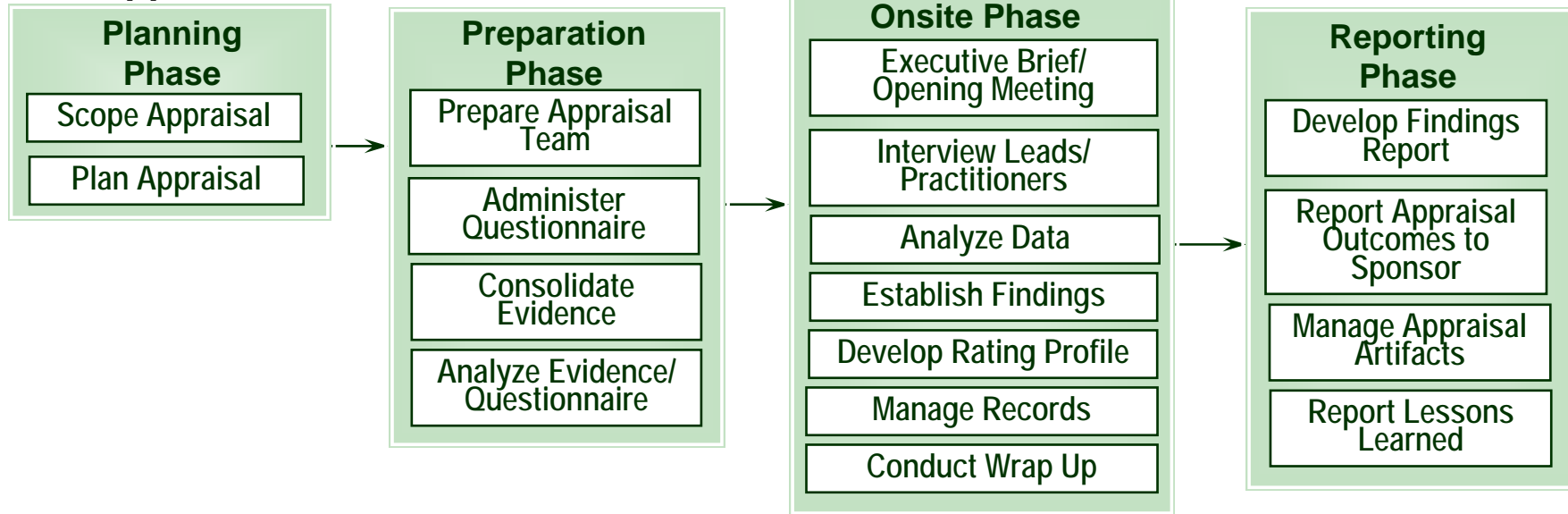
* Systems Security Certification and Accreditation

CMMI processes provided the foundation for implementation of security practices

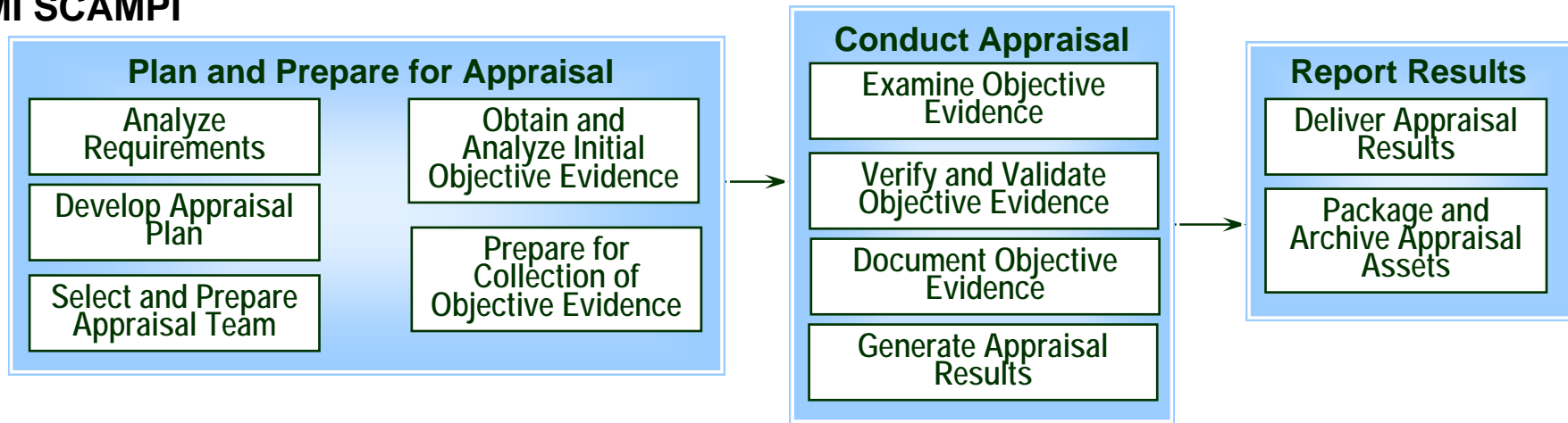
CMMI	ISO/IEC 21827 SSE-CMM
Org Process Focus (L3) Org Process Definition (L3) Org Process Performance (L4) Org Innovation and Deployment (L5)	Define Organization's Systems Security Engineering Process Improve Organization's Systems Security Engineering Process Manage Systems Engineering Support Environment 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 Coordinate Security Manage Project Risk Build Assurance Argument
Requirements Management (L2) Requirements Development (L3) Technical Solution (L3) Product Integration (L3) Verification (L3) Validation (L3)	Specify Security Needs Provide Security Input Verify and Validate Security Administer Security Controls Assess Impact Assess Security Risk Assess Threat Assess Vulnerability Monitor Security Posture
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)	

The SCAMPI and ISO/IEC 21827 Appraisal Method have basically the same steps

SSE-CMM Appraisal Method



CMMI SCAMPI



The approach to a successful combined appraisal is based on integrating ISO/IEC 21827-compliant processes with CMMI-compliant processes

- ▶ Process Development
 - Leverage the foundation of our CMMI processes
 - Security engineers and security process engineers integrate security engineering processes with systems/software processes
- ▶ Process Implementation
 - Security process engineer assigned to projects
 - Leverage infrastructure established by the CMMI program for implementation and institutionalization of security processes
- ▶ Process Assessment
 - Objective evidence can be reused where the models overlap

For More Information

▶ ISO/IEC 21827

- www.sse-cmm.org
- www.issea.org

▶ Information Assurance

- <http://iase.disa.mil/>
- <http://iac.dtic.mil/iatac/>
- <http://www.iatf.net/>
- <http://www.sei.cmu.edu/programs/nss/nss.html>

Karen M. Zimmie
Associate

Booz | Allen | Hamilton

900 Elkridge Landing Rd.
Linthicum, MD 21090
Tel (410) 684-6232
zimmie_karen@bah.com

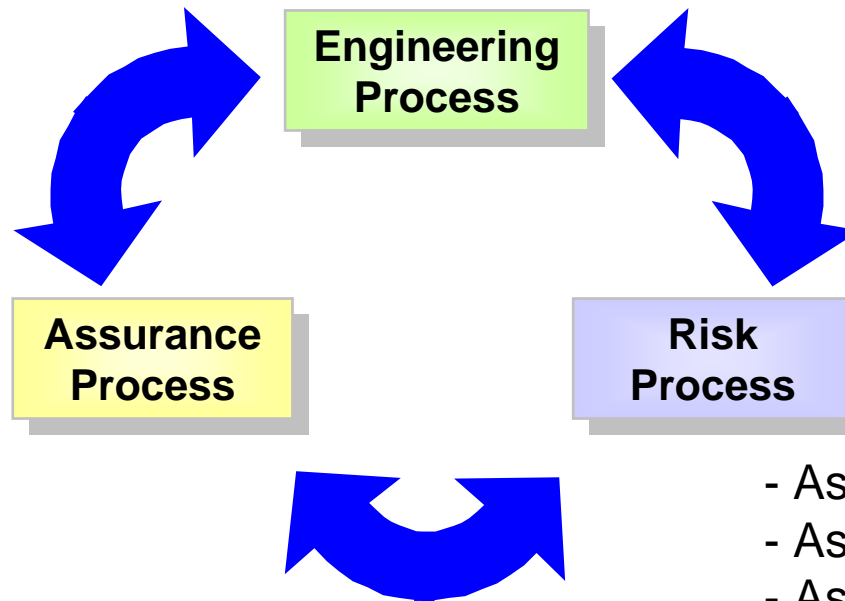
Back up slides

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

Security Engineering Process Areas

- Administer Security Controls
- Coordinate Security
- Monitor Security Posture
- Provide Security Input
- Specify Security Needs



- Build Assurance Argument
- Verify and Validate Security

- Assess Impact
- Assess Security Risk
- Assess Threat
- Assess Vulnerability

Organizational Process Areas

- ▶ Define Organization's Engineering Process
- ▶ Improve Organization's Engineering Process
- ▶ Manage Product Line Evolution
- ▶ Manage Engineering Support Environment
- ▶ Provide Ongoing Skills and Knowledge
- ▶ Coordinate with Suppliers

Project Process Areas

- ▶ Ensure Quality
- ▶ Manage Configurations
- ▶ Manage Program Risk
- ▶ Monitor and Control Technical Effort
- ▶ Plan Technical Effort

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