Tutorial: The Systems Security Engineering Capability Maturity Model

Karen Ferraiolo
Arca Systems, Inc.
8229 Boone Blvd., Suite 750
Vienna, VA 22182
Phone: 703-734-5611
FAX: 703-790-0385
ferraiolo@arca.com

Tutorial Description

The Systems Security Engineering Capability Maturity Model (SSE-CMM) was developed with the objective of advancing security engineering as a defined, mature and measurable discipline. The model and its accompanying appraisal method are currently available tools for evaluating the capability of providers of security engineering products, systems, and services as well as for guiding organizations in defining and improving their security engineering practices.

The SSE-CMM Project began over three years ago as a joint effort between government and industry to develop a CMM for security engineering. The SSE-CMM is rapidly becoming the de facto standard for security engineering practices. Providers of systems, products, and services are now using the model to assess their current practices, identify potential process improvements, and distinguish themselves from competitors. Government acquisition agencies have already begun to use the model to evaluate potential suppliers.

This tutorial describes the SSE-CMM and its appraisal method. A brief introduction to process improvement and CMMs is provided. In addition, a discussion of the application of the SSE-CMM looks at issues as they present themselves throughout a system acquisition, from RFP, through development, and to system operation. The outline of the tutorial is as follows:

- History & the Need
- SSE-CMM Project Status
- Process Improvement and CMMs
- SSE-CMM Overview
- Using the SSE-CMM
- Current Applications

The Systems Security Engineering Capability Maturity Model

Karen Ferraiolo

Arca Systems, Inc.

October 7, 1998

Topics

- **History & the Need**
- **SSE-CMM Project Status**
- **Process Improvement and CMMs**
- **SSE-CMM Overview**
- **Using the SSE-CMM**
- **Current Applications**

History and the Need

What is security engineering?

- **Security engineering, or aspects thereof, attempts to:**
  - **establish a balanced set of security needs**
  - **transform security needs into security guidance**
  - **establish confidence in the correctness and effectiveness of security mechanisms**
  - **judge that operational impacts due to residual security vulnerabilities are tolerable**
  - **integrate all aspects into a combined understanding of the trustworthiness of a system**

Where are we now?

- **Security products come to market through:**
  - **lengthy and expensive evaluation**
  - **no evaluation**
- **Results:**
  - **technology growth more rapid than its assimilation**
  - **unsubstantiated security claims**
- **Causes?**

What is needed?

- **continuity**
- **repeatability**
- **efficiency**
- **assurance**

One Potential Solution

- **Can knowing something about the organization or individual provide a solution?**
- **Examples:**
  - **ISO 9000**
  - **Certification of Information System Security Professionals (CISSP)**
  - **Capability Maturity Model (CMM)**
  - **Malcolm Baldridge National Quality Award**
  - **Past Performance**

Why was the SSE-CMM developed?

Objective

- **advance security engineering as a defined, mature, and measurable discipline**

Project Goal

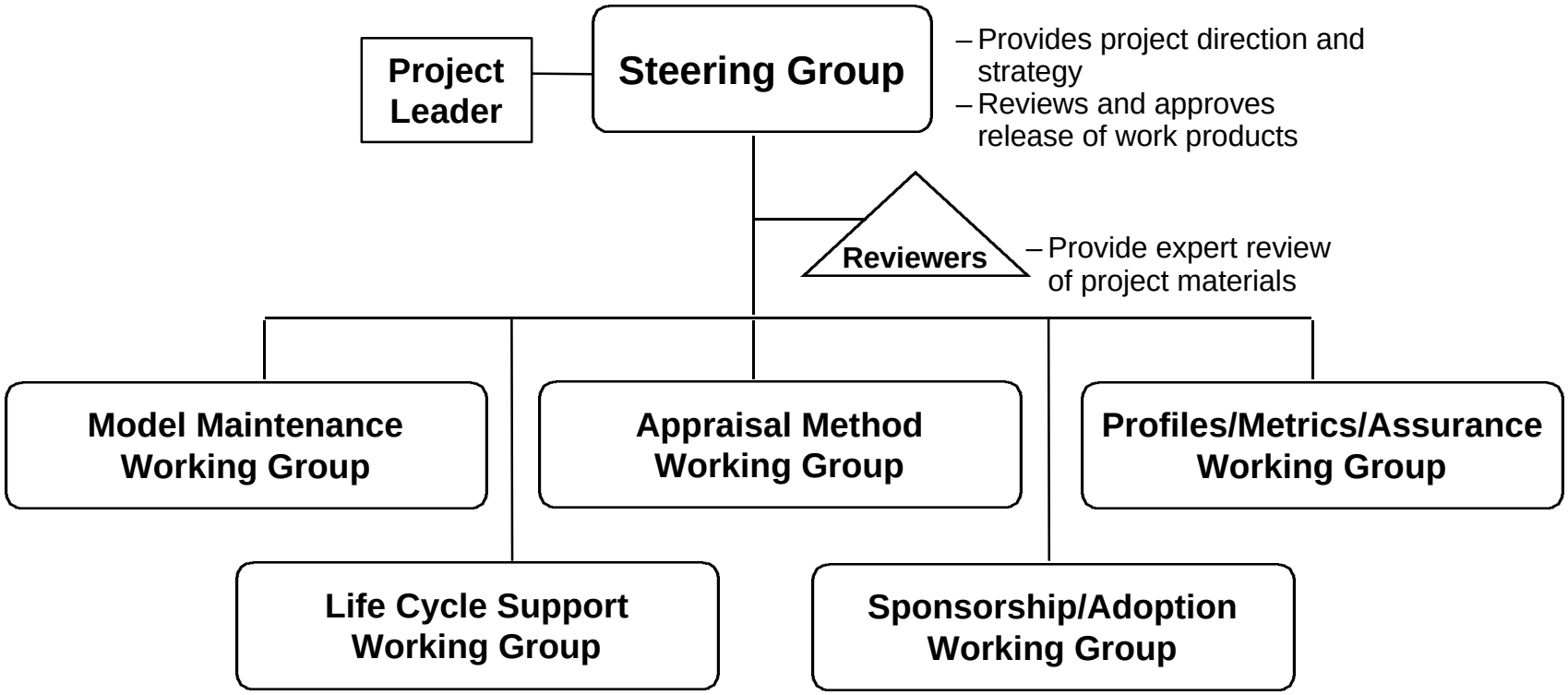
- **Develop a mechanism to enable:**
  - **selection of appropriately qualified security engineering providers**
  - **focused investments in security engineering practices**
  - **capability-based assurance**

Why the CMM approach?

- **accepted way of improving process capability**
- **increasing use in acquisition as indicator of process capability**

The SSE-CMM Project

Project Structure



- **Original work and project infrastructure sponsored by NSA; additional support provided by OSD and Communications Security Establishment (Canada)**
- **Collaborative effort by industry and government on their own funding**

Working Group Schedule

Meetings are held the 2nd week of each month:

- **Monday** — **Profiles, Assurance and Metrics**
  Life Cycle Support
- **Tuesday** — **Model Maintenance**
- **Wednesday** — **Sponsorship, Planning and Adoption**
- **Thursday** — **Steering Group**
- **Friday** — **Appraisal Method**

Points of Contact

Project Sponsor:

Mary Schanken
NSA, V243
410-859-6094
schanken@romulus.ncsc.mil

Steering Group:

Ron Knode
Computer Sciences Corporation
410-691-6580
rknode@csc.com

Model Maintenance:

Jeff Williams
Arca Systems, Inc.
703-734-5611
williams@arca.com

Appraisal Method:

Mal Fordham
IIT Research Institute
301-918-1022
mfordham@atg.iitri.com

Sponsorship/Adoption:

Jim Robbins
EWA Canada, Ltd.
613-230-6067 ext. 216
jrobbins@ewa-canada.com

Life Cycle Support:

Virgil Gibson
Computer Sciences Corp.
410-684-6325
vgibson1@csc.com

Profile/Metrics/Assurance:

George Jelen
G-J Consulting
301-384-5296
gjelen@erols.com

Web site: http://www.sse-cmm.org

Project Participants

- Arca Systems, Inc.
- BDM International Inc.
- Booz-Allen and Hamilton, Inc.
- Communications Security Establishment (Canada)
- Computer Sciences Corporation
- Data Systems Analysts, Inc.
- Defense Information Systems Agency
- E-Systems
- Electronic Warfare Associates - Canada, Ltd.
- Fuentez Systems Concepts
- G-J Consulting
- GRC International, Inc.
- Harris Corp.
- Hughes Aircraft
- Institute for Computer & Information Sciences
- Institute for Defense Analyses
- Internal Revenue Service
- ITT Aerospace
- JOTA System Security Consultants, Inc.
- Lockheed Martin
- Merdan Group, Inc.
- MITRE Corporation
- Mitretek Systems
- Motorola
- National Center for Supercomputing Applications
- National Institute for Standards and Technology
- National Security Agency
- Naval Research Laboratory
- Navy Command, Control, Operations Support Center; Research, Development, Testing, and Evaluation Division (NRaD)
- Northrop Grumman
- NRaD
- Office of the Secretary of Defense
- Oracle Corporation
- pragma Systems Corp.
- San Antonio Air Logistics Center
- Science Applications International Corp.
- SPARTA, Inc.
- Stanford Telecom
- Systems Research & Applications Corp.
- Tax Modernization Institute
- The Sachs Groups
- tOmega Engineering
- Trusted Information Systems
- TRW
- Unisys Government Systems

Project Accomplishments

April 93-December 94	**Initial R&D**
January 95	**1st Public Workshop**
	Working Groups Formed
Summer/Fall 96	**SSE-CMM Pilot Program**
October 96	**SSE-CMM v1.0**
Spring 97	**Appraisal Method v1.0**
Summer 97	**SSE-CMM v1.1**
	Appraisal Method v1.1
14-17 July 97	**2nd Public Workshop**
October 98	**SSE-CMM v2.0**
	Appraisal Method v2.0 (Draft)

Pilot Sites

- **TRW:** **System Integrator**
- **CSC:** **Service Provider - Risk Assessment**
- **Hughes:** **System Integrator**
- **GTIS (Canada):** **Service Provider - Certification Authority**
- **Data General:** **Product Vendor**

Current Activities

- **The Project**
  - **pursuing ISO standard**
  - **planning for transition to new support organization**
  - **seeking more commitments of intended use by acquisition organizations**
- **The Model**
  - **updating risk-related process areas**
  - **reviewing SEI CMM Integration Project results**

Current Activities *(cont.)*

- **The Appraisal Method**
  - **updating to accommodate 3rd party capability evaluations**
- **Assurance**
  - **researching security metrics**
- **Support Activities**
  - **developing plan for qualification of SSE-CMM appraisers**
  - **researching approaches for uniformity of appraisals**
  - **designing SSE-CMM data repository**

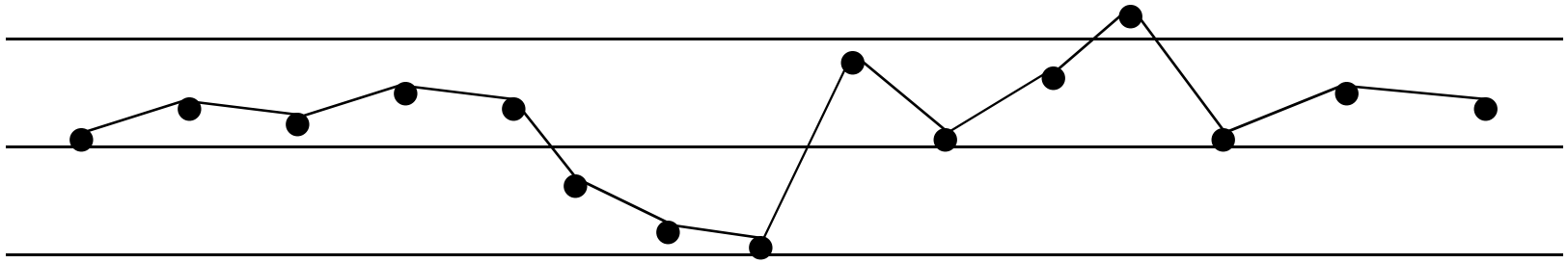
Future Plans

Oct 98	**ISO submission - Project transition phase**
Oct 98 - Feb 99	**Conduct Appraisal Method beta testing**
May 99	**Appraisal Method v2.0 published**
July 99	**SSE-CMM “Project” phase ends - new support organizations begins operations**

Process Improvement & CMMs

Process Capability

- **Process Capability**
  - **the range of expected results that can be achieved by following a process**
  - **a predictor of future project outcomes**
- **Process Performance**
  - **a measure of the actual results achieved from following a process (on a particular project)**



Statistical Process Control

- **A process in statistical control:**
  - **has definable, measurable, communicable:**
    - **identity**
    - **capability**
  - **limits of variation are predictable**
- **however,**
  - **it does not imply the absense of defective items**

Once statistical control has been established, work can begin to improve quality and economy of production

Process Maturity

- **extent to which process is explicitly**
  defined managed measured controlled effective
- **implies a potential for growth in capability**
- **indicates richness of process and consistency of its application**

Why are Maturity Levels Important?

Maturity Levels (in Capability Maturity Models)

- **define ordinal scale for measuring / evaluating process capability**
- **define incremental steps for improving process capability**

Maturity Levels Discriminate Process Capability

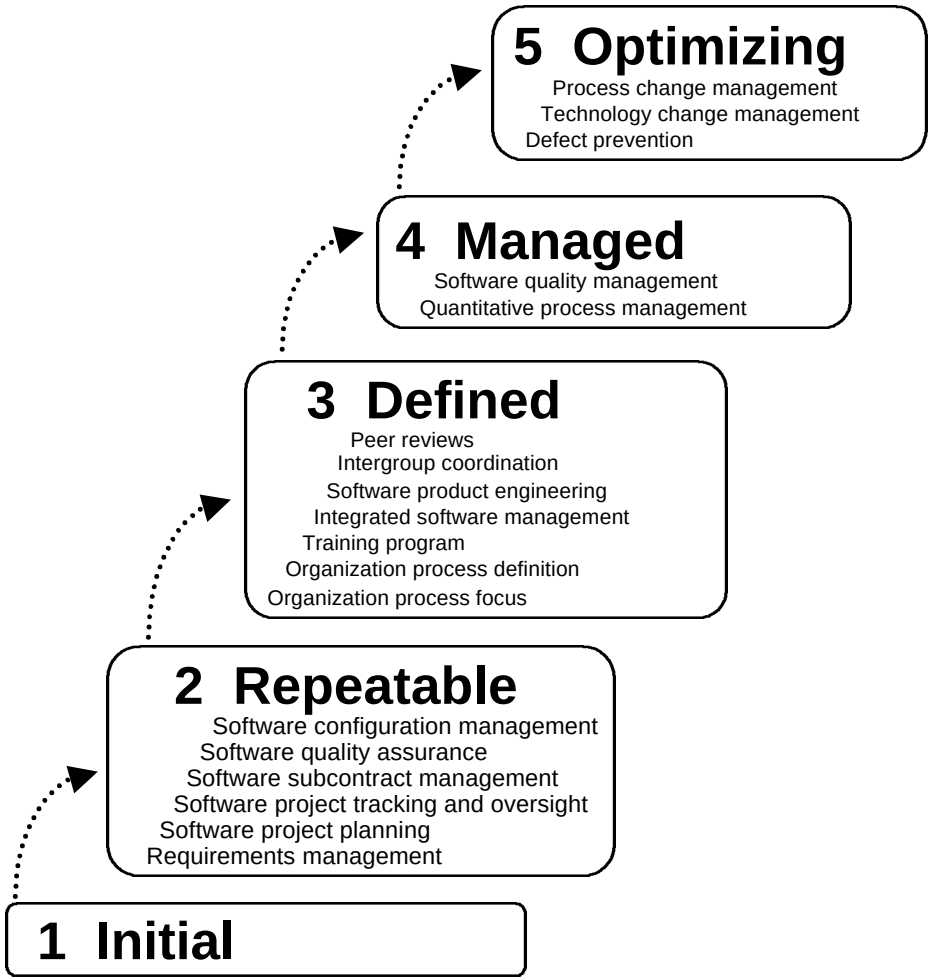
How do CMMs define Maturity?

Two aspects:

- **the domain**
  - **process areas**
  - **base practices**
- **the organization**
  - **institutionalization of process areas**
  - **implementation of process areas**

How do CMMs define Maturity?

Staged Capability Maturity Model

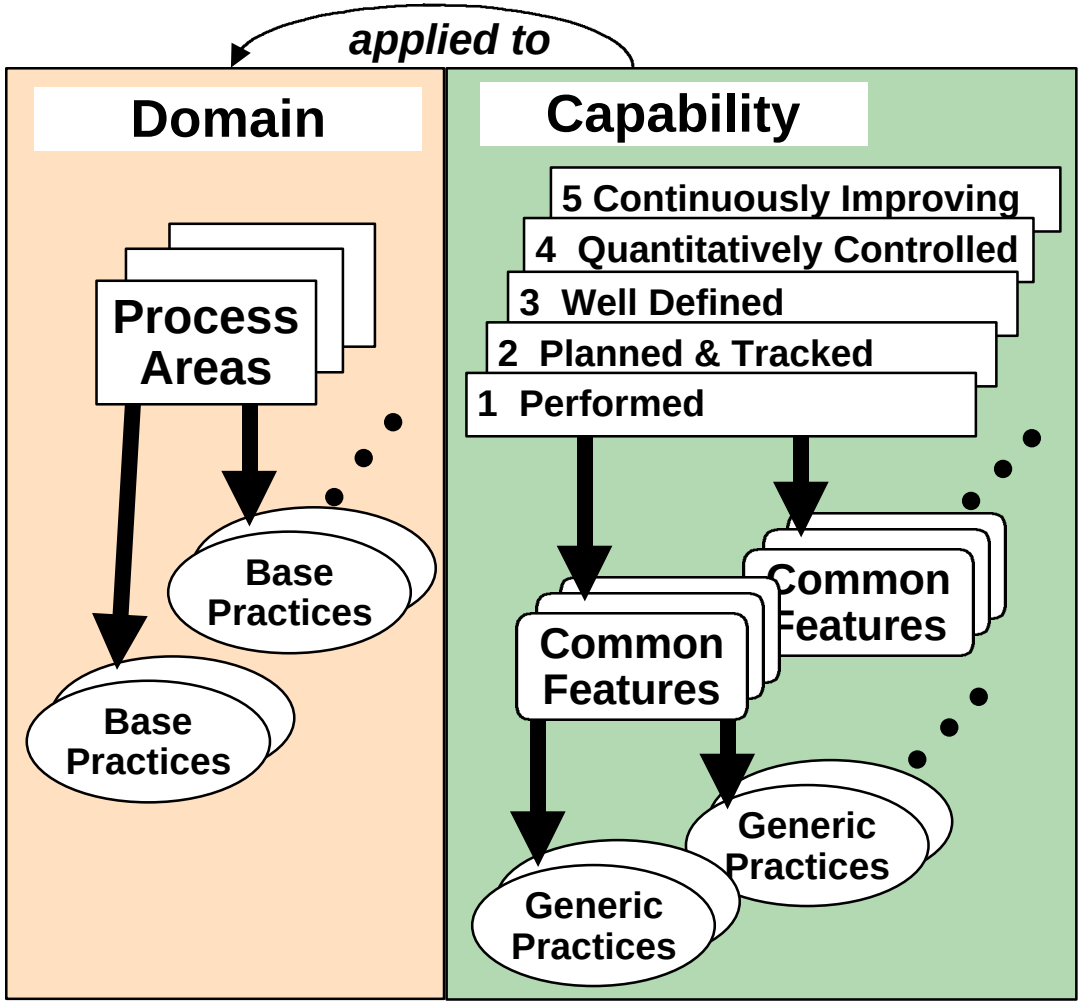


- **Process Areas (PAs) define Process Maturity for a specific domain**
- **Capability Maturity within a specific domain is achieved by implementation of specific PAs**
- **Institutionalization / Implementation aspects are addressed within PAs**

Domain Process Maturity is defined in Model Structure

How do CMMs define Maturity?

Continuous Capability Maturity Model



- **Process Areas (PAs) organize practices of a specific domain**
- **Institutionalization / implementation of PAs define the Process Maturity for any domain**
- **Capability Maturity needs to be interpreted for a specific domain**

Domain Process Maturity must be defined by Model Appraisal Structure

Vocabulary Summary

Vocabulary

- **ORGANIZATION - a company or entity within a company within which many projects are managed as a whole**
- **PROJECT - the aggregate of effort and resources focused on developing and/or maintaining a specific product or providing a service**
- **SYSTEM - the sum of products being delivered to a customer or user; denoting a product as a system acknowledges the need to treat all elements of a product and their inerfaces in a disciplined and systematic way**
- **WORK PRODUCT - all documents, reports, files, data, etc., generated in the course of performing any process**
- **CUSTOMER - the individual(s) or entity for whom a product is developed or service is rendered, and/or who uses the product or service**
- **PROCESS - a set of activities performed to achieve a given purpose**
- **PROCESS AREA (PA) - a defined set of related process characteristics, which when performed collectively, can achieve a defined purpose**

Vocabulary

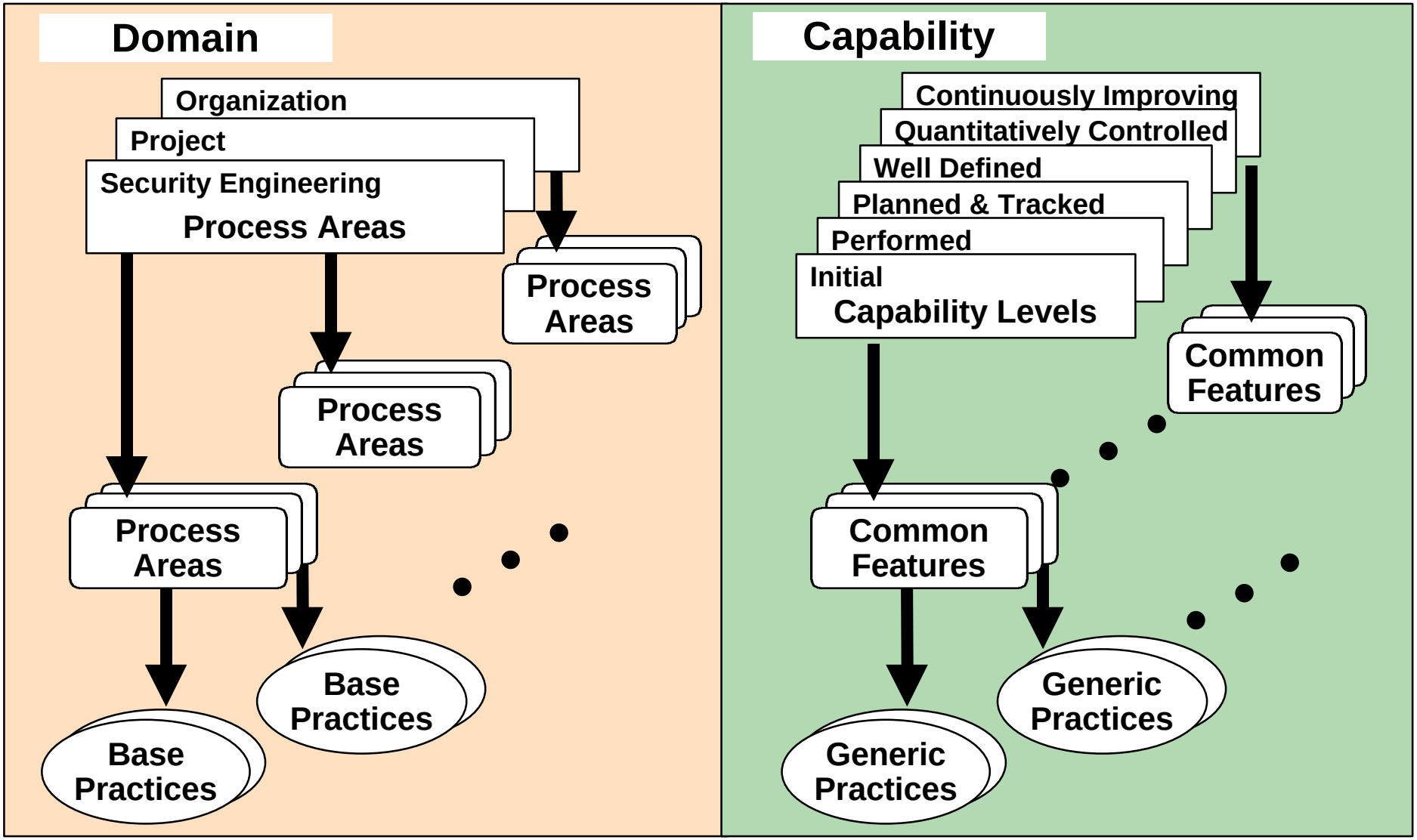
- **PROCESS CAPABILITY - the quantifiable range of expected results that can be achieved by following a process; helps to predict a project's ability to meet its goals**
- **INSTITUTIONALIZATION - the building of infrastructure and corporate culture that support methods, practices, and procedures so that they are the ongoing way of doing business, even after those who originally defined them are gone**
- **PROCESS MANAGEMENT - the set of activities and infrastructures used to predict, evaluate, and control the performance of a process**
- **CAPABILITY MATURITY MODEL (CMM) - describes the stages through which processes progress as they are defined, implemented, and improved**
- **CAPABILITY LEVEL - a set of implementation and institutionalization practices that work together to provide a major enhancement in the ability to perform a process area**

Vocabulary

- **ASSURANCE - the degree of confidence that security needs are satisfied**
- **GROUP - the collection of individuals that has responsibility for a set of tasks or activities**
- **ENGINEERING GROUP - the collection of individuals (both managers and technical staff) that is responsible for project or organizational activities related to a particular engineering discipline**
- **SECURITY ENGINEERING GROUP - the collection of individuals (both managers and technical staff) which is responsible for project or organizational security engineering activities**
- **SYSTEMS ENGINEERING CMM (SE-CMM) - developed for the discipline of systems engineering; structure is the basis for the SSE-CMM**

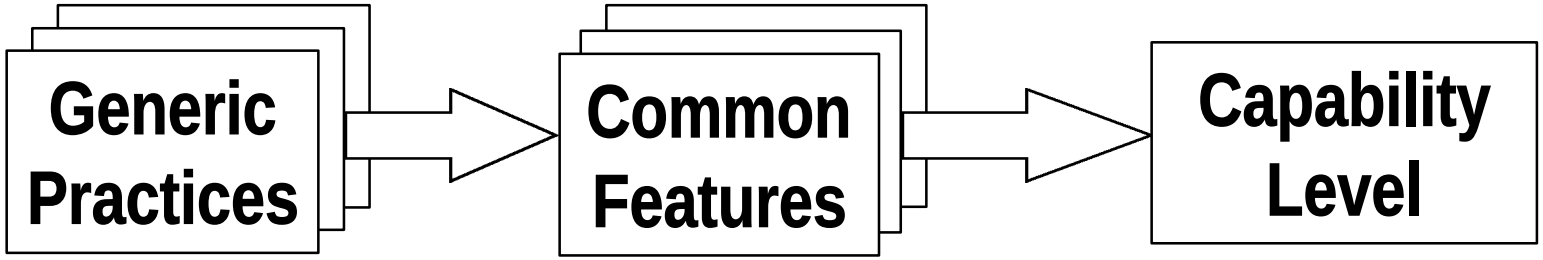
SSE-CMM Overview

SSE-CMM Model Architecture



SSE-CMM Architecture

(Capability Aspect)



Generic Practices	Common Features	Capability Level
Implementation or institutionalization practices that enhance the capability to perform any process	Set of practices that address the same aspect of process management or institutionalization	A set of common features that work together to provide a major enhancement in the capability to perform a process

Capability Levels and Common Features

0 INITIAL

1 PERFORMED INFORMALLY

- **Base practices performed**

2 PLANNED & TRACKED

- **Planning performance**
- **Disciplined performance**
- **Verifying performance**
- **Tracking performance**

3 WELL-DEFINED

- **Defining a standard process**
- **Perform the defined process**
- ***Coordinate practices***

4 QUANTITATIVELY CONTROLLED

- **Establishing measurable quality goals**
- **Objectively managing performance**

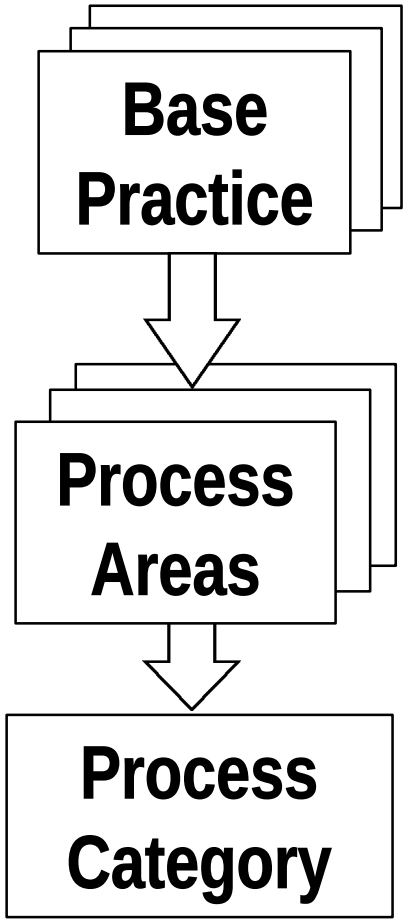
5 CONTINUOUSLY IMPROVING

- **Improving organizational capability**
- **Improving process effectiveness**

Note: Capability Levels and Common Features are taken from the SE-CMM; Italics indicate SSE-CMM additional Common Feature

SSE-CMM Architecture

(Domain Aspect)



Engineering or management practices that address the purpose of a particular process area and thus belong to it

Sets of related practices, which when performed collectively, can achieve the purpose of the process area

A set of process areas addressing the same general area of activity

Security Engineering Process Areas

Administer Security Controls

Assess Impact

Assess Security Risk

Assess Threat

Assess Vulnerability

Build Assurance Argument

Coordinate Security

Monitor System Security Posture

Provide Security Input

Specify Security Needs

Verify and Validate Security

Basis for Engineering Process Areas

(Security Engineering Providers)

	Applicable Source		
Provider with Security Engineering Activities	**Products**	**Systems**	**Services**
Independent Security Verification and Validation			*X*
Operational Risk (Threat, Weaknesses, Impact) Analysis - Development		*X*	*X*
Operational Risk (Threat, Weaknesses, Impact) Analysis - Post Development (AKA Security Audits)			*X*
Product Vendor (of a standard product with security features)	*X*		
Security Penetration Testing	*X*	*X*	*X*
Security Requirements & (High-Level) Architecture Resolution	*X*	*X*	*X*
Security Design & Implementation Guidance			*X*
Security Design & Implementation	*X*	*X*	
Security Testing & Integration Guidance			*X*
Security Testing & Integration	*X*	*X*	
Security Product Vendor (including Security Device Vendor)	*X*		
System Weakness (Attack, Vulnerability, Impact) Analysis - Development	*X*	*X*	*X*
System Weakness (Attack, Vulnerability, Impact) Analysis - Post Development			*X*
Trusted Product Vendor	*X*		
Trusted Software/Applications Developer	*X*	*X*	*X*

from:
"SSE-CMM Model and Application Report"
October 2, 1995

Administer Security Controls

- **Goals:**
  - **Security controls are properly configured and used**
- **Base Practices:**
  - **Establish Security Responsibilities**
  - **Manage Security Configuration**
  - **Manage Security Awareness, Training, and Education Programs**
  - **Manage Security Services and Control Mechanisms**

Assess Impact

- **Goals:**
  - **The security impacts of risks to the system are identified and characterized**
- **Base Practices:**
  - **Prioritize Capabilities**
  - **Identify System Assets**
  - **Select Impact Metric(s)**
  - **Identify Metric Relationship**
  - **Identify and Characterize Impacts**
  - **Monitor Impacts**

Assess Security Risk

- **Goals:**
  - **An understanding of the security risk associated with operating the system within a defined environment is achieved**
  - **Risks are prioritized according to a defined method**
- **Base Practices:**
  - **Select Risk Analysis Method**
  - **Identify Exposures**
  - **Assess Exposure Risk**
  - **Assess Total Uncertainty**
  - **Prioritize Risks**
  - **Monitor Risks and Their Characteristics**

Assess Threat

- **Goals:**
  - **Threats to the security of the system are identified and characterized**
- **Base Practices:**
  - **Identify Natural Threats**
  - **Identify Man Made Threats**
  - **Identify Threat Units of Measure**
  - **Assess Threat Agent Capability**
  - **Assess Threat Likelihood**
  - **Monitor Threats and Their Characteristics**

Assess Vulnerability

- **Goals:**
  - **An understanding of system security vulnerabilities within a defined environment is achieved**
- **Base Practices:**
  - **Select Vulnerability Analysis Method**
  - **Identify Vulnerabilities**
  - **Gather Vulnerability Data**
  - **Synthesize System Vulnerability**
  - **Monitor Vulnerabilities and Their Characteristics**

Build Assurance Argument

- **Goals:**
  - **The work products and processes clearly provide the evidence that the customer's security needs have been met**
- **Base Practices:**
  - **Identify Assurance Objectives**
  - **Define Assurance Strategy**
  - **Control Assurance Evidence**
  - **Analyze Evidence**
  - **Provide Assurance Argument**

Coordinate Security

- **Goals:**
  - **All members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions**
  - **Decisions and recommendations related to security are communicated and coordinated**
- **Base Practices:**
  - **Define Coordination Objectives**
  - **Identify Coordination Mechanisms**
  - **Facilitate Coordination**
  - **Coordinate Security Decisions and Recommendations**

Monitor System Security Posture

- **Goals:**
  - **Both internal and external security related events are detected and tracked**
  - **Incidents are responded to in accordance with policy**
  - **Changes to the operational security posture are identified and handled in accordance with security objectives**
- **Base Practices:**
  - **Analyze Event Records**
  - **Monitor Changes**
  - **Identify Security Incidents**
  - **Monitor Security Safeguards**
  - **Review Security Posture**
  - **Manage Security Incident Response**
  - **Protect Security Monitoring Artifacts**

Provide Security Input

- **Goals:**
  - **All system issues are reviewed for security implications and are resolved in accordance with security goals**
  - **All members of the project team have an understanding of security so they can perform their functions**
  - **The solution reflects the security input provided**
- **Base Practices:**
  - **Understand Security Input Needs**
  - **Determine Security Constraints and Considerations**
  - **Identify Security Alternatives**
  - **Analyze Security of Engineering Alternatives**
  - **Provide Security Engineering Guidance**
  - **Provide Operational Security Guidance**

Specify Security Needs

- **Goals:**
  - **A common understanding of security needs is reached between all applicable parties, including the customer**
- **Base Practices:**
  - **Gain Understanding of Customer Security Needs**
  - **Identify Applicable Laws, Policies, Standards, and Constraints**
  - **Identify System Security Context**
  - **Capture Security View of System Operation**
  - **Capture Security High Level Goals**
  - **Define Security Related Requirements**
  - **Obtain Agreement on Security**

Verify and Validate Security

- **Goals:**
  - **Solutions meet security requirements**
  - **Solutions meet the customer's operational security needs**
- **Base Practices:**
  - **Identify Verification and Validation Targets**
  - **Define Verification and Validation Approach**
  - **Perform Verification**
  - **Perform Validation**
  - **Provide Verification and Validation Results**

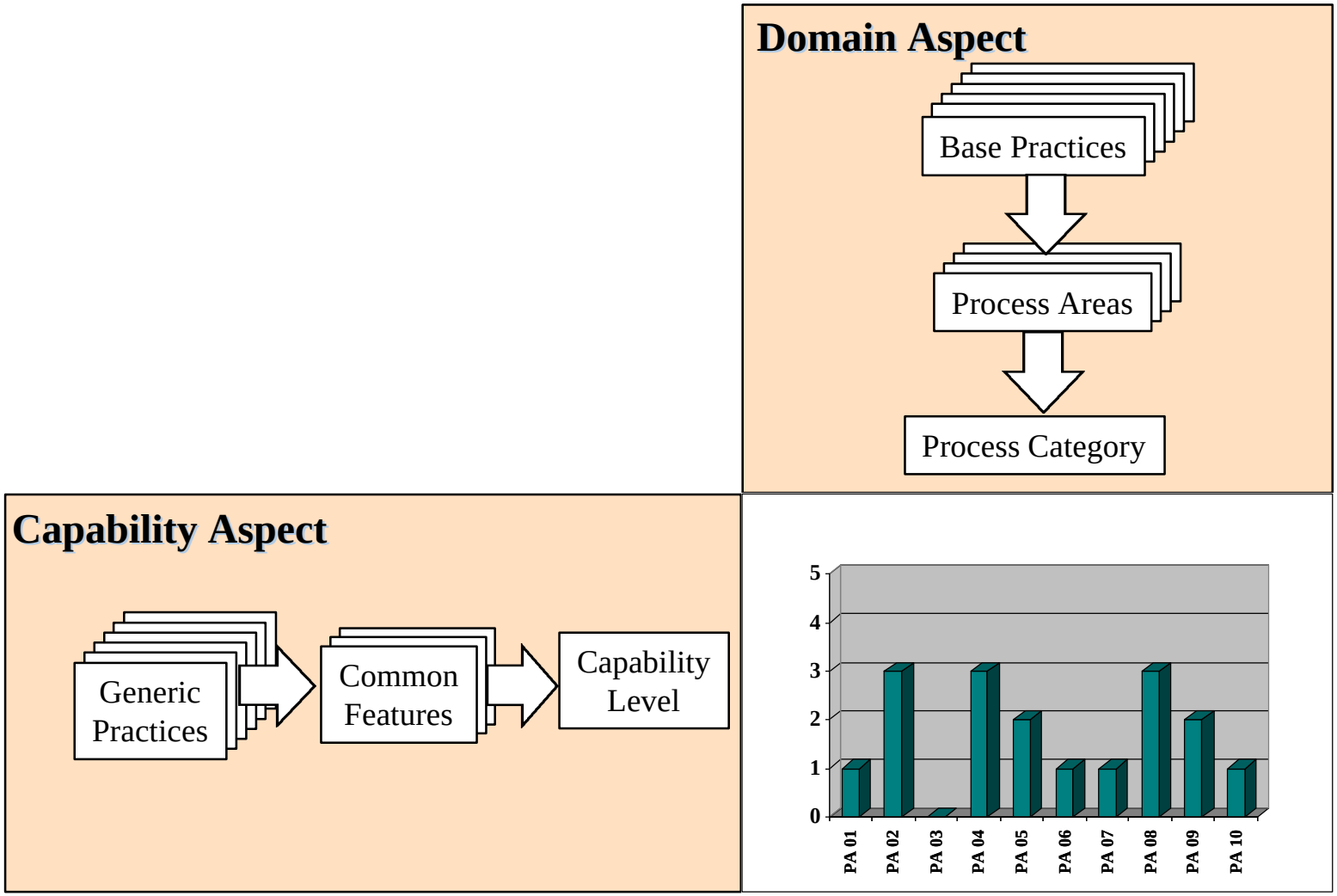
Project/Organization PAs

(based on SE-CMM with Security Considerations)

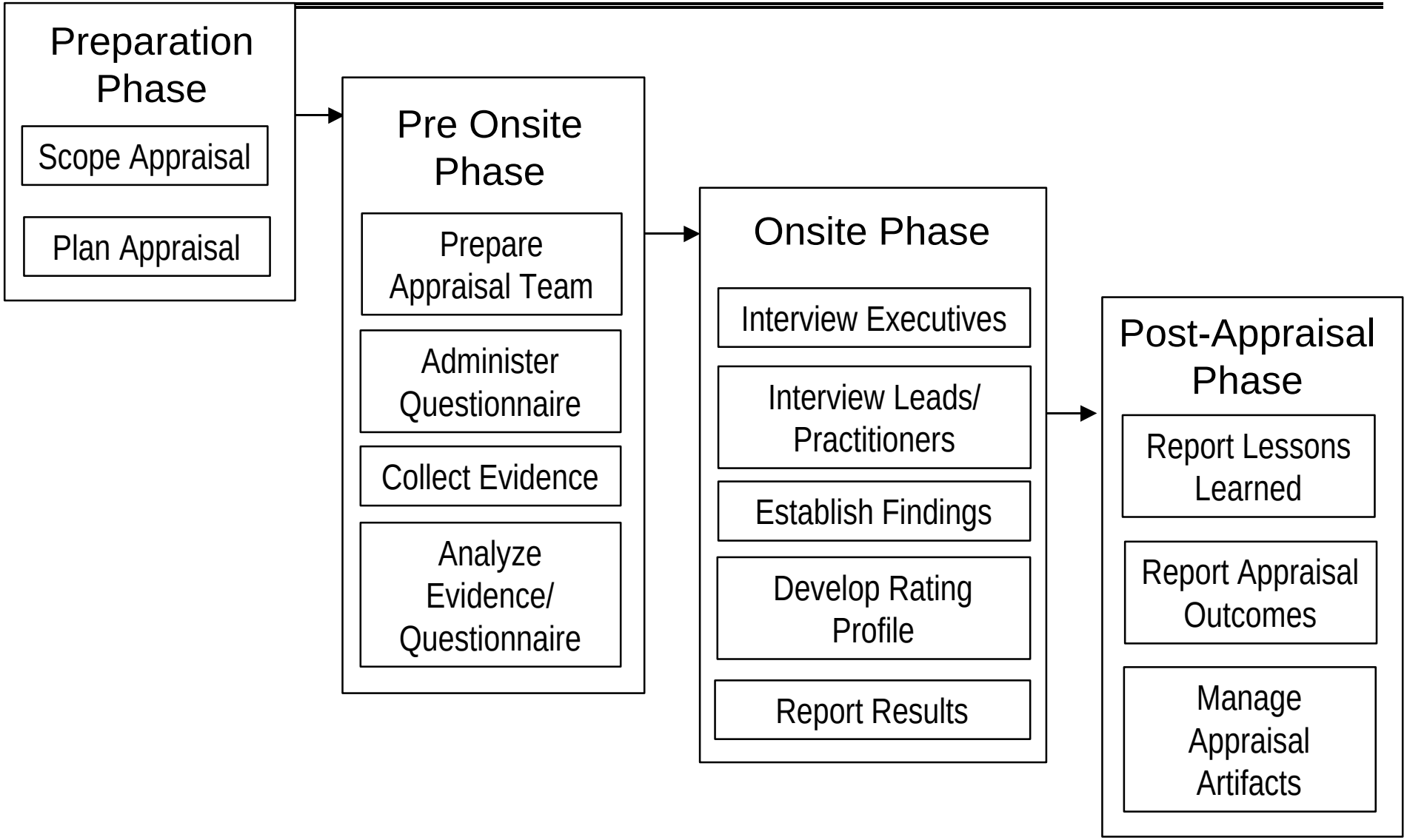
Project	Organization
Ensure Quality	Define Organization's Security Engineering Process
Manage Configurations	Improve Organization's Security Engineering Process
Manage Program Risk	Manage Security Product Line Evolution
Monitor and Control Technical Effort	Manage Security Engineering Support Environment
Plan Technical Effort	Provide Ongoing Skills and Knowledge
	Coordinate with Suppliers

Using the SSE-CMM

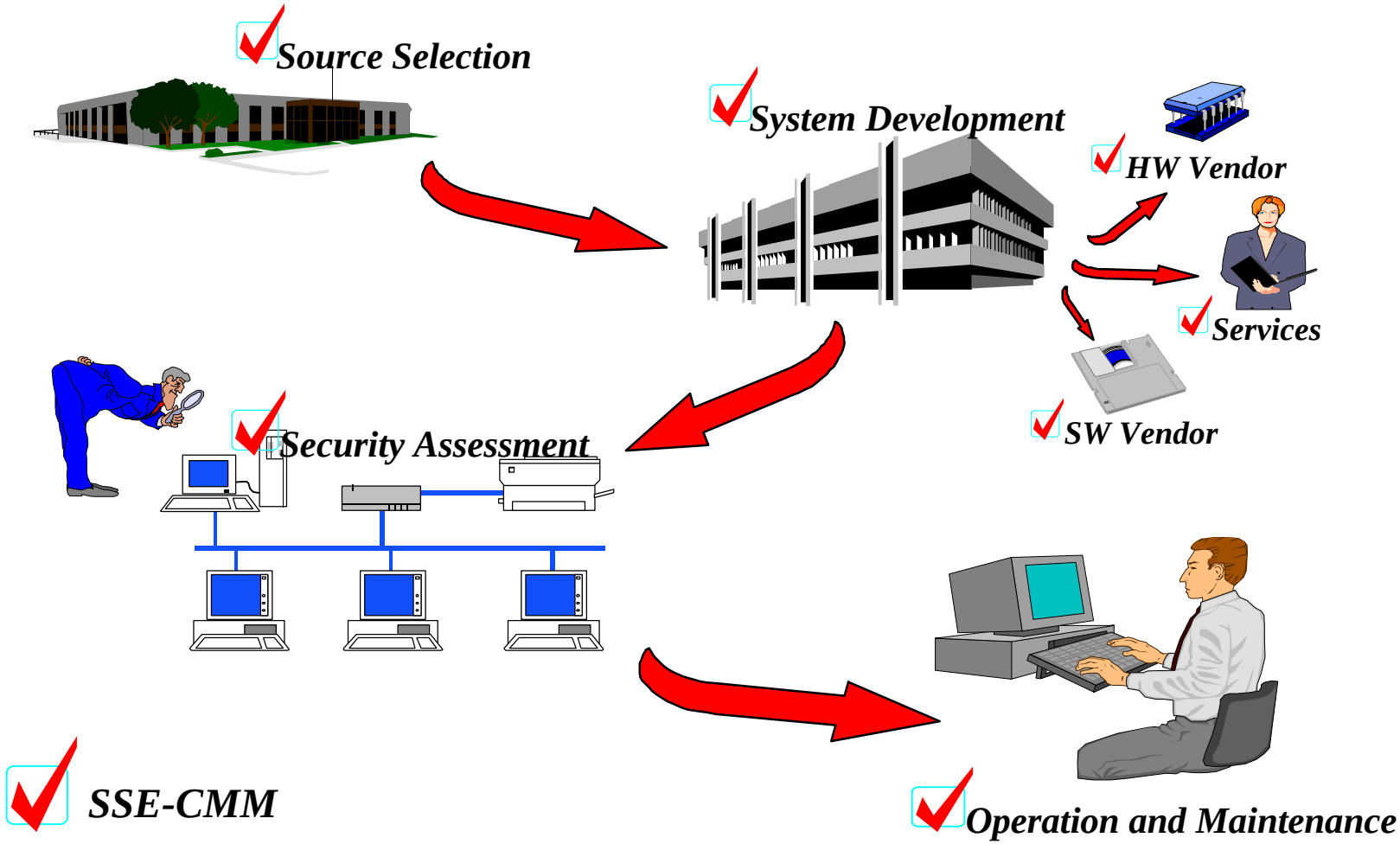
Appraisal Results: a Rating Profile



The Appraisal Process



Using the SSE-CMM



Use by Engineering Organizations

- **Define processes / practices**
- **Use for competitive edge (in source selections)**
- **Focus improvement efforts**

Issues

- **big investment**
- **requires commitment at all levels**
- **need to interpret the PAs in the organization's context**

Use by Acquirers

- **Standard RFP language and bidder evaluation**
- **Understanding programmatic risks**
- **Avoid protests (uniform assessments)**
- **Greater level of confidence in end results**

Issues

- **doesn’t guarantee good results**
- **uniformity of appraisals**
- **need good understanding of model and how to use it**

Use by Security Evaluation Organizations

- **Alternative to extensive evaluation/re-evaluation**
  - **confidence in integration of security engineering with other disciplines**
  - **confidence in end results**

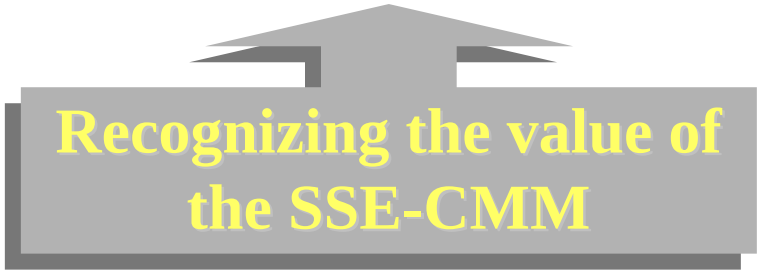
Issues

- **doesn't guarantee good results**
- **uniformity of appraisals**
- **need good understanding of model and how to use it**
- **doesn't eliminate the need for testing/evaluation**
- **understanding how the SSE-CMM actually contributes to assurance**

Current Applications

Where is it taking hold?

- **US National Security Agency (NSA)**
- **Canadian Communications Security Establishment (CSE)**
- **US Federal Aviation Administration (FAA)**
  - **(Draft) FAA Order 1600.69 (FAA Information Systems Security Program)**



Where to get more information

Process Improvement / CMMs

- **Deming, W.E., *Out of the Crisis*, Cambridge MA: Massachusetts Institute of Technology Center for Advanced Engineering Study, 1986.**
- **Humphrey, W.S., "Characterizing the Software Process: A Maturity Framework," IEEE Software, Vol. 5, No. 2, Mar 1988, pp. 73-79.**
- **Office of the Under Secretary of Defense for Acquisition, Washington, D.C., *Report of the Defense Science Board Task Force on Military Software*, Sept 1987.**
- **Paulk, M.C.; Curtis, B.; Chrissis, M.B.; Weber, C.V., *Capability Maturity Model for Software, Version1.1*, Software Engineering Institute, CMU/SEI-93-TR-24, Feb 1993.**
- **Paulk, M.C.; Weber, C.V.; Garcia, S.; Chrissis, M.B.; Bush, M., *Key Practices of theCapability Maturity Model, Version1.1*, Software Engineering Institute, CMU/SEI-93-TR-25, Feb 1993.**
- **Software Engineering Institute, "Benefits of CMM-Based Software Process Improvement: Initial Results," Software Engineering Institute, SEI-94-TR-013, 1994.**

CMM for Security Engineering

- **Ferraiolo, K.; Thompson, V., "Let's Just Be Mature About Security," Crosstalk, The Journal of Defense Software Engineering, August 1997.**
- **Ferraiolo, K.; Sachs, J., "Determining Assurance Levels by Security Engineering Process Maturity," Proceedings of the Fifth Annual Canadian Computer Security Symposium, May 1993.**
- **Ferraiolo, K.; Williams, J.; Landoll, D., "A Capability Maturity Model for Security Engineering," Proceedings of the Sixth Annual Canadian Computer Security Symposium, May 1994.**
- **Ferraiolo, K.; Sachs, J., "Distinguishing Security Engineering Process Areas by Maturity Levels," Proceedings of the Eighth Annual Canadian Computer Security Symposium, May 1996.**
- **Gallagher, L., Thompson, V., "An Update on the Security Engineering Capability Maturity Model Project," Proceedings of the Seventh Annual Canadian Computer Security Symposium, May 1995.**
- **Hefner, R.; Hsiao, D.; Monroe, W., "Experience with the Systems Security Engineering Capability Maturity Model," Proceedings of the International Council on Systems Engineering Symposium, July 1996.**
- **Hosy, H.; Roussely, B., "Industrial Maturity and Information Technology Security," Proceedings of the Seventh Annual Canadian Computer Security Symposium, May 1995.**
- **Menk, C.G. III, "The SSE-CMM & Evaluations: Partners within the Assurance Framework," Proceedings of the 1996 National Information Systems Security Conference, Oct 1996.**
- **Zior, M., "Community Response to CMM-Based Security Engineering Process Improvement," Proceedings of the 1995 National Information Systems Security Conference, Oct 1995.**