Mature and Secure:
Creating a CMMI® and ISO/IEC 21827 Compliant Process Improvement Program

Michele Moss
San Diego, CA
October 27, 2005
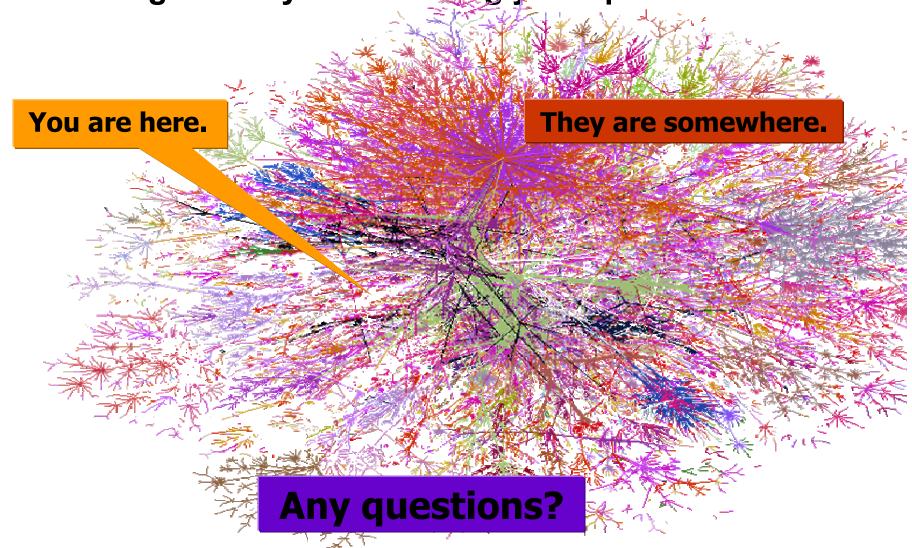
Booz | Allen | Hamilton

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

- ▶ Global interconnection

- ▶ Massive complexity

- ▶ Release of beta versions of software

- ▶ Evolutionary development

Booz | Allen | Hamilton

Addressing security is increasingly complex

You are here.

They are somewhere.

Any questions?

Booz | Allen | Hamilton

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

▶ Headline News

  – Microsoft: "Code Red" Worm

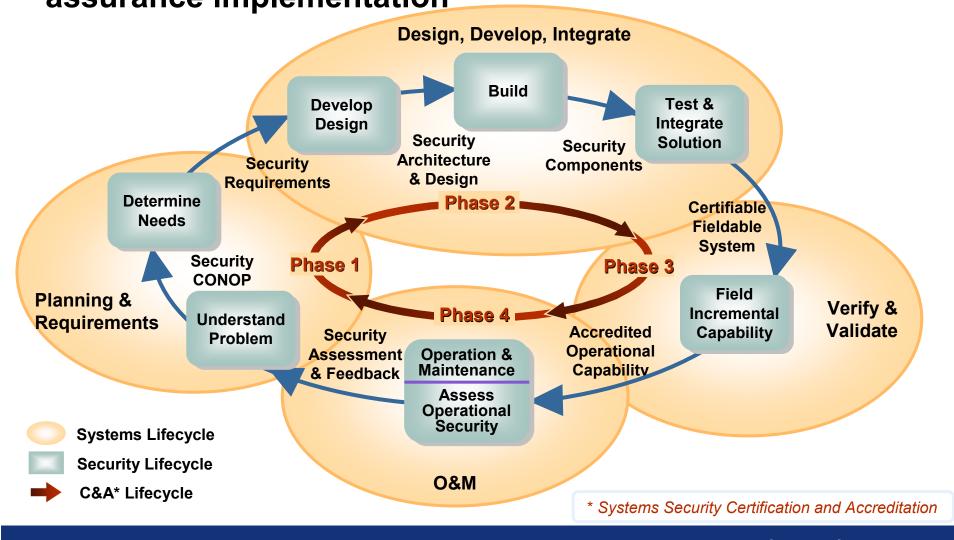 – Air Force: "Hacker Steals Air Force Officer's Personal Information"

▶ Legislation

  – e-Gov Act

  – OMB A-11 Exhibit 300 Section II. B
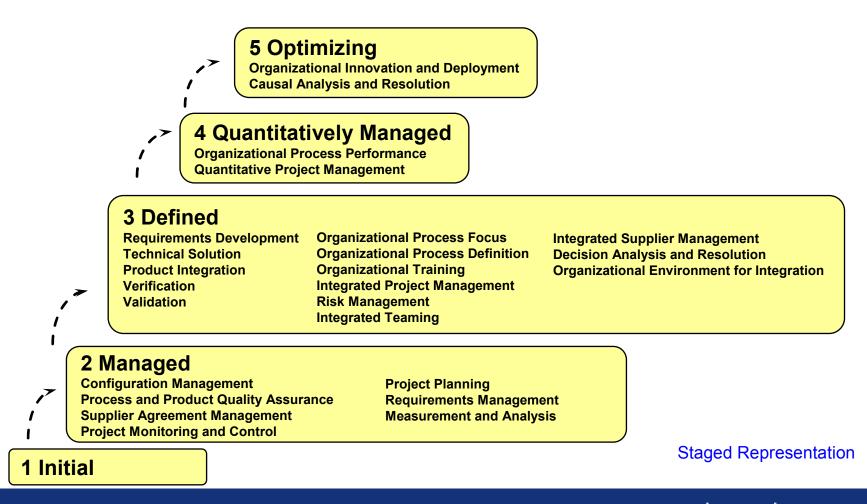
  – FISMA

▶ Market recognition

  – Assurance that security is appropriately addressed

  – Security implementation should be transparent

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

Design, Develop, Integrate

- Develop Design
- Build
- Test & Integrate Solution

Security Requirements

Security Architecture & Design

Security Components

Phase 2

Determine Needs

Security CONOP

Phase 1

Phase 3

Certifiable Fieldable System

Planning & Requirements

Understand Problem

Security Assessment & Feedback

Phase 4

Operation & Maintenance

Assess Operational Security

Accredited Operational Capability

Field Incremental Capability

Verify & Validate

O&M

Legend:
- ⬭ Systems Lifecycle
- ▢ Security Lifecycle
- ➤ C&A* Lifecycle

* Systems Security Certification and Accreditation

Booz | Allen | Hamilton

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

5 Optimizing
Organizational Innovation and Deployment
Causal Analysis and Resolution

4 Quantitatively Managed
Organizational Process Performance
Quantitative Project Management

3 Defined

Requirements Development	Organizational Process Focus	Integrated Supplier Management
Technical Solution	Organizational Process Definition	Decision Analysis and Resolution
Product Integration	Organizational Training	Organizational Environment for Integration
Verification	Integrated Project Management	
Validation	Risk Management	
	Integrated Teaming	

2 Managed

Configuration Management	Project Planning
Process and Product Quality Assurance	Requirements Management
Supplier Agreement Management	Measurement and Analysis
Project Monitoring and Control	

Staged Representation

1 Initial

Booz | Allen | Hamilton

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

Engineering Process

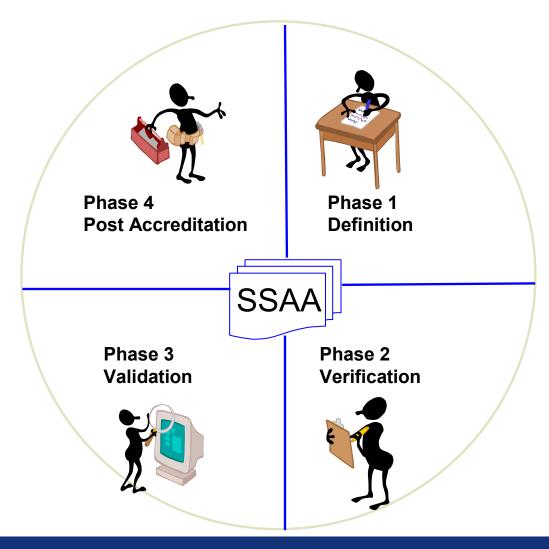Product, System, or Service
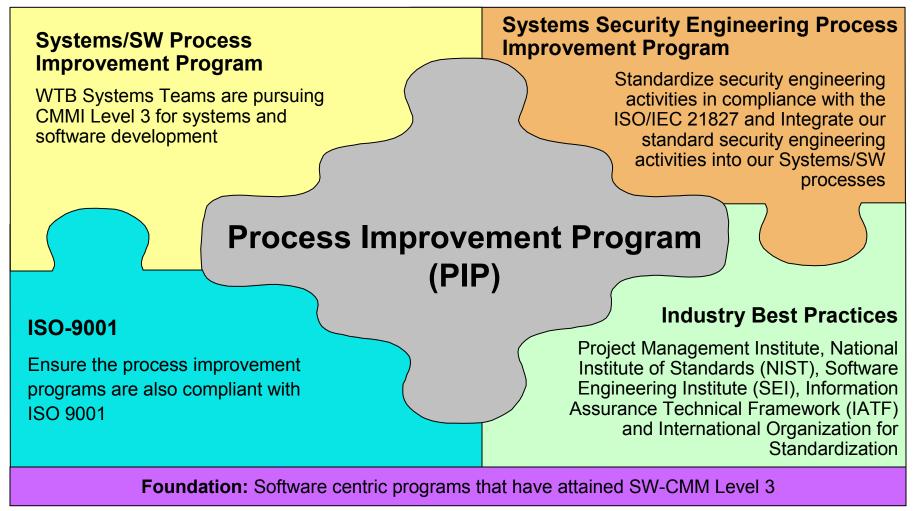
Assurance Process

Assurance Argument

Risk Process

Risk Information

* Systems Security Engineering Capability Maturity Model

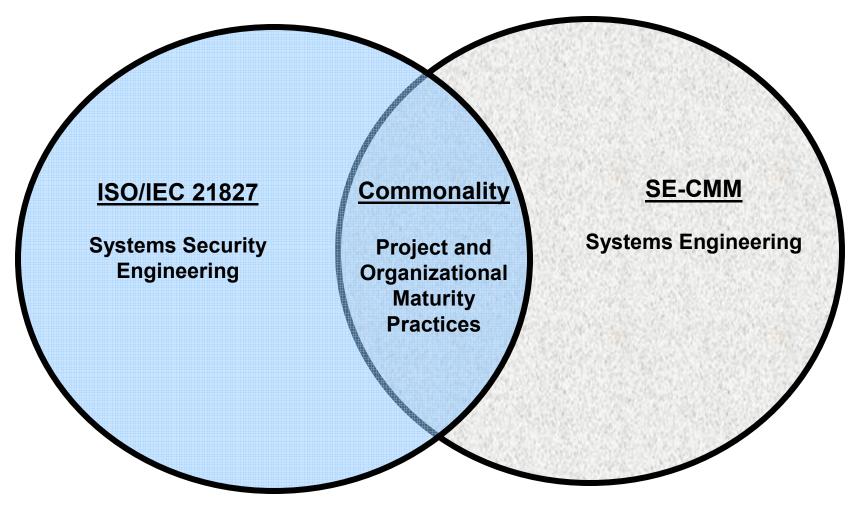# DITSCAP defines the certification and accreditation lifecycle

Phase 4
Post Accreditation

Phase 1
Definition

SSAA

Phase 3
Validation

Phase 2
Verification

Booz | Allen | Hamilton

Organizational Standard Processes leverage industry standards that support diverse clients

Systems/SW Process Improvement Program

WTB Systems Teams are pursuing CMMI Level 3 for systems and software development

Systems Security Engineering Process Improvement Program

Standardize security engineering activities in compliance with the ISO/IEC 21827 and Integrate our standard security engineering activities into our Systems/SW processes

Process Improvement Program (PIP)

ISO-9001

Ensure the process improvement programs are also compliant with ISO 9001

Industry Best Practices

Project Management Institute, National Institute of Standards (NIST), Software Engineering Institute (SEI), Information Assurance Technical Framework (IATF) and International Organization for Standardization

Foundation: Software centric programs that have attained SW-CMM Level 3

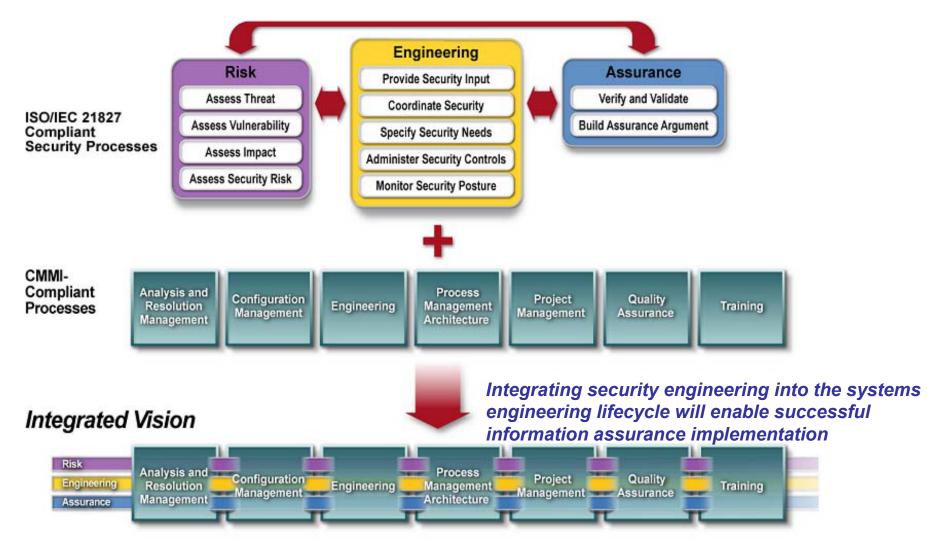**CMMI = Capability Maturity Model Integration**
ISO = International Organization for Standardization

The ISO 21827 is based on the Systems Engineering CMM (SE-CMM), adding security engineering practices to enable improvement of security specific practices

ISO/IEC 21827

Systems Security Engineering

Commonality

Project and Organizational Maturity Practices

SE-CMM

Systems Engineering

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

ISO/IEC 21827 Compliant Security Processes

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

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

Assurance
- Verify and Validate
- Build Assurance Argument

CMMI-Compliant Processes
- Analysis and Resolution Management
- Configuration Management
- Engineering
- Process Management Architecture
- Project Management
- Quality Assurance
- Training

Integrated Vision
- Risk
- Engineering
- Assurance
- Analysis and Resolution Management
- Configuration Management
- Engineering
- Process Management Architecture
- Project Management
- Quality Assurance
- Training

Integrating security engineering into the systems engineering lifecycle will enable successful information assurance implementation

Booz | Allen | Hamilton

There are different CMM Representations

▶ **Staged[1]** - process areas are assessed using specific practices. Predefines the process areas required to attain each maturity level (1-5) and thereby provides a roadmap for institutionalizing best practices.

▶ **Continuous[1]** – process areas are assessed using specific practices within an area and the generic practices required for a specific level. Based on its business objectives, an organization selects the process areas in which it wants to improve and to what degree.

[1]**Software Productivity Consortium, Integrated Processes on the Horizon, Carlos Galvan, Aug 25, 2000**

The SSE-CMM is a continuous model and a target profile is used to scope the appraisal and prioritize the process areas

▶ A target profile is based on

– An analysis of the "Business and Mission Imperatives" and an assessment of which Process Areas are most important to support them

– Industry "best practices" for the type of product, project or service, published Industry sector profiles, or a published profile from another organization in the same or related industry

▶ Organizations may develop their own unique target profiles

– The SSE-CMM does not mandate specific profiles

The ISO 21827 addresses the organization's selected process areas from two dimensions or aspects
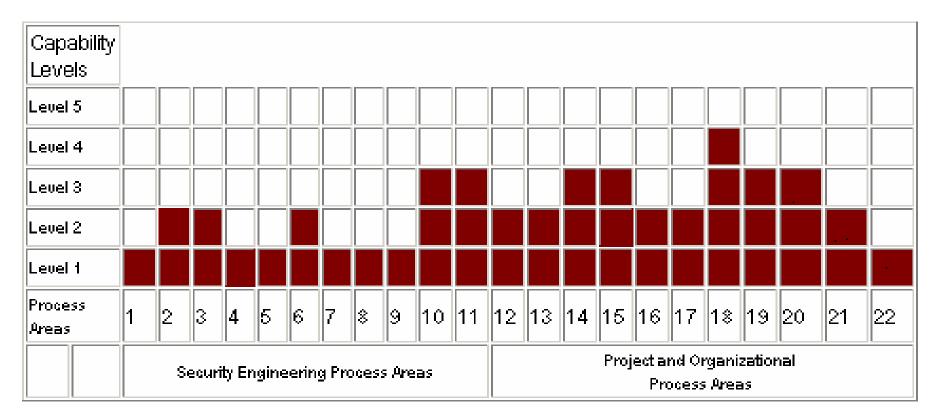

Capability Level → **Common Features** → **Generic Practices**

Capability Aspect – How Well We Do It

Process Areas → **Base Practices**

Domain Aspect – What We Do

▶ The **domain aspect** includes process areas that include base practices for the domain of security engineering

▶ The **capability aspect** addresses institutionalization of the process areas

Booz | Allen | Hamilton

Sample Profile for a Security Product Developer

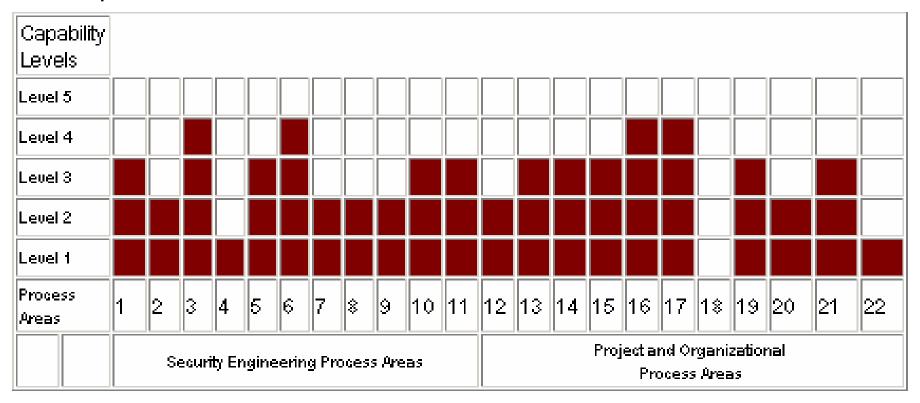▸ For a security product developer, the process areas related to product development activities might target a higher level of maturity.

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.
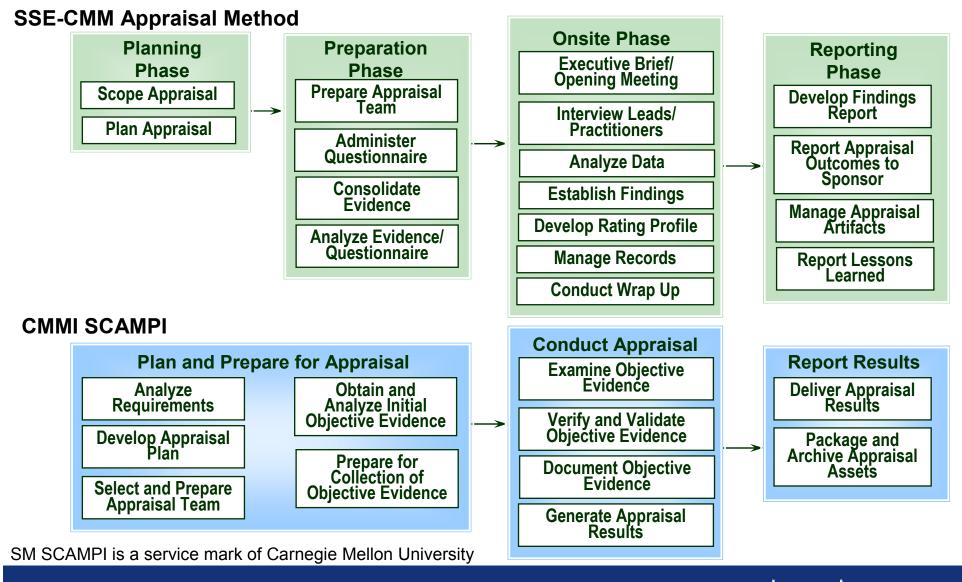

Capability Levels																							
Level 5																							
Level 4			■			■										■	■						
Level 3	■		■		■	■			■	■		■	■	■	■	■			■		■	
Level 2	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■			■	■	■	
Level 1	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■
Process Areas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16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

Security Engineering Process Areas | Project and Organizational Process Areas

Booz | Allen | Hamilton

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)	

An integrated team to 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

Booz | Allen | Hamilton

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

SSE-CMM Appraisal Method

Planning Phase
- Scope Appraisal
- Plan Appraisal

Preparation Phase
- Prepare Appraisal Team
- Administer Questionnaire
- Consolidate Evidence
- Analyze Evidence/ Questionnaire

Onsite Phase
- Executive Brief/ Opening Meeting
- Interview Leads/ Practitioners
- Analyze Data
- Establish Findings
- Develop Rating Profile
- Manage Records
- Conduct Wrap Up

Reporting Phase
- Develop Findings Report
- Report Appraisal Outcomes to Sponsor
- Manage Appraisal Artifacts
- Report Lessons Learned

CMMI SCAMPI

Plan and Prepare for Appraisal
- Analyze Requirements
- Develop Appraisal Plan
- Select and Prepare Appraisal Team
- Obtain and Analyze Initial Objective Evidence
- Prepare for Collection of Objective Evidence

Conduct Appraisal
- Examine Objective Evidence
- Verify and Validate Objective Evidence
- Document Objective Evidence
- Generate Appraisal Results

Report Results
- Deliver Appraisal Results
- Package and Archive Appraisal Assets

SM SCAMPI is a service mark of Carnegie Mellon University

Booz | Allen | Hamilton

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

Development

Implementation

Assessment

Booz | Allen | Hamilton

For More Information

> ISO/IEC 21827

  – www.sse-cmm.org

  – 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.sei.cmu.edu/programs/nss/nss.html

Michele Moss
Associate

Booz | Allen | Hamilton

3190 Fairview Park Drive
Falls Church, VA 22042
Tel (703) 289-5222
moss_michele@bah.com

Booz | Allen | Hamilton

Back up slides

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*

Booz | Allen | Hamilton

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

Booz | Allen | Hamilton
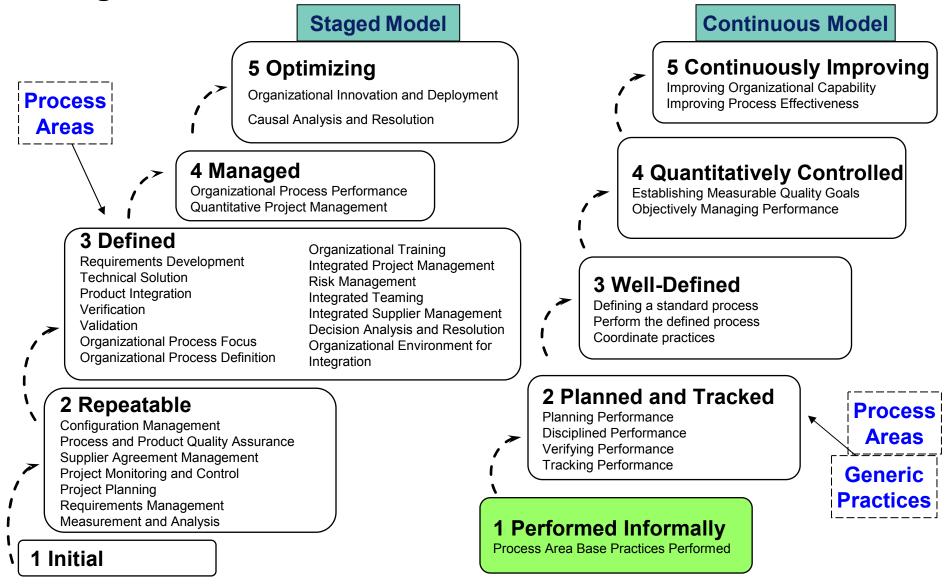
Systems Security Certification & Accreditation

▶ 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

Booz | Allen | Hamilton

Staged vs. Continuous Models

Staged Model

Process Areas

5 Optimizing

Organizational Innovation and Deployment

Causal Analysis and Resolution

4 Managed
Organizational Process Performance
Quantitative Project Management

3 Defined
Requirements Development
Technical Solution
Product Integration
Verification
Validation
Organizational Process Focus
Organizational Process Definition

Organizational Training
Integrated Project Management
Risk Management
Integrated Teaming
Integrated Supplier Management
Decision Analysis and Resolution
Organizational Environment for Integration

2 Repeatable
Configuration Management
Process and Product Quality Assurance
Supplier Agreement Management
Project Monitoring and Control
Project Planning
Requirements Management
Measurement and Analysis

1 Initial

Continuous Model

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

Process Areas

Generic Practices

1 Performed Informally
Process Area Base Practices Performed

Booz | Allen | Hamilton

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	