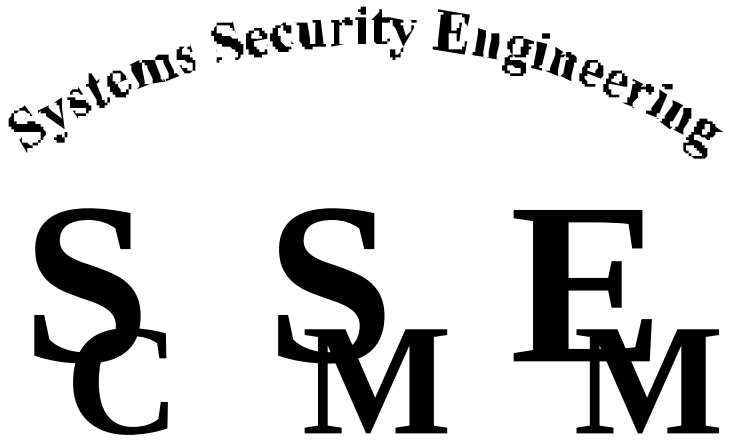

Capability Maturity Model

Model Description, Version 1.1

June 16, 1997

This work is the product of a collaborative effort by various organizations within government, industry, and academia. This document includes many excerpts from "A Systems Engineering Capability Maturity Model, Version 1.1," CMU/SEI-95-MM-003, published in November 1995. Included below is the copyright for this Systems Engineering CMM document:

Copyright © 1995 by Carnegie Mellon University. This work is a collaborative effort of Hughes Space and Communications, Hughes Telecommunications and Space, Lockheed Martin, Software Engineering Institute, Software Productivity Consortium, and Texas Instruments Incorporated. Permission to reproduce this product and to prepare derivative works from this product is granted royalty-free, provided the copyright is included with all reproductions and derivative works.

Acknowledgments

Project Participants

The Systems Security Engineering Capability Maturity Model (SSE-CMM) is a community-owned model, and is a result of the dedicated work of many individuals. The following list acknowledges the efforts and support of those organizations that contributed to the effort through participation in Working Groups or as reviewers:

Arca Systems, Inc.
BDM International, Inc.
Booz-Allen & Hamilton,Inc.
Communications Security Establishment (Canada)
Computer Sciences Canada
Computer Sciences Corporation
Data Systems Analysts, Inc.
Department of Defense Information Systems Agency
E-Systems
Electronic Warfare Associates - Canada, Ltd.
Fuentez Systems Concepts, Inc.
G-J Consulting
GRC International, Inc.
Harris Corporation
Hughes Aircraft
IIT Research Institute
Institute for Computer & Information Sciences
Institute for Defense Analyses
Internal Revenue Service
ITT Aerospace
Lockheed Martin
Merdan Group, Inc.
MITRE Corporation
Mitretek
Motorola
National Center for Supercomputing Applications, Univ. of Illinois
National Institute for Standards and Technology
National Security Agency
Naval Research Laboratory
Navy Command, Control, Operations Support Center Research, Development, Testing & Evaluation Division
Northrop Grumman

continued on next page

Project Participants (cont.)	Office of the Secretary of Defense Oracle Corporation pragma Systems Corporation Predicate Logic, Inc. Rapid Systems Solutions, Inc. San Antonio Air Logistics Center Science Applications International Corporation SPARTA, Inc. Stanford Telecom Systems Research & Applications Tax Modernization Institute The Sachs Groups tOmega Engineering Trusted Information Systems TRW Unisys Government Systems

continued on next page

Acknowledgments, Continued

SSE-CMM Author Group Team Members

The SSE-CMM Author Group has participated in the development of the SSE-CMM since January, 1995. The following are members of the group who have contributed to the development of the model:

Abzug, Charles	Institute for Computer & Information Sciences
Aldrich, Mark	GRC International, Inc.
Bacoyanis, Gus	TRW
Campbell, Chris	Motorola Govt. & Space Technology Group
Casimir, Michael	National Security Agency
Childers, Susy*	Computer Sciences Corporation
Craft, Jim	Systems Research & Applications
DeMello, Jeff	Oracle Corp.
Emery, Patrick*	GRC International, Inc.
Ferraiolo, Karen*	Arca Systems, Inc.
Filsinger, Jarrellann*	Trusted Information Systems
Fowler, Joan*	Data Systems Analysts, Inc.
Hart, Tom	GRC International, Inc.
Heaney, Jody	MITRE Corporation
Hefner, Rick	TRW
Hopkinson, John*	Electronic Warfare Associates - Canada, Ltd.
Hsiao, David	GRC International, Inc.
Lorenz, Natalie*	Booz-Allen & Hamilton
Menk, Chuck*	National Security Agency
Payne, Charles	Secure Computing Corporation
Pearson, Dallas	National Security Agency
Robbins, James	Electronic Warfare Associates - Canada, Ltd.
Rowe, Kenneth*	National Center for Supercomputing Applications, University of Illinois
Sachs, Joel*	The Sachs Groups
Sacksteder, Julie	Merdan Group, Inc.
Schwartz, Robert*	TRW
Shafer, Rob*	Systems Research & Applications
Weiss, Howard*	Sparta, Inc.
West, Charles	Science Applications International Corporation
Wichers, Dave	Arca Systems, Inc.
Williams, Jeff*	Arca Systems, Inc.
Zior, Marcia	National Security Agency

* indicates current Author Group members

continued on next page

SSE-CMM Application Group Team Members

The SSE-CMM Application Group has participated in the development of the SSE-CMM Appraisal Method since January, 1995. The following are members of the group who contributed to the development of the appraisal method:

Bass, Frank	tOmega Engineering
Bratton, Vicky	E-Systems
Casimir, Michael	National Security Agency
Cohen, Aaron	JOTA System Security Consultants, Inc.
DeGrafft, Hart	Sparta, Inc.
Fordham, Mal	IIT Research Institute
Gallagher, Lisa	Computer Sciences Corporation
Gibson, Virgil	Computer Sciences Corporation
Gilmore, Linda	Computer Sciences Corporation
Henning, Ronda	Harris Corporation
Jelen, George	G-J Consulting
Klein, Penny	DISA/CISS
Landoll, Doug	Arca Systems, Inc.
Menk, Chuck	National Security Agency
Monroe, Warren	Hughes Aircraft
Nickel, James	ITT
Niemeyer, Robert	Stanford Telecom
Robbins, James	Electronic Warfare Associates - Canada, Ltd.
Simmons, Marty	Lockheed Martin
Weaver, Gary	Harris Corporation
Zola, Marty	Rapid Systems Solutions, Inc.

continued on next page

SSE-CMM Steering Group Team Members

The SSE-CMM Steering Group has provided oversight and guidance for the SSE-CMM work processes, products, and progress. The following are members of the group:

Adams, John	Trusted Information Systems
Cartier, Gene*	Systems Research & Applications Corp.
Cohen, Aaron*	JOTA System Security Consultants, Inc.
Danner, Bonnie	TRW Government Information Services Division
Dawson, Bill*	BDM International, Inc.
DeGrafft, Hart	Sparta, Inc.
Diggs, Galina	Predicate Logic, Inc.
Gambel, Dan*	Mitretek
George, Bruce*	National Security Agency
Gove, Ron	SAIC
Hefner, Rick*	TRW
Henning, Ronda	Harris Corp.
Jelen, George*	G-J Consulting
Klein, Penny	DISA/CISS
Knode, Ron*	Computer Sciences Corporation
Koepnick, Glenn	San Antonio Air Logistics Center
Lorenz, Natalie	Booz-Allen & Hamilton
Monroe, Warren*	Hughes Aircraft
Robbins, Jim*	Electronic Warfare Associates - Canada, Ltd.
Sachs, Joel*	The Sachs Groups
Schanken, Mary*	National Security Agency
Thompson, Victoria*	Arca Systems, Inc.
Toth, Pat	National Institute of Standards and Technology
Wager, Gene	CPSG/San Antonio Air Force Logistics Center
Weaver, Gary*	Harris Corp.
Wilson, William	Arca Systems, Inc.

* indicates current Steering Group members

continued on next page

Acknowledgments, Continued

Sponsoring Organizations

The authors thank the following for providing sponsorship of the SSE-CMM Project:

Charlie Baggett	National Security Agency
Roger Callahan	Office of the Secretary of Defense
Michael Fleming	National Security Agency
Bill Marshall	National Security Agency
David McKerrow	Communications Security Establishment, Canada
Barbara Valeri	Department of Defense

Other Contributors

The authors thank the many other people who contributed to the success of this effort. These include several expert reviewers who commented on intermediate releases of the model and other SSE-CMM project products as well as those who participated in formal Project Reviews. Their comments and suggestions were important in ensuring the quality and validity of the model and the assessment method. This group includes:

R. Batie (Northrop Grumman); D. Busson (Booz-Allen & Hamilton); K. Cusick (SECAT); B. Danner (TRW); D. Evans (Unisys Govt. Systems); S. Garcia (SEI); L. Gates (NRaD); T. Havighurst (NSA); G. Miller (BDM Federal); W. Pearce (TRW); D. Preston (IIT Research Institute); B. Riski (Hughes Information Technology Systems); M. Shupack (US Navy/SPAWAR); G. Stephens (GTE); S. Welke (IDA): D. Werling (BDM International).

Pilot Appraisals

The authors thank the organizations who assisted in validating the model through the conduct of pilot appraisals. These pilots were crucial in understanding the strengths and weaknesses of earlier drafts of the model, and evaluating the applicability of the model to a diverse set of organizations. We would like to recognize the following organizations for providing input to this version through pilots:

Computer Sciences Corporation
Data General
Government Telecommunication Informatics Service (Canada)
Hughes Aircraft
TRW

Chapter 1 : Introduction

Purpose of this chapter

The purpose of this chapter is to introduce the reader to the document and to the SSE-CMM Project.

In this chapter

The following table provides a guide to the information found in this chapter.

1.1 About this Document

Purpose of this document	This document is designed to acquaint the reader with the SSE-CMM Project as a whole and present the project's major work product - the Systems Security Engineering Capability Maturity Model (SSE-CMM).
Basic organization	This document contains five chapters plus appendices: • Introduction • Overview of the SSE-CMM • Using the SSE-CMM • Capability Levels and Generic Practices • Process Areas and Base Practices • Appendices: Change Request Form, Model Requirements; Bibliography; Glossary; and SE-CMM Project and Organization Process Areas
Chapter 1: Introduction	This chapter provides the document overview and a brief description of the model, the need the model has been designed to meet, and how the initial version has been constructed.
Chapter 2: Overview	This chapter introduces the model, presenting basic concepts that are key to understanding the details of the model. The architecture of the model is presented. Constructs and conventions used in expressing the model are explained to help readers understand the model.
Chapter 3: Using the SSE-CMM	This chapter provides information that will be useful to individuals interested in adopting the model and adapting it to different organizational situations and contexts.
Chapter 4: SSE-CMM Generic Practices	This chapter contains the generic practices which are grouped by capability level. The generic practices (GPs) are used in an assessment to determine the capability of any process.
Chapter 5: SSE-CMM Practices	This chapter presents the base practices (BPs), which are characteristics considered essential to successful security engineering. BPs are grouped into process areas (PAs).

continued on next page

Appendices The appendices include a a change request form, the requirements for the model, a bibliography, a glossary of terms; and the SE-CMM Project and Organization Process Areas.

Related products In addition to this document, the SSE-CMM Project has developed the following work products listed in Table 1-1.

Name	Description
SSE-CMM Appraisal Method Description	Provides a description of the appraisal method developed for use with the SSE-CMM.
SSE-CMM Pilot Appraisal Report	Describes the results of piloting activities for the security engineering community to use as they adopt and work with the SSE-CMM and its associated appraisal method.

Table 1-1. SSE-CMM Work Products

Conventions Within this document the terms "security engineering" and "systems security engineering" are considered synonymous.

1.2 Background

What is the SSE-CMM?

The Systems Security Engineering Capability Maturity Model (SSE-CMM) describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The SSE-CMM does not specify a particular process or sequence, but captures practices generally observed in industry. The model is a standard metric for security engineering practices covering:

- the entire life cycle, including development, operation, maintenance, and decommissioning activities;
- the whole organization, including management, organizational, and engineering activities;
- concurrent interactions with other disciplines, such as system, software, hardware, human factors, and test engineering; system management, operation, and maintenance; and
- interactions with other organizations, including acquisition, system management, certification, accreditation, and evaluation.

The *SSE-CMM Model Description* provides an overall description of the principles and architecture upon which the SSE-CMM is [1]based, an executive overview of the model, suggestions for appropriate use of the model, the practices included in the model, and a description of the attributes of the model. It also includes the requirements used to develop the model.

Proper security engineering is done in context with systems engineering, and where possible, this document attempts to show this inter-relationship. It must be stressed that security engineering is a unique discipline, requiring unique knowledge, skills, and processes which warrants the development of a distinct CMM for security engineering. The architecture, project, and organizational aspects from the SE-CMM have been adopted to form the SSE-CMM model (see chapter 2).

continued on next page

Why was it developed?

Both customers and suppliers are interested in improving the development of security products, systems, and services. The field of security engineering has several well-accepted principles, but it currently lacks a comprehensive framework for evaluating security engineering practices. The SSE-CMM, by identifying such a framework, provides a way to measure and improve performance in the application of security engineering principles.

Modern statistical process control suggests that higher quality products can be produced more cost-effectively by emphasizing the quality of the processes that produce them, and the maturity of the organizational practices inherent in those processes. More efficient processes are warranted, given the increasing cost and time required for the development of secure systems and trusted products. The operation and maintenance of secure systems relies on the processes that link the people and technologies. These interdependencies can be managed more cost effectively by emphasizing the quality of the processes being used, and the maturity of the organizational practices inherent in the processes.

The objective of the SSE-CMM Project is to advance security engineering as a defined, mature, and measurable discipline. The SSE-CMM model and appraisal methods are being developed to enable:

- Selection of appropriately qualified providers of security engineering through differentiating bidders by capability levels and associated programmatic risks;
- Focused investments in security engineering tools, training, process definition, management practices, and improvements by engineering groups; and
- Capability-based assurance, that is, trustworthiness based on confidence in the maturity of an engineering group's security practices and processes.

continued on next page

Why is security engineering important?

With the increasing reliance of society on information, the protection of that information is becoming increasingly important. Many products, systems, and services are needed to maintain and protect information. The focus of security engineering has moved from one of safeguarding classified government data to the wider applications of financial transactions, contractual agreements, personal information, and the Internet. These trends only elevate the future importance of security engineering.

continued on next page

What is the scope of the SSE-CMM?

The scope of the SSE-CMM encompasses the following:

- The SSE-CMM addresses security engineering activities that span the entire trusted product or secure system life cycle, including concept definition, requirements analysis, design, development, integration, installation, operations, maintenance, and decommissioning;
- The SSE-CMM applies to secure product developers, secure system developers and integrators, and organizations that provide security services and security engineering;
- The SSE-CMM applies to all types and sizes of security engineering organizations, such as commercial, government, and academic.

How should it be used?

The SSE-CMM and the method for applying the model (i.e., appraisal method) are intended to be used as a:

- Tool for engineering organizations to evaluate their security engineering practices and define improvements to them.
- Standard mechanism for customers to evaluate a provider's security engineering capability.
- Basis for security engineering evaluation organizations (e.g., system certifiers and product evaluators) to establish organizational capability-based confidences (as an ingredient to system or product security assurance).

The appraisal techniques can be used in applying the model for self improvement and in selecting suppliers, if the users of the model and appraisal methods thoroughly understand the proper application of the model and its inherent limitations. The appraisal process is outlined in Chapter 3. Further description of the appraisal method is documented in the *SSE-CMM Appraisal Method Description* [SSECMM97].

continued on next page

Additional information

Questions, further information, or contacts concerning this model or pilot appraisals using this model can be referred to the SSE-CMM Web Site:

http://www.sse-cmm.org

Data rights associated with the SSE-CMM

The members of the SSE-CMM Project are committed to free use of project materials by the systems engineering, and security engineering communities. Participants have agreed that this and future versions of this document, when released to the public, will retain the concept of free access via a permissive copyright notice. Permission to reproduce this work and to prepare derivative works from this product is granted royalty-free, provided the copyright is included with all reproductions and derivative works.

1.3 About the SSE-CMM Project

Project history

The SSE-CMM initiative began as an NSA-sponsored effort in April 1993 with research into existing work on Capability Maturity Models (CMMs) and investigation of the need for a specialized CMM to address security engineering. During this Conceive Phase, a strawman Security Engineering CMM was developed to seed the effort.

The information security community was invited to participate in the effort at the First Public Security Engineering CMM Workshop in January 1995. Representatives from over 60 organizations reaffirmed the need for such a model. As a result of the community's interest, Project Working Groups were formed at the workshop, initiating the Develop Phase of the effort. The first meetings of the working groups were held in March 1995. Development of the model and appraisal method continued through the work of the SSE-CMM Steering, Author, and Application Working Groups with the first version of the model published in October 1996 and of the appraisal method in April 1997. To validate the model and appraisal method, pilots occurred from June 1996 through June 1997. These pilots provided valuable input to Version 1.1 of the model and appraisal method.

continued on next page

Project organization chart

The SSE-CMM Project progresses through the active participation and corporate investment of the security engineering community, coupled with partial sponsorship by the National Security Agency, the Office of the Secretary of Defense, and the Communications Security Establishment (Canada). The SSE-CMM Project structure, illustrated in Figure 1-1, consists of a Steering Group, Author Group, Application Group, and Key and Community Reviewers.

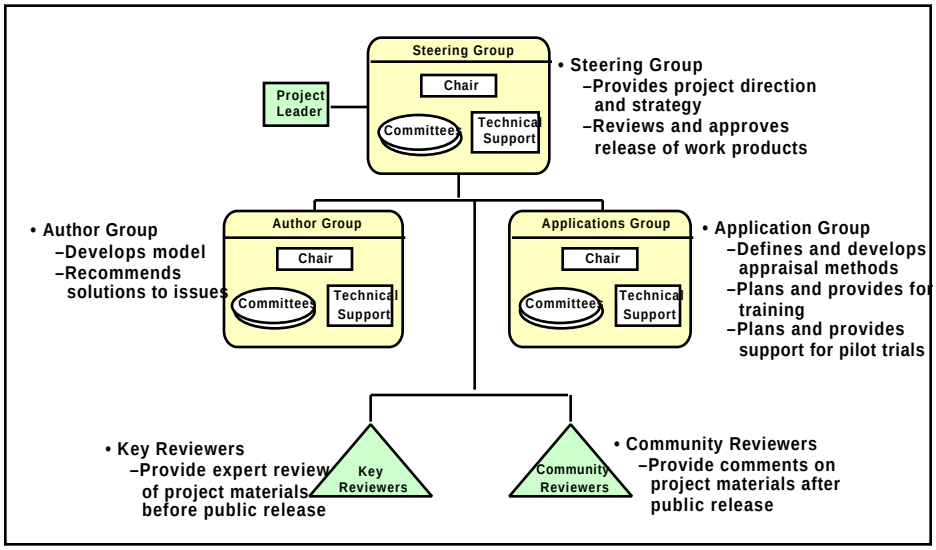

Figure 1-1. SSE-CMM Project Structure

continued on next page

SSE-CMM Project composition

The Steering Group provides oversight and guidance for the SSE-CMM work processes, products, and progress while encouraging the widespread acceptance and adoption of the SSE-CMM.

The Author Group is responsible for evolving the SSE-CMM into a model that can be employed and validated in the security engineering community.

The mission of the Application Group is to develop and validate mechanisms for self-assessment and independent evaluation, training materials and approaches, and oversee pilots of the SSE-CMM.

Key Reviewers make a formal commitment to review and provide timely comments on SSE-CMM Project work products. Community Reviewers may also review work products but without formal commitment.

Member organizations in turn participate by sponsoring participants to support the working groups. The SSE-CMM Project Sponsor, the National Security Agency, with additional support form the Office of the Secretary of Defense and the Communications Security Establishment (Canada), provides funding for technology transfer, project facilitation, and technical support.

Incorporating community feedback

The SSE-CMM was developed by the collaboration of a group of companies with long and successful histories in building secure products and systems, and/or in the provision of secure services. The principal authors are supplemented by Key Reviewers, selected from various backgrounds for their security engineering expertise. The authors also incorporated feedback from the 1st public workshop where an early version of the model was critiqued.

continued on next page

Validating the Model

The initial version of the SSE-CMM was developed with the intention of being applicable to a broad range of organizations including:

- Organizations of varying size and structure.
- Commercial, government, and academic organizations that practice security engineering. and
- Developers/maintainers of secure systems and trusted products as well as service providers.

The first version of the model was used in pilots that appraised two large system integration efforts, two service providers, and a product developer.

The following organizational aspects were considered in piloting and use of the model in order to validate and refine the SSE-CMM:

Size:	Organizations of various sizes.
Focus:	Both contract-driven system development and market-driven product development environments.
Assurance:	Both high and low assurance developments;
Perceived Maturity:	At least one project or organization perceived to have a mature process capability.
Type of Organization:	Both development and service provider organizations.

Chapter 2: Overview of the SSE-CMM

Purpose of this chapter

The purpose of this chapter is to provide an overview of the concepts and constructs used in the SSE-CMM. It provides information on the requirements that led to the design of the SSE-CMM, a description of the architecture, and a section on key concepts and terms which are helpful in understanding the model. It serves as an introduction to the detailed discussion of the model in Chapter 4.

In this chapter

The following table provides a guide to the information found in this chapter.

2.1 Introduction

Introduction

The SSE-CMM provides a community-wide (Government and industry) standard metric to establish and advance security engineering as a mature, measurable discipline. The model and its appraisal methods for management, organization, and engineering practices of security engineering intend that security become an integral part of engineering efforts dealing with hardware, software, systems, or enterprise security issues by defining characteristics of a security engineering process that is explicitly defined, managed, measured, controlled, and effective in all engineering efforts.

2.2 Benefits

Benefits to Engineering Organizations

Engineering organizations include System Integrators, Application Developers, Product Vendors, and Service Providers. Benefits of the SSE-CMM include:

- Savings with less rework from repeatable, predictable processes/practices.
- Credit for true capability to perform, particularly in source selections.
- Focus on measured organizational competency (maturity) and improvements.

Benefits to Acquirers

Acquirers include organizations acquiring systems, products, and services from external/internal sources and end users. Benefits of the SSE-CMM include:

- Re-usable standard Request for Proposal language and evaluation means.
- Reduced risks (performance, cost, schedule) of choosing an unqualified bidder.
- Fewer protests due to uniform assessments based on industry standard.
- Predictable, repeatable level of confidence in product or service.

Benefits to Security Evaluation Organizations

Security evaluation organizations include System Certifiers, System Accreditors, Product Evaluators, and Product Assessors. Benefits of the SSE-CMM include:

- Re-usable process appraisal results, independent of system/product changes.
- Confidence in security engineering and its integration with other disciplines.
- Capability-based confidence in evidence, reducing security evaluation workload.

2.3 Security Engineering

What is Security Engineering?

The drive toward pervasive interconnectivity and interoperability of networks, computers, applications, and even enterprises is creating a more pivotal role for security in all systems and products. The focus of security has moved from safeguarding classified government data, to a wider application, including financial transactions, contractual agreements, personal information, and the Internet. As a result, it is necessary that potential security needs are considered and determined for any application. Examples of needs to consider include confidentiality, integrity, availability, accountability, privacy, and assurance.

The shift in focus of security issues elevates the future importance of security engineering. Security engineering is becoming an increasingly critical discipline and should be a key component in multi-disciplinary, concurrent, engineering teams. This applies to the development, integration, operation, administration, maintenance, and evolution of systems and applications as well as to the development, delivery, and evolution of products. Security concerns must be addressed in the definition, management, and re-engineering of enterprises and business processes. Security engineering can then be delivered in a system, in a product, or as a service.

continued on next page

Definition of Security Engineering

Security engineering is an evolving discipline. A precise definition with community consensus does not exist today. However, pointers as to what security engineering addresses are provided below.
Security engineering, or aspects thereof, attempts to:

- Establish a balanced set of security needs in accordance with identified threats.
- Transform security needs into security guidance to be integrated into the activities of other disciplines employed on a project and into descriptions of a system configuration or operation.
- Establish confidence in the correctness and effectiveness of security mechanisms.
- Judge that operational impacts due to residual security vulnerabilities in a system or its operation are tolerable (acceptable risks).
- Integrate the efforts of all engineering disciplines and specialties into a combined understanding of the trustworthiness of a system.

Types of Security Engineering Organizations

Security engineering activities are practiced by various types of organizations, such as:

- Developers
- Product vendors
- Integrators
- Buyers (acquisition organization or end user)
- Security evaluation organizations (system certifier, product evaluator, or operation accreditor)
- System administrator
- Trusted third parties (certification authority)
- Consulting/service organizations

continued on next page

Security Engineering Life cycle

Security engineering activities are practiced during all life cycle phases, for example:

- Pre-concept
- Concept exploration and definition
- Demonstration and validation
- Engineering, development, and manufacturing
- Production and deployment
- Operations and support
- Disposal

Security Engineering and Other Disciplines

Security engineering activities interface with many other disciplines including:

- Enterprise engineering
- Systems engineering
- Software engineering
- Hardware engineering
- Test engineering
- System administration

Security engineering activities must be coordinated with many external entities because assurance and the acceptability of residual operational impacts are established in conjunction with the developer, integrator, buyer, user, independent evaluator, and other groups. It is these interfaces and the requisite interaction across a broad set of organizations that make security engineering particularly complex and different from other engineering disciplines.

Security Engineering Specialties

Security engineering can draw upon a number of security specialties, for example:

- Operations security
- Information security
- Network security
- Physical security
- Personnel security
- Administrative security
- Communications security
- Emanations security
- Computer security

continued on next page

Assurance

Assurance is defined as the degree of confidence that security needs are satisfied [NIST94a]. It is a very important product of security engineering. There are many forms of assurance. The SSE-CMM contributes to one aspect, the confidence in the repeatable quality of the results from the security engineering process. The basis for this confidence is that a mature organization is more likely to repeat results than an immature organization. The detailed relationship between different forms of assurance is the subject of ongoing research.

Assurance does not add any additional controls to counter risks related to security, but it does provide the confidence that the controls that have been implemented will reduce the anticipated risk.

Assurance can also be viewed as the confidence that the safeguards will function as intended. This confidence derives from the properties of correctness and effectiveness. Correctness is the property that the safeguards, as designed, implement the requirements. Effectiveness is the property that the safeguards provide security adequate to meet the customer's security needs. The strength of the mechanism also plays a part but is moderated by the level of protection and assurance being sought.

Assurance is often stated in terms of a claim, supported by evidence, that a particular assurance level is achieved. The evidence is frequently in the form of documentation developed during the normal course of security engineering activities. The evidence can indicate that the development has followed a well defined and mature engineering process that is subject to continuous improvement. Many of the typical work products included within the PAs will contribute to, or form part of that evidence. Modern statistical process control suggests that higher quality and higher assurance products can be produced more cost effectively and repeatedly by focusing on the process used to produce them. The maturity of the organizational practices will influence and contribute to the process.

continued on next page

Risk

A goal of security engineering is the reduction of risk. Risk is the likelihood that the impact of an unwanted incident will be realized. Associated with that likelihood is a factor of uncertainty, which will vary dependent upon a particular situation. This means that the likelihood can only be predicted within certain limits. In addition, impact assessed for a particular risk also has associated uncertainty as the unwanted incident may not turn out as expected. Thus the majority of factors have uncertainty as to the accuracy of the predictions associated with them. In many cases these uncertainties may be large. This makes planning and the justification of security very difficult.
Anything that can reduce the uncertainty associated with a particular situation is of considerable importance. For this reason, assurance is important as it indirectly reduces the risk of the system.

The unwanted incident is made up of two components: threat and vulnerability. Vulnerabilities are properties of the asset that may be exploited by a threat and include weaknesses. If neither is present there can be no unwanted incident and thus no risk. Risk management is the process of accessing and quantifying risk, and establishing an acceptable level of risk for the organization. It is an important part of the management of security.

continued on next page

Risk (cont.)	Risks are mitigated by the implementation of safeguards, which may address the threat, the vulnerability, the impact, or risk itself. However, it is not feasible to mitigate all risks or completely mitigate all of any particular risk. This is in large part due to the cost of risk mitigation, and to the associated uncertainties. Thus, some residual risk must always be accepted. In the presence of high uncertainty, risk acceptance becomes very problematical due to its inexact nature. One of the few areas under the "risk taker's" control is the uncertainty associated with the system. The SSE-CMM PAs include activities that ensure that the provider organization is analyzing threats, vulnerabilities, impacts, and associated risk.

2.4 Process Improvement

What is process improvement?

Process is a sequence of steps performed for a given purpose. It is the system of tasks, supporting tools, and people involved in the production and evolution of some end result (e.g., product, system). Realizing that process is one of the determinants of product cost, schedule, and quality (the others being people and technology), various engineering communities have started to focus on ways to improve their processes for producing products.

Process capability refers to an organization's potential. It is a range within which an organization is expected to perform. Process performance is the measure of actual results on a particular project which may or may not fall within the range. An example taken from "Out of the Crisis" by W. Edwards Deming illustrates these points:

> In a manufacturing plant, a manager observes problems with a certain production line. All he knew, though, was that people on the line make a lot of defective items. His first inclination might be to plead with the workers to work harder and faster. But instead, he collected data and plotted the percentage of defective items. The plot showed that the number of defective items and the variation from day to day were predictable.

This example illustrates a system that is in statistical process control. That is, the capability is defined by a specific range, and the limits of variation are predictable. There is a stable system for producing defective items. The example illustrates that having a system in statistical process control does not imply the absence of defective items.

However, it does mean that repeating the work in roughly the same way will produce roughly the same results. An important point is that statistical control of a process needs to be established in order to identify where effective improvements can be made. (Many organizations have used CMMs as a guide to assist them in achieving statistical process control.)

continued on next page

What is Process Improvement, continued

Another concept, process maturity, indicates the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Process maturity implies a potential for growth in capability and indicates both the richness of an organization's process and the consistency with which it is applied throughout the organization.

Deming's work with the Japanese applied the concepts of statistical process control to industry [DEM82]. In "Characterizing the Software Process: A Maturity Framework," [HUM88] Watts Humphrey describes a software-process maturity framework that interprets the work of Deming for the software development process. Humphrey asserted that "while there are important differences, these concepts are just as applicable to software as they are to automobiles, cameras, wristwatches, and steel. A software-development process that is under statistical control will produce the desired results within the anticipated limits of cost, schedule, and quality." Applying the concepts of statistical process control to software process, Humphrey describes levels of process maturity which guide organizations in improving their process capability in small, incremental steps. These levels he described form the basis of the SEI (Security Engineering Institute) CMM for Software.

A CMM is a framework for evolving an engineering organization from an ad hoc, less organized, less effective state to a highly structured and highly effective state. Use of such a model is a means for organizations to bring their practices under statistical process control in order to increase their process capability. As a result of applying the CMM for Software, many software organizations have shown favorable results with regard to cost, productivity, schedule, and quality [SEI94]. The SSE-CMM was developed with the anticipation that applying the concepts of statistical process control to security engineering will promote the development of secure systems and trusted products within anticipated limits of cost, schedule, and quality.

continued on next page

Common Misunderstanding 1
"CMMs define the engineering process"

A common misconception is that CMMs define a specific process. CMMs provide guidance for organizations to define their processes and then improve the processes over time. The guidance applies regardless of the particular processes that are performed. CMMs describe WHAT activities must be performed to help define, manage, monitor, and improve the organization's process rather than exactly HOW the specific activities must be performed.

Discipline-specific CMMs, such as the SSE-CMM, require that certain fundamental engineering activities be performed as part of an engineering process for that discipline, but they do not specify exactly how these engineering activities must be performed.

The basic philosophy behind CMMs is to empower engineering organizations to develop and improve an engineering process that is most effective for them. This is based on the ability to define, document, and manage the engineering process, and standardize the process throughout the entire organization. The philosophy is not focused on any specific development life cycle, organizational structure, or engineering techniques.

Common Misunderstanding 2
"CMMs are handbooks or training guides"

CMMs are intended to guide organizations in improving their capability to perform a particular process (for example, security engineering). CMMs are not intended to be handbooks or training guides for helping individuals improve their particular engineering skills. The goal is for an organization to adopt the philosophy described in the CMM and use the techniques defined in the CMM as a guide for defining and improving its engineering process.

continued on next page

Common Misunderstanding 3
"The SSE-CMM is a replacement for product evaluation"

It is unlikely that organizational ratings against a CMM would replace a product evaluation or system certification. But, it could certainly focus the analysis being performed by a third party on areas that have been indicated as weak by the CMM evaluation. Having a process under statistical process control does not mean that there are no defects. Rather, it makes defects more predictable, so some sampling in the form of analysis is still necessary.

Any benefits anticipated from use of the SSE-CMM are based on interpretations of experiences using the SEI CMM for Software. To make claims with regard to the SSE-CMM's contribution to evaluations and certifications, the security engineering community will need to reach consensus on what maturity means for security engineering. As in the SEI CMM for Software, the claims will need to be studied as the SSE-CMM continues to be used within the community.

Common Misunderstanding 4
"Too much documentation is required"

When reading a CMM, it is easy to get overwhelmed by the plethora of implied processes and plans. CMMs include requirements to document processes and procedures and then make sure they are performed as documented. While a number of processes, plans, and other types of documentation are called for in CMMs, it is not intended to dictate the number or type of documents to be developed. The intent of CMMs are to indicate the type of information that is to be documented.

2.5 Applicability of the SSE-CMM

Applicability of the SSE-CMM

The SSE-CMM was designed to be flexible with regard to the type of system or product being developed and operated, or with regard to the context of the service being provided by the target organization. The model was designed for application to organizations that focus on high-level issues (e.g., ones dealing with operational use or system architecture), on low-level issues (e.g., mechanism selection or design), and on organizations that do both. Use of the SSE-CMM should not imply that one focus is better than another or that both are necessary. An organization's business focus should not be biased by use of the SSE-CMM.

Based on the focus of the organization, some, but not all, of the security engineering practices defined will apply. In addition, the organization may need to look at relationships between different practices within the model to determine their applicability. The following examples illustrate how SSE-CMM practices apply to organizations or groups with a specific focus.

Applicability to Risk Assessment

To measure the process capability of an organization that performs risk assessments, several groups of practices come into play. In the case of pre-operation, one would need to assess the organization with regard to its ability to determine and analyze security vulnerabilities and assess the operational impacts. In the operational case, one would need to assess the organization with regard to its ability to monitor the security posture of the system, identify and analyze security vulnerabilities, and assess the operational impacts.

Applicability to Counter-measure Development

In the case of a group that focuses on the development of countermeasures, the process capability of an organization would be characterized by a combination of SSE-CMM practices. The model contains practices to address determining and analyzing security vulnerabilities, assessing operational impacts, and providing input and guidance to other groups involved (such as a software group). The group providing the service of developing countermeasures needs to understand the relationships between these practices.

continued on next page

Applicability to Security Needs For Products	The SSE-CMM includes practices that focus on gaining an understanding of the customer's security needs. Interaction with the customer is required to ascertain them. In the case of a product, the customer is generic as the product is developed a priori independent of a specific customer. When this is the case, the product marketing group or another group can be used as the hypothetical customer, if one is required.

2.6 Relationship to Other Efforts

Relationship to other disciplines and efforts

There are various ongoing efforts that share goals, approaches, and benefits with the SSE-CMM. Table 2.1 describes a representative sampling of these efforts as a comparison to the SSE-CMM. None of these other efforts comprehensively targets the practice of security engineering. This is justification, in part, for a distinct model for security engineering.

While the SSE-CMM is a distinct model to improve and assess security engineering capability, this should not imply that security engineering should be practiced in isolation from other engineering disciplines. On the contrary, the SSE-CMM promotes such integration, taking the view that security is pervasive across all engineering disciplines (e.g., systems, software, hardware) and defining components of the model to address such concerns. The Common Feature "Coordinate Security Practices" recognizes the need to integrate security with all disciplines and groups involved on a project or within an organization. Similarly, the Process Area “Coordinate Security” defines the objectives and mechanisms to be used in coordinating the security engineering activities.

continued on next page

Effort	Goal	Approach	Benefits
Systems Security Engineering CMM	provide mechanism for security engineering process improvement and capability evaluation	continuous maturity model of security engineering practices	improved security engineering process
Systems Engineering CMM	provide mechanism for system or product engineering process improvement	continuous maturity model of systems engineering practices	improved systems engineering process
SEI CMM for Software	provide mechanism for improving management of software development	staged maturity model of software engineering and management practices	improved software development management process
Trusted CMM	provide mechanism for high integrity software development and environment process improvement	staged maturity model of software engineering and management practices including security	improved software development process with security awareness
Trusted Software Development Methodology	levy specific, strict controls on development process and environment to prevent flaws, defects, and malicious code from entering software	set of "trust principles" that apply to the development process and environment	controlled development process and development environment to minimize flaws, defects, and malicious code in high integrity software
INCOSE Systems Engineering Capability Assessment Method	provide mechanism for improving software development and systems engineering interfaces	questionnaire for self assessment of systems engineering practices	improved systems engineering process
Common Criteria	provide mechanism for evaluating security features and assurance evidence	rigorous examination of security relevant design, software, hardware, and other evidence	confidence in enforcement of applicable security policy and encouraged use of trusted products
Generally Accepted Security Principles (GSSP)	define security features, assurances, and practices	standard to be used by security practitioners and against products	uniform use of security principles and identification of practitioner's knowledge
Certification of Information Systems Security Professional	provide mechanism for certification of security professionals	an INFOSEC body of knowledge and certification tests for security practitioners	identification of knowledgeable security practitioners
ISO 9001	provide mechanism for establishing quality management	specific requirements for quality management practices	improved quality assurance processes
Assurance Frameworks	provide a mechanism to allow the combination of alternative assurance sources	framework which allows for reasoning about the methods, artifacts, and concepts involved with producing and analyzing assurance	improved assurance arguments which establish a broad and deep confidence in security.

Table 2-1 — Comparison of the SSE-CMM to Other Efforts.

2.7 Key Concepts of the SSE-CMM

Introduction

Terms and concepts are introduced in this document that have particular meaning within the context of the SSE-CMM. This section elaborates on concepts that are critical to effective understanding, interpretation, and use of the SSE-CMM. Some concepts specific to the model, such as "generic practice" and "base practice," are defined and discussed in the sections of the model description that address them. The concepts to be discussed in this section are:

Organization
Project
System
Work product
Customer
Process
Process area
Role independence
Process capability
Institutionalization
Process management
Capability maturity model

Organizations and projects

Two terms used within the SSE-CMM to differentiate aspects of organizational structure are organization and project. Other constructs such as teams exist within business entities, but there is no commonly accepted terminology that spans all business contexts. These two terms were chosen because they are commonly used/understood by most of the anticipated audience of the SSE-CMM.

continued on next page

Organization

For the purposes of the SSE-CMM, an organization is defined as a unit within a company, the whole company or other entity (e.g., government agency or branch of service), within which many projects are managed as a whole. All projects within an organization typically share common policies at the top of the reporting structure. An organization may consist of co-located or geographically distributed projects and supporting infrastructures.

The term "organization" is used to connote an infrastructure to support common strategic, business, and process-related functions. The infrastructure exists and must be maintained for the business to be effective in producing, delivering, supporting, and marketing its products.

Project

The project is the aggregate of effort and other resources focused on developing and/or maintaining a specific product or providing a service. The product may include hardware, software, and other components. Typically a project has its own funding, cost accounting, and delivery schedule. A project may constitute an organizational entity of its own, or it may be structured as a team, task force, or other entity used by the organization to produce products or provide services.

The process areas in the domain side of the SSE-CMM have been divided into the three categories of engineering, project, and organization. The categories of organization and project are distinguished based on typical ownership. The SSE-CMM differentiates between project and organization categories by defining the project as focused on a specific product, whereas the organization encompasses one or more projects.

continued on next page

System

In the SSE-CMM, system refers to an:

> Integrated composite of people, products, services, and processes that provide a capability to satisfy a need or objective. [MIL-STD-499B]
>
> Assembly of things or parts forming a complex or unitary whole (i.e., a collection of components organized to accomplish a specific function or set of functions).
>
> Interacting combination of elements, viewed in relation to function. [INCOSE 95]

A system may be a product that is hardware only, hardware/software, software only, or a service. The term “system” is used throughout the model to indicate the sum of the products being delivered to the customer(s) or user(s). Denoting a product as a system is an acknowledgment of the need to treat all the elements of the product and their interfaces in a disciplined and systematic way, so as to achieve the overall cost, schedule, and performance (including security) objectives of the business entity developing the product.

Work product

Work products are all the documents, reports, files, data, etc., generated in the course of performing any process. Rather than list individual work products for each process area, the SSE-CMM lists "typical work products" of a particular base practice, to elaborate further the intended scope of a base practice. These lists are illustrative only and reflect a range of organizational and product contexts. They are not to be construed as "mandatory" work products.

continued on next page

Customer

A customer is the individual(s) or entity for whom a product is developed or service is rendered, and/or the individual or entity who uses the product or service.

In the context of the SSE-CMM, a customer may be either negotiated or non-negotiated. A negotiated customer is an individual or entity who contracts with another entity to produce a specific product or set of products according to a set of specifications provided by the customer. A non-negotiated, or market-driven, customer is one of many individuals or business entities who have a real or perceived need for a product. The customer may also be represented by a customer surrogate such as marketing or product focus groups.
In most cases, the SSE-CMM uses the term customer in the singular, as a grammatical convenience. However, the SSE-CMM does not intend to preclude the case of multiple customers.

Note that in the context of the SSE-CMM, the individual or entity using the product or service is also included in the notion of customer. This is relevant in the case of negotiated customers, since the entity to whom the product is delivered is not always the entity or individual who will actually use the product or service. The concept and usage of the term customer in the SSE-CMM is intended to recognize the responsibility of the security engineering function to address the entire concept of customer, which includes the user.

continued on next page

Process

A process is a set of activities performed to achieve a given purpose. Activities may be performed iteratively, recursively, and/or concurrently. Some activities may transform input work products into output work products needed for other activities. The allowable sequence for performing activities is constrained by the availability of input work products and resources, and by management control. A well-defined process includes activities, input and output artifacts of each activity, and mechanisms to control performance of the activities.

Several types of processes are mentioned in the SSE-CMM, including "defined" and "performed" processes. A defined process is formally described for or by an organization for use by its security engineers. This description may be contained, for example, in a document or a process asset library. The defined process is what the organization's security engineers are supposed to do. The performed process is what the security engineers actually do.

Process area

A process area (PA) is a defined set of related security engineering process characteristics, which when performed collectively, can achieve a defined purpose.

A PA is composed of base practices (BPs) are mandatory characteristics that must exist within an implemented security engineering process before an organization can claim satisfaction in a given PA.

Role independence

The process areas of the SSE-CMM are groups of practices, when taken together, achieve a common purpose. But, the groupings are not intended to imply that all base practices of a process are necessarily performed by a single individual or role. All base practices are written in verb-object format (i.e., without a specific subject) so as to minimize the perception that a particular base practice "belongs to" a particular role. This is one way in which the syntax of the model supports the use of it across a wide spectrum of organizational contexts.

continued on next page

Process capability

Process capability is defined as the quantifiable range of expected results that can be achieved by following a process. The SSE-CMM Appraisal Method (SSAM), is based upon statistical process control concepts which define the use of process capability (The appraisal method is further described in Section 3). The SSAM can be used to determine process capability levels for each process area within a project or organization. The capability side of the SSE-CMM reflects these concepts and provides guidance in improving the process capability of the security engineering practices which are referenced in the domain side of the SSE-CMM.

The capability of an organization's process helps to predict the ability of a project to meet goals. Projects in low capability organizations experience wide variations in achieving cost, schedule, functionality, and quality targets. These concepts are further discussed in Chapter 3.

Institution-alization

Institutionalization is the building of infrastructure and corporate culture that establish methods, practices, and procedures, even after those who originally defined them are gone. The process capability side of the SSE-CMM supports institutionalization by providing practices and a path toward quantitative management and continuous improvement. In this way the SSE-CMM asserts that organizations need to explicitly support process definition, management, and improvement. Institutionalization provides a path toward gaining maximum benefit from a process that exhibits sound security engineering characteristics.

Process management

Process management is the set of activities and infrastructures used to predict, evaluate, and control the performance of a process. Process management implies that a process is defined (since one cannot predict or control something that is undefined). The focus on process management implies that a project or organization takes into account both product- and process-related factors in planning, performance, evaluation, monitoring, and corrective action.

continued on next page

Capability maturity model

A capability maturity model (CMM) such as the SSE-CMM describes the stages through which processes progress as they are defined, implemented, and improved. The model provides a guide for selecting process improvement strategies by determining the current capabilities of specific processes and identifying the issues most critical to quality and process improvement within a particular domain. A CMM may take the form of a reference model to be used as a guide for developing and improving a mature and defined process.

A CMM may also be used to appraise the existence and institutionalization of a defined process that implements referenced practices. A capability maturity model covers the processes used to perform the tasks of the specified domain, (e.g., security engineering). A CMM can also cover processes used to ensure effective development and use of human resources, as well as the insertion of appropriate technology into products and tools used to produce them. The latter aspects have not yet been elaborated for security engineering.

2.8 SSE-CMM Architecture Description

Introduction

The SSE-CMM consists of a set of practices that have been grouped into two “aspects”. This architecture was adopted from the Systems Engineering CMM (SE-CMM) which was, in turn, closely based on the SPICE Project Baseline Practices Guide. This approach was deemed particularly applicable to the SSE-CMM because it clearly separates basic characteristics of the security engineering process (domain aspect) from process management and institutionalization characteristics of the systems engineering process (capability aspect).

Capability Aspect

The “capability aspect” consists of “generic practices” (GP) that are related to overall process management and institutionalization capability. This aspect is used during an appraisal to determine how well an organization performs the practices in the domain aspect. The capability aspect is discussed in detail later in this section.

The SSE-CMM groups process capability into the three tiers of capability levels, common features, and generic practices. The capability levels indicate increasing levels of process maturity and are composed of one or more common features. Each common feature is further detailed by several generic practices. The three components of the capability aspect are illustrated in Figure 2.1.

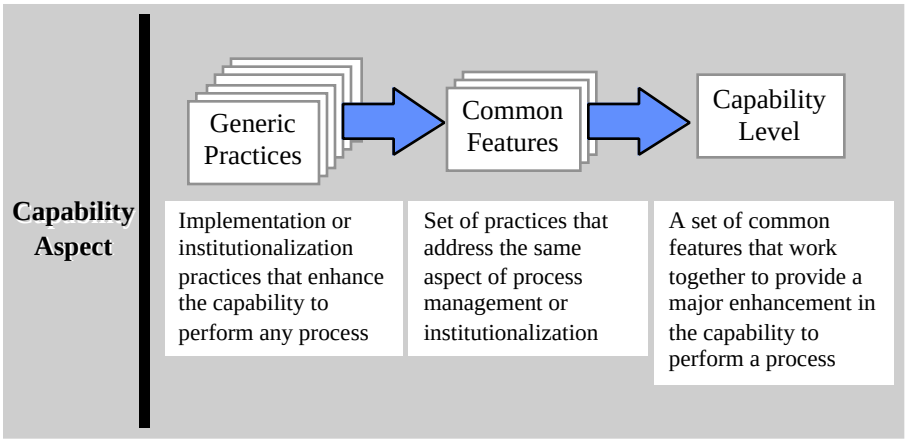

Figure 2.1 — The capability aspect has three components.

continued on next page

Domain Aspect

The "domain aspect" consists of "base practices" (BP) that are specific to security engineering. For example, BP.02.03 (see chapter 5) is "Identify alternative solutions to security related engineering problems." In an appraisal, this aspect is used to determine the practices that an organization performs. The domain aspect is discussed in detail later in this section. The three components of the domain aspect are illustrated in Figure 2.2.

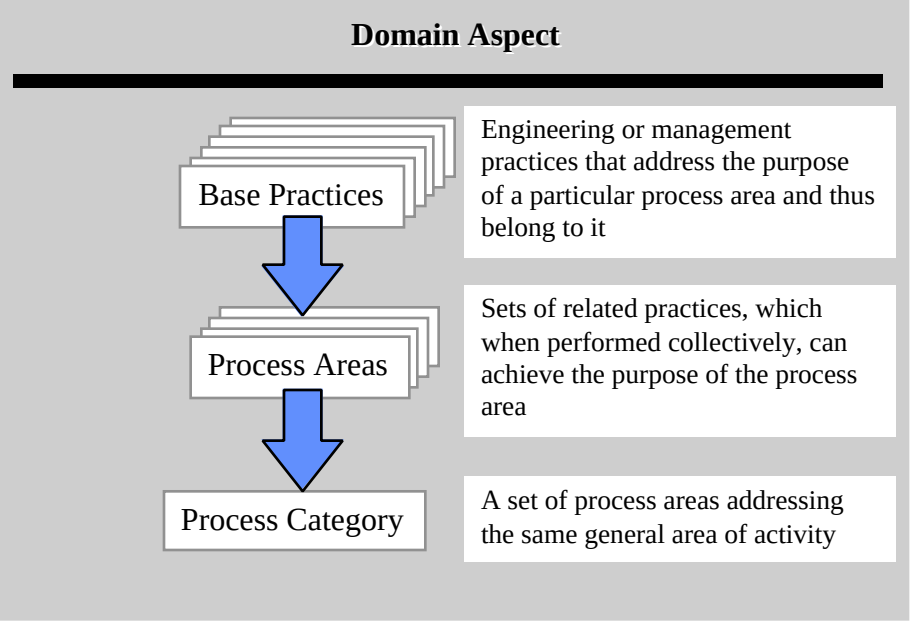

Figure 2.2 — The domain aspect has three components.

continued on next page

Appraisal

An appraisal determines an organization's capability to perform each part of the domain. In practice, this means that each PA is evaluated against each of the generic practices to determine a capability level. The SSE-CMM architecture is illustrated in Figure 2.3 showing how a profile can be created to represent an organization's capability in each of the process areas.

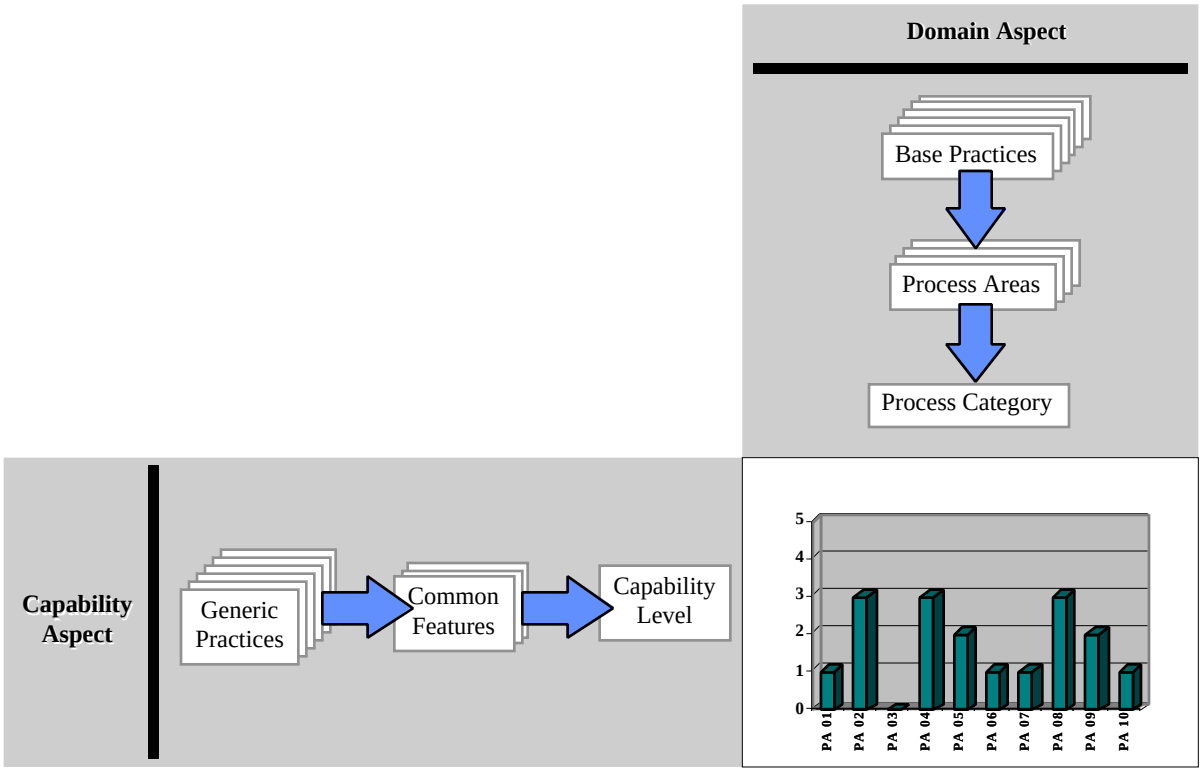

Figure 2.3 — The SSE CMM measures the capability of an organization performing activities in the security engineering domain.

2.9 Capability Aspect of the SSE-CMM

Introduction

The capability aspect of the SSE-CMM measures the capability of an organization to perform security engineering activities. The SSE-CMM groups process capability in the three tiers of capability levels, common features, and generic practices. The capability levels indicate increasing levels of process maturity and are composed of one or more common features. Each common feature is further detailed by several generic practices. Figure 2.4 illustrates this relationship.

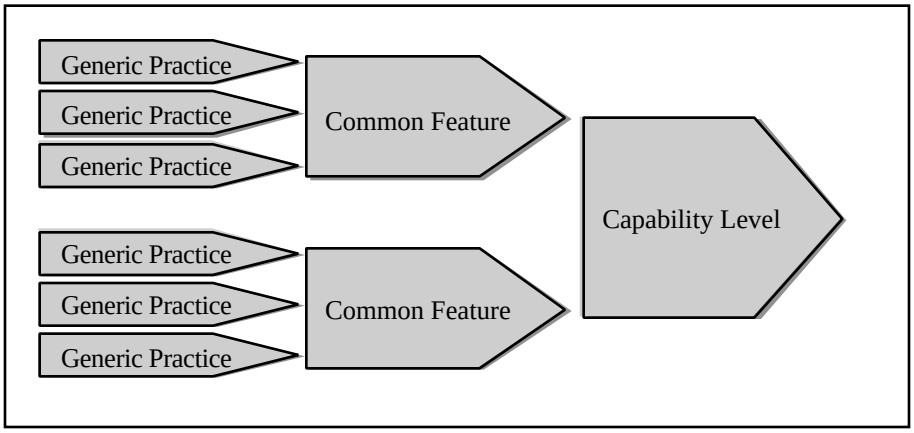

Figure 2.4 — Capability levels consist of common features, which consist of generic practices.

The common features are designed to describe major shifts in an organization's characteristic manner of performing work processes (in this case, the security engineering domain). Each common feature has one or more generic practices. With one exception, the generic practices can be applied to each of the process areas (from the domain side of the SSE-CMM) in addition to the basic performance of the practice. The one exception is the first common feature, "Base practices are performed."

Subsequent common features have generic practices that help determine how well a project manages and improves each process area as a whole. The generic practices, described in Chapter 4A, are grouped to emphasize any major shift in an organization's characteristic manner of doing security engineering.

continued on next page

Why group common features by capability level?

There is more than one way to group practices into common features and common features into capability levels. The following discussion addresses these common features.

The ordering of the common features stems from the observation that implementation and institutionalization of some practices benefit from the presence of others. This is especially true if practices are well established. Before an organization can define, tailor, and use a process effectively, individual projects should have some experience managing the performance of that process. Before institutionalizing a specific estimation process for an entire organization, for example, an organization should first attempt to use the estimation process on a project. However, some aspects of process implementation and institutionalization should be considered together (not one ordered before the other) since they work together toward enhancing capability.

Common features and capability levels are important both in performing an assessment and improving an organization's process capability. In the case of an assessment where an organization has some, but not all common features implemented at a particular capability level for a particular process, the organization usually is operating at the lowest completed capability level for that process. For example, at capability level 2, if the Tracking Performance common feature is lacking, it will be difficult to track project performance. An organization may not reap the full benefit of having implemented a common feature if it is in place, but not all common features at lower capability levels. An assessment team should take this into account in assessing an organization's individual processes.

continued on next page

Why group common features by capability level? (cont.)

In the case of improvement, organizing the practices into capability levels provides an organization with an "improvement road map," should it desire to enhance its capability for a specific process. For these reasons, the practices in the SSE-CMM are grouped into common features which are ordered by capability levels.

An assessment should be performed to determine the capability levels for each of the process areas. This indicates that different process areas can and probably will exist at different levels of capability. The organization will then be able to use this process-specific information as a means to focus improvements to its processes. The priority and sequence of the organization's activities to improve its processes should take into account its business goals.

continued on next page

SSE-CMM Capability Levels

The SSE-CMM has defined six levels of process capability. Figure 2.5 lists the capability levels and common features of the capability aspect of the SSE-CMM.

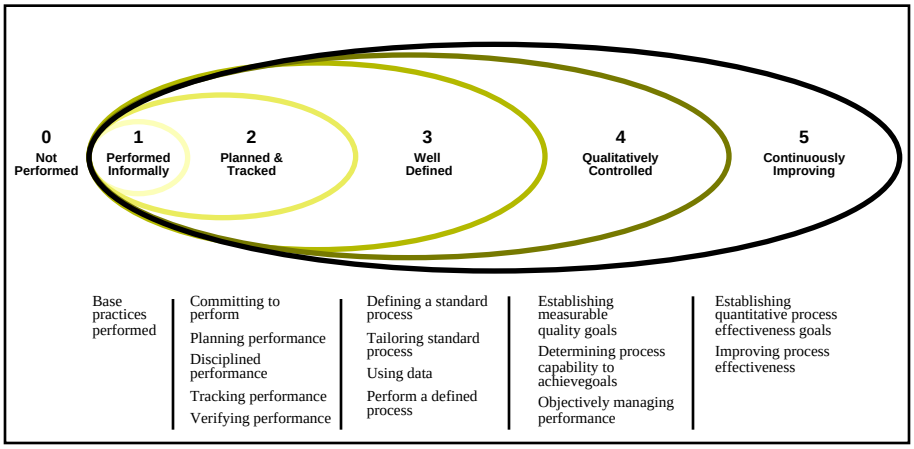

Figure 2.5 — Capability levels represent the maturity level of a security engineering organization.

Level 0: Not Performed

The Not Performed level (Level 0) displays no common features. It is characteristic of an organization just entering the security engineering field, or one that has not focused on the systematic application of security engineering principles in their product development. They accomplish some of the tasks, but are not necessarily sure how. Performance is not generally consistent, particularly if key individuals are absent or the tasks become more complex.

Level 1: Performed Informally

At this level, all base practices are performed somewhere in the project's or organization's implemented process. However, consistent planning and tracking of that performance is missing. Good performance, therefore, depends on individual knowledge and effort. Work products are generally adequate, but quality and efficiency of production depend on how well individuals within the organization perceive that tasks should be performed. Based on experience, there is general assurance that an action will be performed adequately when required. However, the capability to perform an activity is not generally repeatable or transferable.

continued on next page

Level 2: Planned & Tracked	At the Planned and Tracked level, planning and tracking are introduced. There is general recognition that the organization's performance is dependent on how efficiently the security engineering base practices are implemented within a project's or organization's process. Therefore, work products related to base practice implementation are periodically reviewed and placed under version control. Corrective action is taken when indicated by variances in work products. The primary distinction between the Performed Informally and the Planned and Tracked levels is that at the latter level, the execution of base practices in the project's implemented process is planned and managed. Therefore, it is repeatable within the implementing project, though not necessarily transferable across the organization.
Level 3: Well Defined	At this level, base practices are performed throughout the organization via the use of approved, tailored versions of standard, documented processes. Data from using the process are gathered and used to determine if the process should be modified or improved. This information is used in planning and managing the day-to-day execution of multiple projects within the organization and is used for short- and long-term process improvement. The main difference between the Planned and Tracked and Well Defined levels is the use of organization-wide, accepted standard processes, that implement the characteristics exhibited by the base practices. The capability to perform an activity is, therefore, directly transferable to new projects within the organization.
Level 4: Quantitatively Controlled	At the Quantitatively Controlled level, measurable process goals are established for each defined process and associated work products, and detailed measures of performance are collected and analyzed. These data enable quantitative understanding of the process and an improved ability to predict performance. Performance, then, is objectively managed and defects are selectively identified and corrected.

continued on next page

Level 5: Continuously Improving	This is the highest achievement level from the viewpoint of process capability. The organization has established quantitative, as well as qualitative, goals for process effectiveness and efficiency, based on long-range business strategies and goals. Continuous process improvement toward achievement of these goals using timely, quantitative performance feedback has been established. Further enhancements are achieved by pilot testing of innovative ideas and planned insertion of new technology.

2.10 Domain Aspect of the SSE-CMM

Domain Aspect of the SSE-CMM

The SSE-CMM characterizes the security engineering domain by using process areas. Each process area is further detailed by several base practices and explanatory notes. There are 21 process areas, grouped into the three process categories of engineering, project, and organization.

The process areas are designed to describe the major topic areas essential to effective security engineering within an organization. In your home organization, your process will include base practices from the process areas that are executed by (or primarily by) individuals in the role of security engineers. These are the practices primarily grouped in the engineering category. Other process areas may be included in processes that are executed by people who are performing other roles. These are the project and organization process areas, which can also be thought of as support process areas.

continued on next page

Domain Aspect of the SSE-CMM (cont.)

The authors included support process areas in the SSE-CMM because effective security engineering is unlikely unless these support tasks are performed. For example, it is unlikely that effective security engineering will be executed if no one ensures that all the engineering staff is working to the same requirement and design baselines at a given period in time (an aspect of the Manage Configurations process area).

The point of the SSE-CMM is not to indicate "who" does the kinds of things described in a particular process area, but to indicate that the work needs to be performed by someone regardless of their role. Figure 2.6 illustrates that process area categories are made up of process areas which are composed of base practices.

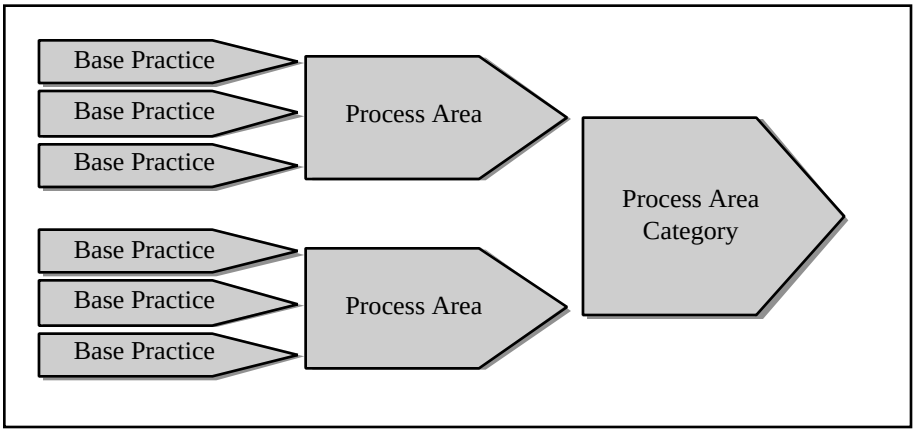

Figure 2.6 — Base practices are grouped into process areas, which are grouped into categories.

continued on next page

Process areas of the domain aspect

Table 2.2 lists the SSE-CMM process areas. The Engineering process areas that have been developed for the SSE-CMM are listed in the first column. The Project and Organizational PAs that were adopted from the SE-CMM, and interpreted for security engineering, are in the second and third columns. To emphasize that the SSE-CMM does not prescribe a specific process or sequence, the process areas are arranged alphabetically by title within each group.

Engineering PAs	Project PAs	Organizational PAs
Administer Security Controls	Ensure Quality	Coordinate with Suppliers
Assess Operational Security Risk	Manage Configurations	Define Organization's Security Engineering Process
Attack Security	Manage Program Risk	Improve Organization's Security Engineering Processes
Build Assurance Argument	Monitor and Control Technical Effort	Manage Security Product Line Evolution
Coordinate Security	Plan Technical Effort	Manage Security Engineering Support Environment
Determine Security Vulnerabilities		Provide Ongoing Knowledge and Skills
Monitor System Security Posture		
Provide Security Input		
Specify Security Needs		
Verify and Validate Security		

Table 2.2 — The domain aspect of the SSE-CMM consists of engineering, project, and organizational PAs.

continued on next page

Base practice selection

Identifying the set of security engineering base practices is complicated by the many different names for activities that are essentially the same. Some of these activities occur later in the life cycle, at a different level of abstraction, or are typically performed by individuals in different roles. The SSE-CMM ignores these distinctions and identifies practices that are essential to the practice of good security engineering.
The following criteria express the requirements derived for base practices:

- The base practice should apply across the life cycle.
- Overlap between the base practices should be minimized.
- A base practice should not be in the model if it is the state-of -the-art.
- Base practices should be applicable using multiple methods in multiple business contexts. They should not specify a particular method or tool.

Process area selection

Independent of how the base practices were identified, there are a large number of possible ways to group them into process areas. Some strategies try to model the real world and others try to model the ideal practice of security engineering. The SSE-CMM compromises between these competing goals in the current set of process areas.
The following criteria express the requirements derived for process areas:

- Process areas should assemble related activities in one area for ease of use.
- Process areas should be related to valuable security engineering services.
- Process areas should not be tied to a particular life cycle phase.
- Process areas should be implementable in multiple organization and product contexts.
- Process areas are generally improvable as a distinct process.
- Process areas are generally improvable by a group with similar interests in the process.
- Process areas include all base practices that are required to meet the goals of the process area.

continued on next page

Relationship between generic and base practices	The SSE-CMM may appear to contain a certain amount of redundancy between the generic practices and base practices. This is because process capability levels are primarily determined by applying the generic practices to the base practices. This is most visible when looking at some of the project and organizational process areas.
Example of relationship between generic/base practices	The SSE-CMM contains both base practices and a generic practice that address security coordination in the Coordinate Security process area (PA09) and the generic practices within Common Feature 3.3 (Coordinate Security Practices). The focus of Coordinate Security is the *process* being used for coordinating security engineering activities. The generic practice, however, addresses whether a project's process for coordinating security results in coordination with various entities (i.e., within the security engineering activities, with other engineering disciplines, and with external organizations).

2.11 Process Area Summaries

Security Engineering Process Areas	The security engineering category groups together those process areas that are primarily concerned with meeting customer security needs.
Administer Security Controls	1. Establish security responsibilities 2. Manage security configuration 3. Manage security awareness, training, and education programs 4. Manage security services and control mechanisms
Assess Operational Security Risk	1. Select risk analysis method 2. Prioritize operational capabilities and assets 3. Identify threats 4. Assess operational impacts
Attack Security	1. Scope attack 2. Develop attack scenarios 3. Perform attacks 4. Synthesize attack results
Build Assurance Argument	1. Identify assurance objectives 2. Define assurance strategy 3. Control assurance evidence 4. Analyze evidence 5. Provide assurance argument
Coordinate Security	1. Define coordination objectives 2. Identify coordination mechanisms 3. Facilitate coordination 4. Coordinate security decisions and recommendations
Determine Security Vulnerabil-ities	1. Select vulnerability analysis method 2. Analyze system assets 3. Identify threats 4. Identify vulnerabilities 5. Synthesize system vulnerability
Monitor System Security Posture	1. Analyze event records 2. Monitor changes 3. Identify security incidents 4. Monitor security safeguards 5. Review security posture 6. Manage security incident response 7. Protect security monitoring artifacts
Provide Security Input	1. Understand security input needs 2. Determine constraints and considerations 3. Identify security alternatives 4. Analyze security of engineering alternatives 5. Provide security engineering guidance 6. Provide operational security guidance
Specify Security Needs	1. Gain an understanding of customer security needs 2. Identify applicable laws, policies, standards, and constraints 3. Identify system security context 4. Capture security view of system operation 5. Capture security high-level goals 6. Define security related requirements 7. Obtain agreement on security
Verify and Validate Security	1. Identify verification and validation targets 2. Define verification and validation approach 3. Perform verification 4. Perform validation 5. Provide verification and validation results

Project Process Areas	The project category groups together those process areas that are primarily concerned with improving project capability. They are organized alphabetically within the category to discourage the reader from implying a particular sequencing of the process areas.
Ensure Quality	1. Monitor conformance to the defined process 2. Measure work product quality 3. Measure quality of the process 4. Analyze quality measurements 5. Obtain participation 6. Initiate quality improvement activities 7. Detect need for corrective actions
Manage Configura-tions	1. Establish configuration management methodology 2. Identify configuration units 3. Maintain work product baselines 4. Control changes 5. Communicate configuration status
Manage Program Risk	1. Develop risk management approach 2. Identify risks 3. Assess risks 4. Review risk assessment 5. Execute risk mitigation 6. Track risk mitigation
Monitor and Control Technical Effort	1. Direct technical effort 2. Track project resources 3. Track technical parameters 4. Review project performance 5. Analyze project issues 6. Take corrective action
Plan Technical Effort	1. Identify critical resources 2. Estimate project scope 3. Develop cost estimates 4. Determine project's process 5. Identify technical activities 6. Define project interface 7. Develop project schedules 8. Establish technical parameters 9. Develop technical management plan 10. Review and approve project plans

Organization Process Areas	The organization category groups together process areas that are primarily concerned with the improvement of the organization overall.
Coordinate With Suppliers	1. Identify systems components or services 2. Identify competent suppliers or vendors 3. Choose suppliers or vendors 4. Provide expectations 5. Maintain communications
Define Organization's Security Engineering Process	1. Establish process goals 2. Collect process assets 3. Develop organization's security engineering process 4. Define tailoring guidelines
Improve Organization's Security Engineering Processes	1. Appraise the process 2. Plan process improvements 3. Change the standard process 4. Communicate process improvements
Manage Product Line Evolution	1. Define product evolution 2. Identify new product technologies 3. Adapt development processes 4. Ensure critical components availability 5. Insert product technology
Manage Security Engineering Support Environment	1. Maintain technical awareness 2. Determine support requirements 3. Obtain engineering support environment 4. Tailor engineering support environment 5. Insert new technology 6. Maintain environment 7. Monitor engineering support environment
Provide Ongoing Skills And Knowledge	1. Identify training needs 2. Select mode of knowledge or skill acquisition 3. Assure availability of skill and knowledge 4. Prepare training materials 5. Train personnel 6. Assess training effectiveness 7. Maintain training records 8. Maintain training materials

Chapter 3: Using the SSE-CMM

Introduction

This chapter provides information on using the SSE-CMM for organizational process improvement and design.

In this chapter

3.1 Many Usage Contexts

Product/ project context

Practitioners in security engineering recognize that the product contexts and the methods used to accomplish product development are as varied as the products themselves. However, there are some issues related to product and project context that are known to have an impact on the way products are conceived, produced, delivered, and maintained. The following issues in particular have significance for the SSE-CMM:

1. Type of customer base (products, systems, or services).
2. Assurance requirements (high vs. low).
3. Support for both development and operational organizations.

The differences between two diverse customer bases, differing degrees of assurance requirements, and the impacts of each of these differences in the SSE-CMM are discussed below. These are provided as an example of how an organization or industry segment might determine appropriate use of the SSE-CMM in their environment.

SSE-CMM not limited to a particular industry segment

Every industry reflects its own particular culture, terminology, and communication style. By minimizing the role dependencies and organization structure implications, it is anticipated that the SSE-CMM concepts can be easily translated by all industry segments into their own language and culture.

continued on next page

SSE-CMM Use

There are two major ways that the SSE-CMM is intended to be used:

Independent capability evaluation involves an acquisition organization that wants to understand the security engineering process capability of organizations that are potential participants on a project.

Self-appraisal involves a security engineering organization that wants to get an idea about their own level of security engineering process capability to use for process improvement purposes.

SSE-CMM Appraisal Scenarios

The SSE-CMM was developed using the same structure of the SE-CMM because of the recognition that security engineering is sometimes practiced within the context of systems engineering (e.g., large system integrators). It is also recognized that security engineering service providers may perform security engineering activities as separate activities coordinated with a separate systems or software (or other) engineering effort. These two scenarios were motivation to determine the following different ways in which the SSE-CMM could be used with the SE-CMM:

After a SE-CMM appraisal, the SSE-CMM appraisal can focus on the security engineering processes within the organization.

When performed in conjunction with an SE-CMM appraisal, the SSE-CMM appraisal can be tailored to integrate with the SE-CMM.

When performed independent of an SE-CMM appraisal, the SSE-CMM appraisal will have to look beyond security to see if the appropriate project and organizational foundation is in place to support a security engineering process.

continued on next page

3.2 Using the SSE-CMM to Support Appraisal

Introduction

The SSE-CMM is structured to support a wide variety of improvement activities, including self-administered appraisals, or internal appraisals augmented by expert "facilitators" from inside or outside the organization. Although it is primarily intended for internal process improvement, the SSE-CMM can also be used to evaluate a potential vendor's capability to perform its security engineering process. This is in contrast to the SE-CMM which does not recommend its model be used for capability evaluations, the SSE-CMM project does intend that the SSE-CMM model be used in such evaluations.

The SSE-CMM Appraisal Method

It is not required that any particular appraisal method be used with the SSE-CMM. However, an appraisal method designed to maximize the utility of the model has been designed by the SSE-CMM Project. The SSE-CMM Appraisal Method (SSAM) is fully described, along with some support materials for conducting appraisals, in *SSE-CMM Appraisal Method Description* [SSECMM97]. The basic premises of the appraisal method are listed in this document to provide context for how the model might be used in an appraisal.

The SSE-CMM Application Group is considering ways to augment the SSAM to support anticipated use of the SSE-CMM in capability evaluations by many methods, including for example, requiring demonstration of evidence.

continued on next page

Features of the SSAM

The SSAM is an organizational or project-level appraisal method that uses multiple data-gathering methods to obtain information on the processes being practiced within the organization or project selected for appraisal. The purposes of a SSAM-style appraisal in its first release version are to:

- Obtain a baseline or benchmark of actual practice related to security engineering within the organization or project.
- Create and support momentum for improvement within multiple levels of the organizational structure.

The SSAM is a method which is tailorable to meet the organization's or project's need. Some guidance on tailoring is provided in the SSAM description document.

Data gathering consists of 1) questionnaires that directly reflect the contents of the model, 2) a series of structured and unstructured interviews with key personnel involved in the performance of the organization's processes, and 3) review of security engineering evidence generated. Individuals involved may not have a formal title of "security engineer," but the SSE-CMM does not require such roles. The SSE-CMM applies to those who have the responsibility for executing security engineering activities.

Multiple feedback sessions are conducted with the appraisal participants. This is culminated in a briefing to all participants plus the sponsor of the appraisal. The briefing includes capability levels determined for each of the process areas appraised. It also includes a set of prioritized strengths and weaknesses that support process improvement based on the organization's stated appraisal goals.

continued on next page

SSAM overview

There are several steps involved in a SSAM appraisal. This list is an overview of those steps, which are described in detail in the SSAM itself.

1. Preparation - During the preparation phase, a sponsor commitment is obtained and the details of the appraisal are negotiated.

2. On Site - During the on-site phase, a team of both internal and external appraisers will conduct an opening meeting and familiarize all members of the team with the appraisal process. The questionnaire results are analyzed and detailed interviews with security engineering leads are conducted. This information is analyzed and a set of findings and a rating profile are produced and presented.

3. Post-Appraisal - After the appraisal, the team will report lessons learned and report the appraisal output to other parties, if authorized by the sponsor.

continued on next page

Determine capability to perform security engineering processes

Figure 3-1 illustrates how the process areas (base practices) and the common features (generic practices) can be used to determine the process capability of security engineering processes. A capability level of 0 to 5 can be determined for each process area.

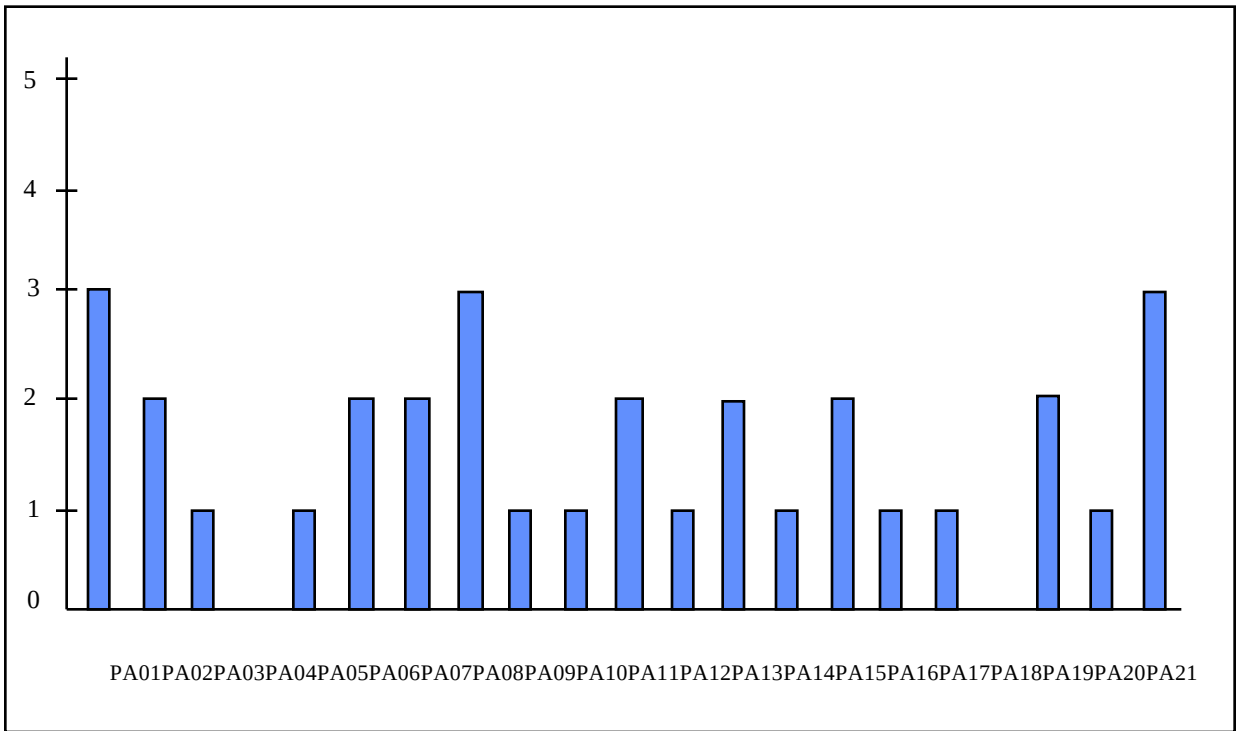

Figure 3-1. Determining Process Capability

continued on next page

Defining security engineering context for appraisal

The first step in assessing an organization is to determine the context within which security engineering is practiced in the organization. Security engineering can be practiced in any engineering context, particularly in the context of systems, software, and communications engineering. The SSE-CMM is intended to be applicable in all contexts. Determination of the context needs to be made in order to decide:

1) Which PAs are applicable to the organization.
2) How the PAs may need to be interpreted (for example, development vs. operational environment).
3) Which personnel need to be involved in the assessment.

Note again that the SSE-CMM does not imply the existence of a separately defined security engineering organization. The intent is to focus on those in the organization who have the responsibility for executing security engineering tasks.

continued on next page

Using both sides of the architecture in appraisal

The first step in developing a profile of an organization's capability to perform its security engineering processes is to determine whether the basic security engineering processes (all the base practices) are *implemented* within the organization (not just written down) via their performed processes. The second step is to assess how well the characteristics (base practices) of the processes that have been implemented are managed and institutionalized by looking at the base practices in the context of the generic practices. Consideration of both the base practices and generic practices in this way results in a process capability profile that can help the organization to determine the improvement activities that will be of most benefit in the context of its business goals.

In general the appraisal consists of evaluating each process area against the generic practices. The base practices should be viewed as guidance on the basic aspects of the topics that need to be addressed. The related generic practices deal with deployment of the base practices to the project. Keep in mind that the application of the generic practices to each process area results in a unique interpretation of the generic practice for the subject process area.

Sequencing

The practices of many of the process areas would be expected to be seen a number of times in the execution of an organization's processes for the life cycle of a project. The process areas should be considered a source for practices whenever there is a need to incorporate the purpose of a process area in a project's or organization's process. In an appraisal, always keep in mind that the SSE-CMM does not imply a sequence. Sequencing should be determined based on an organization's or project's selected life cycle and other business parameters (see Section 3.4, Using the SSE-CMM in Process Design).

3.3 Using the SSE-CMM to Support Process Improvement

Introduction	Any process improvement effort, using any reference model, should be constructed to support the business goals of an organization. An organization using the SSE-CMM should prioritize the process areas relative to their business goals and strive for improvement in the highest priority process areas first.
Tailoring	The model defines those elements that were considered to be essential for the practice of security engineering. However, not all projects may need to use processes that exhibit all the characteristics associated with each process area. Under such circumstances, the project should follow a process to tailor out the activity related to the unnecessary process area from an organization's security engineering process. Tailoring should, in all cases, be based on the organization's goals and customer needs. Note that the tailoring is intended to be done at the PA level. The PAs were written with the intention that all base practices need to be in place in order to meet the goals of the PA.

continued on next page

Process Improvement Principles

The business goals are the primary driver in interpreting a model such as the SSE-CMM. But, there is a fundamental order of activities and basic principles that drive the logical sequence of typical improvement efforts. This order of activities is expressed in the common features and generic practices of the capability level side of the SSE-CMM architecture. These principles and order of activities are summarized in Table 3-3.

Principle	How Expressed in SSE-CMM
You have to do it before you can manage it.	The Performed Informally level focuses on whether an organization or project performs a process that incorporates the base practices.
Understand what's happening on the project (where the products are!) before defining organization-wide processes.	The Planned and Tracked level focuses on project-level definition, planning, and performance issues.
Use the best of what you've learned from your projects to create organization-wide processes.	The Well Defined level focuses on disciplined tailoring from defined processes at the organization level.
You can't measure it until you know what "it" is.	Although it is essential to begin collecting and using basic project measures early (i.e., at the Planned and Tracked level). Measurement and use of data is not expected organization wide until the Well Defined and particularly the Quantitatively Controlled levels have been achieved.
Managing with measurement is only meaningful when you're measuring the right things.	The Quantitatively Controlled level focuses on measurements being tied to the business goals of the organization.
A culture of continuous improvement requires a foundation of sound management practice, defined processes, and measurable goals.	The Continuously Improving level gains leverage from all the management practice improvements seen in the earlier levels, then emphasizes the cultural shifts that will sustain the gains made.

Table 3-3. Process Improvement Principles in the SSE-CMM

continued on next page

Some expected results	Based on analogies in the software and other communities, some results of process and product improvement can be predicted. These are discussed below.
Improving predictability	The first improvement expected as an organization matures is *predictability*. As capability increases, the difference between targeted results and actual results decreases across projects. For instance, Level 1 organizations often miss their originally scheduled delivery dates by a wide margin, whereas organizations at a higher capability level should be able to predict the outcome of cost and schedule aspects of a project with increased accuracy.
Improving control	The second improvement expected as an organization matures is *control.* As process capability increases, incremental results can be used to establish revised targets more accurately. Alternative corrective actions can be evaluated based on experience with the process and other projects process results in order to select the best application of control measures. As a result, organizations with a higher capability level will be more effective in controlling performance within an acceptable range.
Improving process effectiveness	The third improvement expected as an organization matures is *process effectiveness*. Targeted results improve as the maturity of the organization increases. As an organization matures, costs decrease, development time becomes shorter, and productivity and quality increase. In a Level 1 organization, development time can be quite long because of the amount of rework that must be performed to correct mistakes. In contrast, organizations at a higher maturity level can obtain shortened overall development times via increased process effectiveness and reduction of costly rework.

3.4 Using the SSE-CMM in Process Design

Introduction

This section provides brief guidance on issues related to using the SSE-CMM to support process design. The guidance sets a context for how the SSE-CMM could be used in a security engineering process design activity.

Analyzing your organizational context

Organizations often overlook many internal and/or intermediate processes or products when first defining their processes. However, it is not necessary to address all of the possibilities when first defining a security engineering process for an organization. An organization should describe with reasonable accuracy its current process as a baseline. It is best to focus on capturing a reasonable baseline process that be produced in six months to a year, and one that can be improved over time.

Organizations must have a stable baseline to determine whether future changes constitute improvements. There is no value in looking for improvements in a process that the organization does not perform. An organization may find it useful to include current "delays" and "queues" in the baseline process. During subsequent process improvement efforts, these allow a good starting point for cycle-time reduction.

A security engineering organization may define its process from the point of view of what its engineers are responsible for. This may include interfaces with the implementing disciplines of systems engineering, software engineering, hardware engineering, as well as others.

continued on next page

Analyzing your organizational context (cont.)

The first step in designing processes that will meet the business needs of an enterprise is to understand the business, product, and organizational context that will be present when the process is being implemented. Some questions that need to be answered before the SSE-CMM can be used for process design include:

- How is security engineering practiced within the organization?
- What life cycle will be used as a framework for this process?
- How is the organization structured to support projects?
- How are support functions handled (e.g., by the project or the organization)?
- What are the management and practitioner roles used in this organization?
- How critical are these processes to organizational success?

Understanding the cultural and business contexts in which the SSE-CMM will be used is a key to its successful application in process design.

continued on next page

Adding role and structure information

Figure 3-2 illustrates the factors that need to be added to the content of the SSE-CMM process areas and common features to come up with a performable and sustainable process design. It is an organization's context regarding role assignments, organizational structure, security engineering work products, and life cycle that combined with guidance from SSE-CMM generic practices and base practices, produce sound organizational processes that have the potential for deliberate improvement.

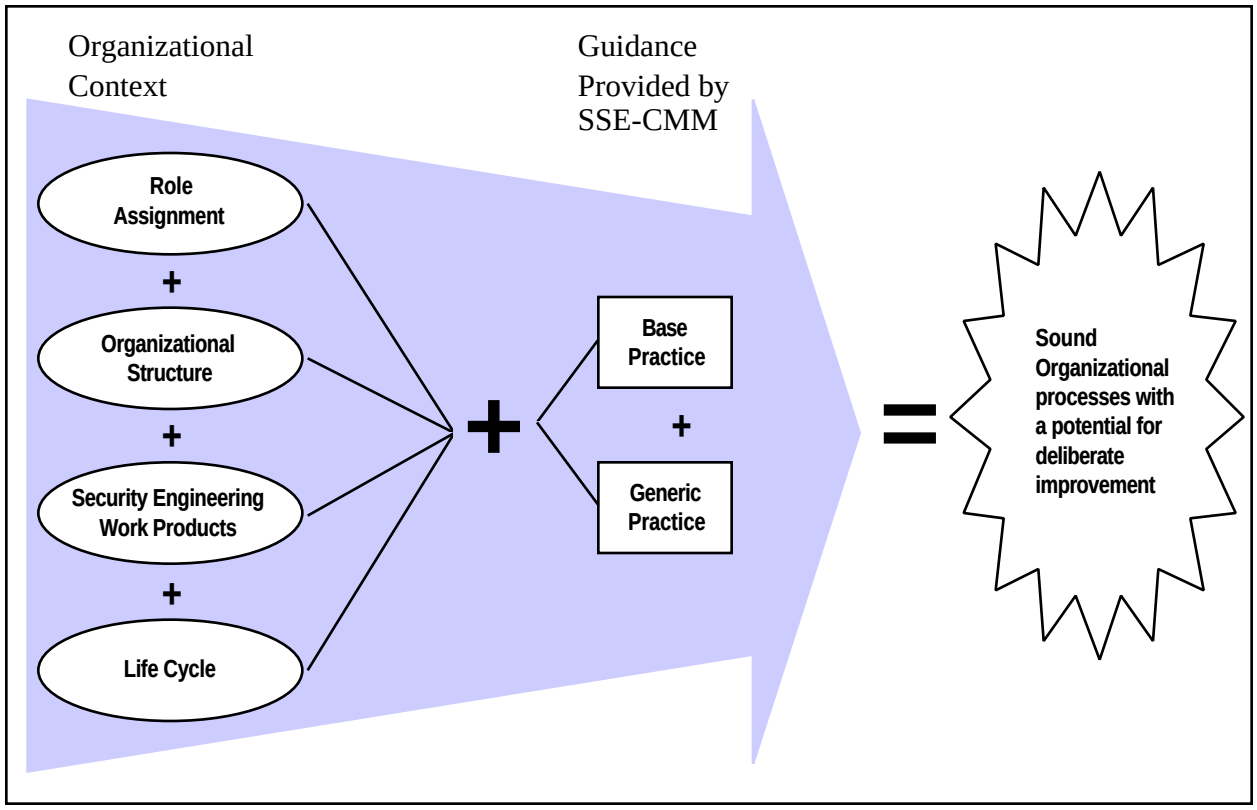

Figure 3-2. Factors for Successful Process Design

3.5 Using the SSE-CMM to Address Customer Assurance Needs

Introduction

A number of the processes that form a part of the SSE-CMM focus on identifying customer security needs. The security needs are divided into two the types of 1) security requirements that deal with the functionality needs, and 2) the needs related to the confidence that the customer can have in the effectiveness of the security, referred to as assurance. The processes that focus on these two types of security requirements are intended to capture customer needs regardless of whether the customer will be provided with a service, product, or integrated solution. Thus, the processes identified in the SSE-CMM address all aspects of the life cycle.

continued on next page

3.5 Using the SSE-CMM to Address Assurance Needs

Assurance Needs

Security functionality needs are derived based upon the customers functionality requirements for the systems and the way in which the system will be used (often referred to as the concept of operations). Thus, the SSE-CMM focuses on the processes that are being used to capture these aspects.

Security functionality, particularly of a commercial product, is normally stated in terms of functionalities and capabilities. Thus, it is relatively easy to relate the functionalities and capabilities to the customer needs. Product assurance, on the other hand, is normally stated in the form claims and evidence to support those claims. In the case of process maturity, claims and evidence also play a significant role, but in a slightly different manner. It is frequently more difficult to relate the claims to the customer needs. Often an interpretation is required. Claims and evidence are further described below.

The assurance needs that the customer has are harder to define. Assurance needs are based upon the confidence that a customer requires in the correct functioning of a system or service and the resulting impact should the system or service cease to function correctly. The process adopted must be sensitive to these aspects and flexible so needs are captured efficiently and effectively.

Part of the objective of the SSE-CMM is to generate confidence based on the maturity of processes used. History has shown that the reliance on process improvement has greatly reduced costs to all participants (see Appendix C Bibliography).

continued on next page

Achieving Assurance

Assurance can be achieved in a number of general ways. Additional controls can be implemented so there is more than one way to prevent an undesirable result from occurring, and thus higher confidence in the effectiveness of the security feature. The effectiveness of controls can be rigorously examined to ensure that the security feature will function effectively and thereby generate confidence in the feature. The security feature can be attacked to see if penetrations can be achieved, again generating confidence in the effectiveness of the feature. The developer can take some actions to insulate the customer from the impacts should the security feature be breached. Finally, the developer of a product, system, or provider of a service may make use of proven and mature processes, and have a demonstrably successful approach which will provide the customer with the assurance they require. In this case all stages of the life cycle including operations, maintenance and disposal need to be included. The processes identified to address these areas are designed to be flexible in approach and to the particular situation under consideration. They should not constrain the CMM users to the choice of an approach.

Assurance is less specific and thus harder to measure as seen from the preceding paragraphs. This means that it can be more costly to generate assurance.

continued on next page

Claims and Evidence

Confidence is gained through the analysis of the assurance claims and the associated evidences that back up the claims.

Assurance Claim: an assertion or supporting assertion that a system or service meets its security needs (i.e., addresses relevant threats). Claims address both direct threats (i.e., system data compromised by outsiders or service subversion by an outsider), and indirect threats (system code flaws to disrupt a service). The processes themselves assist in the production and development of the claims.

Assurance Evidence: data on which a judgment or conclusion about a claim may be based. Evidence consists of observations, documentation, test results, analysis results, and appraisals providing support for the associate claims. The processes themselves and their maturity may form a part of the evidence for a claim.

All claims and associated evidences contribute to assurance.

continued on next page

SSE-CMM Project Goals for Assurance

The SSE-CMM Project Goals are identified in chapter 1 of this document. Of those goals, three are of particular importance with regard to customer needs, namely:

To provide a way to measure and enhance the way in which an organization translates customer security needs into a security engineering process to produce products that effectively meet their need.

To provide an alternate assurance viewpoint for customers who may not need the formal assurances provided by full evaluation or certification and accreditation efforts.

To provide a standard which customers can use to gain confidence that their security needs will be adequately addressed.

It is of paramount importance that customer needs for security functionality and assurance are accurately recorded, understood and translated into security and assurance requirements for a system. Once the final product is produced, the users must be able to see that it reflects and satisfies their needs. The SSE-CMM specifically includes processes designed to achieve these goals.

Chapter 4: Capability Levels and Generic Practices

Introduction

This chapter contains the generic practices, that is, the practices that apply to all processes. The generic practices (GPs) are used in a process appraisal to determine the capability of any process. The generic practices are grouped according to common feature and capability level.

SSE-CMM Adaptations of the SE-CMM

The common features and generic practices are adopted from the SE-CMM v1.1 with 2 changes:

a common feature was added for the SSE-CMM, 3.3 Coordinate Security Practices; and

the "Notes" sections of the generic practices were modified to reference the SSE-CMM process areas.

In this chapter

Chapter 4 is divided into the six process capability levels shown below:

Capability Level 0 - Not Performed

Description	The Not Performed level has no common features. There is general failure to perform the base practices in the process area. Where there are work products that result from performing the process, they are not easily identifiable or accessible.

Capability Level 1 - Performed Informally

Description	Base practices of the process area are generally performed. The performance of these base practices may not be rigorously planned and tracked. Performance depends on individual knowledge and effort. Work products of the process area testify to their performance. Individuals within the organization recognize that an action should be performed, and there is general agreement that this action is performed as and when required. There are identifiable work products for the process.
Common Feature 1.1: Base Practices are Performed	**1.1.1 Perform the process.** Perform a process that implements the base practices of the process area to provide work products and/or services to a customer. *Note:* This process may be termed the "informal process." The customer(s) of the process area may be internal or external to the organization.

Capability Level 2 - Planned and Tracked

Description	Performance of the base practices in the process area is planned and tracked. Performance according to specified procedures is verified. Work products conform to specified standards and requirements. Measurement is used to track process area performance, thus enabling the organization to manage its activities based on actual performance. The primary distinction from the Performed Informally level is that the performance of the process is planned and managed.
Common Feature 2.1: Planning Performance	**2.1.1 Allocate resources.** Allocate adequate resources (including people) for performing the process area. *Relationship to process areas:* Identification of critical resources is done in process area PA 15 Plan Technical Effort. **2.1.2 Assign responsibilities.** Assign responsibilities for developing the work products and/or providing the services of the process area. *Relationship to process areas:* This practice is particularly related to process area PA 15 Plan Technical Effort.

continued on next page

Common Feature 2.1: Planning Performance, continued

2.1.3 Document the process. Document the approach to performing the process area in standards and/or procedures.

Note: Participation of the people who perform a process (its owners) is essential to creating a usable process description. Processes in an organization or on a project need not correspond one to one with the process areas in the SE-CMM. Therefore, a process covering a process area may be described in more than one way (e.g., policies, standards, and/or procedures), to cover a process area, and a process description may span more than one process area.

Relationship to other generic practices: This is the "level 2" process description. The process descriptions evolve with increasing process capability (see 3.1.1, 3.1.2, 5.2.3, 5.2.4 for descriptions of this process).

Standards and procedures that describe the process at this level are likely to include measurements, so that the performance can be tracked with measurement (see common feature 2.4).

Relationship to process areas: This practice is related to process areas PA 16 Define Organization's Security Engineering Process and PA 17 Improve Organization's Security Engineering Processes.

2.1.4 Provide tools. Provide appropriate tools to support performance of the process area.

Relationship to other generic practices: Tool changes may be part of process improvements (see 5.2.3, 5.2.4 for practices on process improvements).

Relationship to process areas: Tools are managed in PA 19 Manage Security Engineering Support Environment.

continued on next page

Common Feature 2.1: Planning Performance, continued

2.1.5 Ensure training. Ensure that the individuals performing the process area are appropriately trained in how to perform the process.

Note: Training, and how it is delivered, will change with process capability due to changes in how the process(es) is performed and managed.

Relationship to process areas: Training and training management is described in PA 20 Provide Ongoing Skills and Knowledge.

2.1.6 Plan the process. Plan the performance of the process area.

Note: Plans for process areas in the engineering and project categories may be in the form of a project plan, whereas plans for the organization category may be at the organizational level.

Relationship to process areas: Project planning is described in process area PA 15 Plan Technical Effort.

continued on next page

Common Feature 2.2: Disciplined Performance

2.2.1 Use plans, standards, and procedures. Use documented plans, standards, and/or procedures in implementing the process area.

Note: A process performed according to its process descriptions is termed a "described process." Process measures should be defined in the standards, procedures, and plans.

Relationship to other generic practices: The standards and procedures used were documented in 2.1.3, and the plans used were documented in 2.1.6. This practice is an evolution of 1.1.1 and evolves to 3.2.1.

2.2.2 Do configuration management. Place work products of the process area under version control or configuration management, as appropriate.

Note: ???[2]Where process area PA 12 Manage Configurations focuses on the general practices of configuration management, this generic practice is focused on the deployment of these practices in relation to the work products of the individual process area under investigation.

Relationship to process areas: ???[3]The typical practices needed to support systems engineering in the configuration management discipline are described in process area PA 12 Manage Configurations.

continued on next page

Common Feature 2.3: Verifying Performance

2.3.1 Verify process compliance. Verify compliance of the process with applicable standards and/or procedures.

Relationship to other generic practices: The applicable standards and procedures were documented in 2.1.3 and used in 2.2.1.

Relationship to process areas: The quality management and/or assurance process is described in process area PA 11 Ensure Quality.

2.3.2 Audit work products. Verify compliance of work products with the applicable standards and/or requirements.

Relationship to other generic practices: The applicable standards and procedures were documented in 2.1.3 and used in 2.2.1.

Relationship to process areas: Product requirements are developed and managed in process area PA 01 Specify Security Needs. Verification and validation is further addressed in PA 03 Verify and Validate Security.

Common Feature 2.4: Tracking Performance

2.4.1 Track with measurement. Track the status of the process area against the plan using measurement.

Note: Building a history of measures is a foundation for managing by data, and is begun here.

Relationship to other generic practices: The use of measurement implies that the measures have been defined and selected in 2.1.3 and 2.1.6, and data have been collected in 2.2.1.

Relationship to process areas: Project tracking is described in process area PA 14 Monitor and Control Technical Effort.

continued on next page

Common Feature 2.4: Tracking Performance, continued	**2.4.2 Tracking Performance.** Take corrective action as appropriate when progress varies significantly from that planned. *Note:* Progress may vary because estimates were inaccurate, performance was affected by external factors, or the requirements, on which the plan was based, have changed. Corrective action may involve changing the process(es), changing the plan, or both. *Relationship to process areas:* Project control is described in process area PA 14 Monitor and Control Technical Effort.

Capability Level 3 - Well Defined

Description

Base practices are performed according to a well-defined process using approved, tailored versions of standard, documented processes. The primary distinction from the Planned and Tracked level is that the process is planned and managed using an organization-wide standard process.

Common Feature 3.1: Defining a Standard Process

3.1.1 Standardize the process. Document a standard process or family of processes for the organization, that describes how to implement the base practices of the process area.

Note: The critical distinction between generic practices 2.1.3 and 3.1.1, the level 2 and level 3 process descriptions, is the scope of application of the policies, standards, and procedures. In 2.1.3, the standards and procedures may be in use in only a specific instance of the process, e.g., on a particular project. In 3.1.1, policies, standards, and procedures are being established at an organizational level for common use, and are termed the "standard process definition."

More than one standard process description may be defined to cover a process area, as the processes in an organization need not correspond one to one with the process areas in this capability maturity model. Also, a defined process may span multiple process areas. The SSE-CMM does not dictate the organization or structure of process descriptions. Therefore, more than one standard process may be defined to address the differences among application domains, customer constraints, etc. These are termed a "standard process family."

Relationship to other generic practices: The "level 2" process description was documented in 2.1.3. The "level 3" process description is tailored in 3.1.2.

Relationship to process areas: The process for developing a process description is described in process area PA 16 Define Organization's Security Engineering Process.

continued on next page

Common Feature 3.1, continued

3.1.2 Tailor the standard process. Tailor the organization's standard process family to create a defined process that addresses the particular needs of a specific use.

Note: Tailoring the organization's standard process creates the "level 3" process definition. For defined processes at the project level, the tailoring addresses the particular needs of the project.

Relationship to other generic practices: The organization's standard process (family) is documented in 3.1.1. The tailored process definition is used in 3.2.1.

Relationship to process areas: Tailoring guidelines are defined in process area PA 16 Define Organization's Security Engineering Process.

Common Feature 3.2: Perform the Defined Process

3.2.1 Use a well-defined process. Use a well-defined process in implementing the process area.

Note: A "defined process" will typically be tailored from the organization's standard process definition. A well-defined process is one with policies, standards, inputs, entry criteria, activities, procedures, specified roles, measurements, validation, templates, outputs, and exit criteria that are documented, consistent, and complete.

Relationship to other generic practices: The organization's standard process definition is described in 3.1.1. The defined process is established through tailoring in 3.1.2.

3.2.2 Perform defect reviews. Perform defect reviews of appropriate work products of the process area.

Note: There is no process area for defect reviews, called "peer reviews" in ISO SPICE and the CMM for Software (in this regard, the SE-CMM differs from SPICE and the CMM for Software).

continued on next page

Common Feature 3.2, continued

3.2.3 Use well-defined data. Use data on performing the defined process to manage it.

Note: Measurement data that were first collected at level 2 are more actively used by this point, laying the foundation for quantitative management at the next level.

Relationship to other generic practices: This is an evolution of 2.4.2; corrective action taken here is based on a well-defined process, which has objective criteria for determining progress (see 3.2.1).

Common Feature 3.3: Coordinate Security Practices

3.3.1 Perform Intra-Group Security Coordination. Coordinate communication within the security engineering group.

Note: This type of coordination addresses the need of security engineers to ensure that decisions with regard to technical security issues (e.g. Access Controls, Security Testing) are arrived at as a group. The commitments, expectations, and responsibilities of the security engineering group are documented and agreed upon within the security engineering group. Security engineering issues are tracked and resolved within the security engineering group.

Relationship to other generic practices: This GP is closely tied to GP 3.2.1 in that processes need to be well defined in order to be effectively coordinated.

Relationship to process areas: Coordination objectives and approaches are addressed in PA09 Coordinate Security.

continued on next page

Common Feature 3.3: Coordinate Security Practices, continued

3.3.2 Perform Inter-Group Security Coordination. Coordinate communication among the various groups within the organization.

Note: This type of coordination addresses the need of security engineers to ensure that the relationships between technical security areas (e.g. Risk Assessment, Design Input, Security Testing) are addressed among the affected engineering groups. The intent is to verify that the data gathered as part of GP 3.3.1 is coordinated with the other engineering groups.

A relationship between engineering groups is established via a common understanding of the commitments, expectations, and responsibilities of each engineering activity within an organization. These activities and understandings are documented and agreed upon throughout the organization and address the interaction among various groups within a project / organization. Security engineering issues are tracked and resolved among all the affected engineering groups within a project / organization.

Relationship to other generic practices: This GP is closely tied to GP 3.2.1 in that processes need to be well defined in order to be effectively coordinated.

Relationship to process areas: Coordination objectives and approaches are addressed in PA09 Coordinate Security. Specific security engineering practices for ensuring other engineering groups are provided with timely and accurate input are addressed in PA02 Provide Security Input.

continued on next page

Common Feature 3.3: Coordinate Security Practices, continued

3.3.3 Perform External Security Coordination. Coordinate communication with external groups.

Note: This type of coordination addresses the needs of external entities that request or require security (e.g., consumers, certification activities, evaluators).

A relationship between external groups (e.g., customer, systems security certifier, signature authority, user) is established via a common understanding of the commitments, expectations, and responsibilities of each engineering activity within an organization. The engineering groups will identify, track, and resolve external technical issues.

Relationship to other generic practices: This GP is closely tied to GP 3.2.1 in that processes need to be well defined in order to be effectively coordinated.

Relationship to process areas: Coordination objectives and approaches are addressed in PA09 Coordinate Security. Security needs of the customer are identified in PA01 Specify Security Needs. The customer's assurance needs are addressed in PA06 Build Assurance Argument.

Capability Level 4 - Quantitatively Controlled

Description	Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance. Performance is objectively managed, and the quality of work products is quantitatively known. The primary distinction from the Well Defined level is that the defined process is quantitatively understood and controlled.
Common Feature 4.1: Establishing Measurable Quality Goals	**4.1.1 Establish quality goals.** Establish measurable quality goals for the work products of the organization's standard process family. *Note:* These quality goals can be tied to the strategic quality goals of the organization, the particular needs and priorities of the customer, or to the tactical needs of the project. The measures referred to here go beyond the traditional end-product measures. They are intended to imply sufficient understanding of the processes being used to enable intermediate goals for work product quality to be set and used. *Relationship to other generic practices:* Data gathered via defect reviews (3.2.2) can be particularly important in setting goals for work product quality.
Common Feature 4.2: Objectively Managing Performance	**4.2.1 Determine process capability.** Determine the process capability of the defined process quantitatively. *Note:* This is a quantitative process capability based on a well-defined (3.1.1) and measured process. Measurements are inherent in the process definition and are collected as the process is being performed. *Relationship to other generic practices:* The defined process is established through tailoring in 3.1.2 and performed in 3.2.1.

continued on next page

Common Feature 4.2: Objectively Managing Performance (cont.)	**4.2.2 Use process capability.** Take corrective action as appropriate when the process is not performing within its process capability. *Note:* Special causes of variation, identified based on an understanding of process capability, are used to understand when and what kind of corrective action is appropriate. *Relationship to other generic practices:* This practice is an evolution of 3.2.3, with the addition of quantitative process capability to the defined process.

Capability Level 5 - Continuously Improving

Description

Quantitative performance goals (targets) for process effectiveness and efficiency are established, based on the business goals of the organization. Continuous process improvement against these goals is enabled by quantitative feedback from performing the defined processes and from piloting innovative ideas and technologies. The primary distinction from the Quantitatively Controlled level is that the defined process and the standard process undergo continuous refinement and improvement, based on a quantitative understanding of the impact of changes to these processes.

Common Feature 5.1: Improving Organizational Capability (organization-level common feature)

5.1.1 Establish process effectiveness goals. Establish quantitative goals for improving process effectiveness of the standard process family, based on the business goals of the organization and the current process capability.

5.1.2 Continuously improve the standard process. Continuously improve the process by changing the organization's standard process family to increase its effectiveness..

Note: The information learned from managing individual projects is communicated back to the organization for analysis and deployment to other applicable areas. Changes to the organization's standard process family may come from innovations in technology or incremental improvements. Innovative improvements will usually be externally driven by new technologies. Incremental improvements will usually be internally driven by improvements made in tailoring for the defined process. Improving the standard process attacks common causes of variation.

Relationship to other generic practices: Special causes of variation are controlled in 4.2.2.

Relationship to process areas: Organizational process improvement is managed in process area PA 17 Improve Organization’s Security Engineering Processes.

continued on next page

Common Feature 5.2: Improving Process Effectiveness

5.2.1 Perform causal analysis. Perform causal analysis of defects.

Note: Those who perform the process are typically participants in this analysis. This is a pro-active causal analysis activity as well as re-active. Defects from prior projects of similar attributes can be used to target improvement areas for the new effort.

Relationship to other generic practices: Results of these analyses are used in 5.2.2, 5.2.3, and/or 5.2.4.

5.2.2 Eliminate defect causes. Eliminate the causes of defects in the defined process selectively.

Note: Both common causes and special causes of variation are implied in this generic practice, and each type of defect may result in different action.

Relationship to other generic practices: Causes were identified in 5.2.1.

5.2.3 Continuously improve the defined process. Continuously improve process performance by changing the defined process to increase its effectiveness.

Note: The improvements may be based on incremental improvements (5.2.2) or innovative improvements such as new technologies (perhaps as part of pilot testing). Improvements will typically be driven by the goals established in 5.1.1.

Relationship to other generic practices: Practice 5.2.2 may be one source of improvements. Goals were established in 5.1.1.

Relationship to process areas: Product technology insertion is managed in PA 18 Manage Security Product Line Evolution.

Chapter 5: Process Areas & Base Practices

In this chapter

This chapter contains the base practices, that is, the practice considered essential to the conduct of basic security engineering. Note that the process areas are numbered in no particular order since the SSE-CMM does not prescribe a specific process or sequence.

Process Area Format

Overview

At present, the SSE-CMM domain aspect consists of 21 process areas (PAs), each of which contains a number of base practices. Each process area is identified in the following subsections.

The general format of the process areas is shown in Figure 4-1. The summary description contains a brief overview of the purpose of the PA. Each PA is decomposed into a set of base practices (BPs). The BPs are considered mandatory items (i.e., they must be successfully implemented to accomplish the purpose of the process area they support). Each base practice is described in detail following the PA summary. Goals identify the desired end result of implementing the PA.

An organization can be assessed against any one single PA or combination of PAs. The PAs together, however, are intended to cover all base practices for security engineering and there are many inter-relationships between the PAs.

continued on next page

Format

Figure 5-1 provides the general format of the process areas and describes the content of each part.

PA #: PA Title	
Summary description	The purpose of <PA Title> is <description of the purpose of the PA and summary of its major points>
Goals	<list of results expected from performance of the PA>
Process area notes	<additional explanatory information>
Base practices list	The following list contains the base practices that are essential elements of good security engineering: BP #: <base practice statement> . . .
	end of PA Summary Section
BP # **BP Title**	<BP statement: imperative, verb-object statement that describes an essential element for attaining the purpose of the PA> *Description* <provides elaboration of the base practice statement> *Example Work Products* <list of work products> *Notes* <conceptual examples, potential techniques, methods, etc. Content varies from BP to BP>
	end of Process Area <PA title>

Figure 5-1. Process Area Format

PA 01: Specify Security Needs

Summary description

The purpose of Specify Security Needs is to explicitly identify the needs related to security for the system. Specify Security Needs involves defining the basis for security in the system in order to meet all legal, policy, and organizational requirements for security. These needs are tailored based upon the target operational security context of the system, the current security and systems environment of the organization, and a set of security objectives are identified. A set of security-related requirements is defined for the system which upon approval becomes the baseline for security within the system.

Goals

- A common understanding of security needs is reached between all parties, including the customer.

Process area notes

This process area covers the activities defining all aspects of security in the entire information system (e.g., physical, functional, procedural). The base practices address how the security needs are identified and refined into a coherent baseline of security-related requirements which used in the design, development, verification, operation, and maintenance of the system. In most cases it is necessary to take into account the existing environment and associated security needs. The information gained and produced by this process area is collected, further refined, used, and updated throughout a project (particularly in Provide Security Input (PA02)), in order to ensure customer needs are being addressed.

Base practices list

The following list contains the base practices that are essential elements of good systems security engineering:

BP.01.01	Gain an understanding of the customer's security needs.
BP.01.02	Identify which laws, policies, standards, external influences and constraints govern the system.
BP.01.03	Identify the purpose of the system in order to determine the security context.
BP.01.04	Capture a high-level security oriented view of the system operation.
BP.01.05	Capture high-level goals that define the security of the system.
BP.01.06	Define a consistent set of statements which define the protection to be implemented in the system.
BP.01.07	Obtain agreement that the specified security meets the customer's needs.

continued on next page

BP 01.01 Gain Understanding of Customer's Security Needs

Gain an understanding of the customer's security needs.

Description

The purpose of this base practice is to collect all information necessary for a comprehensive understanding of the customer's security needs. These needs are influenced by the importance to the customer of security risk. The target environment in which the system is intended to operate also influences the customer's needs with regard to security.

Example Work Products

- customer security needs statement
  high-level description of security required by the customer

Notes

The term customer may refer to a specific recipient of a product, system, or service, or may refer to a genericized recipient based upon market research or product targeting.

continued on next page

BP 01.02 Identify Applicable Laws, Policies, And Constraints

Identify which laws, policies, standards, external influences and constraints govern the system.

Description

The purpose of this base practice is to gather all external influences which affect the security of the system. A determination of applicability should identify the laws, regulations, policies and commercial standards which govern the target environment of the system. A determination of precedence between global and local policies should be performed. Requirements for security placed on the system by the system customer must be identified and the security implications extracted.

Example Work Products

- security constraints
  laws, policies, regulations, and other constraints that influence the security of a system
- security profile
  security environment (threats, organizational policy); security objectives (e.g., threats to be countered); security functional and assurance requirements; rationale that system developed to these requirements will meet the objectives

Notes

Particular consideration is required when the system will cross multiple physical domains. Conflict may occur between laws and regulations that are applicable in different countries and different types of business. As part of the identification process, conflicts should at a minimum, be identified and resolved if possible.

continued on next page

BP 01.03 Identify System Security Context

Identify the purpose of the system in order to determine the security context.

Description

The purpose of this base practice is to identify how the system's context impacts security. This involves understanding the purpose of the system (for example, intelligence, financial, medical). Mission processing and operations scenarios are assessed for security considerations. A high-level understanding of the threat to which the system is or may be subject to is required at this stage. Performance and functional requirements are assessed for possible impacts on security. Operating constraints are also reviewed for their security implications.

The environment might also include interfaces with other organizations or systems in order to define the security perimeter of the system. Interface elements are determined to be either inside or outside of the security perimeter.

Many factors external to the organization also influence to varying degrees the security needs of the organization. These factors include the political orientation and changes in political focus, technology developments, economic influences, global events, and Information Warfare activities. As none of these factors are static they require monitoring and periodic assessment of the potential impact of change.

Example Work Products

- expected threat environment
  any known or presumed threats to the system assets against which protection is needed; include threat agent (expertise, available resources, motivation), the attack (method, vulnerabilities exploited, opportunity), the asset
- target of evaluation
  description of the system or product whose security features are to be evaluated (type, intended application, general features, limitations of use) [CCEB96]

continued on next page

BP 01.03 Identify System Security Context (cont.)	*Notes* The security perimeter of the system is not necessarily identical to the system boundary. For example, the security perimeter could contain the facility in which the system resides and the personnel operating the system whereas the system boundary may stop at the human-machine interface. This expanded security perimeter enables physical measures to be considered as effective safeguards for access control in addition to purely technical measures.

continued on next page

BP 01.04 Capture Security View of System Operation

Capture a high-level security oriented view of the system operation.

Description

The purpose of the base practice is to develop a high-level security oriented view of the enterprise, including roles, responsibilities, information flow, assets, resources, personnel protection, and physical protection. This description should include a discussion of how the enterprise can be conducted within the constraints of the system requirements. This view of the system is typically provided in a security concept of operations and should include a high-level security view of the system architecture, procedures, and the environment. Requirements related to the system development environment are also captured at this stage.

Example Work Products

- security concept of operations
  high-level security oriented view of the system (roles, responsibilities, assets, information flow, procedures)
- conceptual security architecture
  a conceptual view of the security architecture; see BP02.03 security architecture

Notes

None.

continued on next page

BP 01.05 Capture Security High-Level Goals

Capture high-level goals that define the security of the system.

Description

The purpose of this base practice is to identify what security objectives should be met to provide adequate security for the system in its operational environment. The assurance objectives of the system, determined in PA06 Build Assurance Argument may influence the security objectives.

Example Work Products

- operational/environmental security policy
  rules, directives, and practices that govern how assets are managed, protected, and distributed within and external to an organization
- system security policy
  rules, directives, and practices that govern how assets are managed, protected, and distributed by a system or product

Notes

The objectives should be, as far as possible, independent of any particular implementation. If particular constraints are present due to the existing environment they should be addressed in PA02 Provide Security Input when security constraints and considerations for making informed engineering choices are determined. The security objectives should as a minimum address the availability, accountability, authenticity, confidentiality, integrity and reliability requirements of the system and information.

continued on next page

BP 01.06 Define Security Related Requirements

Define a consistent set of requirements which define the protection to be implemented in the system.

Description

The purpose of this base practice is to define the security-related requirements of the system. The practice should ensure each requirement is consistent with the applicable policy, laws, standards, requirements for security and constraints on the system. These requirements should completely define the security needs of the system including those requirements to be provided through non-technical means. It is normally necessary to define or specify the boundary of the target, logical or physical, to ensure that all aspects are addressed. The requirements should be mapped or related to the objectives of the system. The security-related requirements should be clearly and concisely stated and should not contradict one another. Security should, whenever possible, minimize any impact on the system functionality and performance. The security-related requirements should provide a basis for evaluating the security of the system in its target environment.

Example Work Products

- security related requirements
  requirements which have a direct effect on the secure operation of a system or enforce conformance to a specified security policy
- traceability matrix
  mapping of requirements to security needs of the system

Notes

Many requirements apply to multiple disciplines, so few requirements are exclusively security. This process area, therefore, requires a great deal of coordination with other disciplines to work out exactly what the system requirements are. The activities associated with this interaction are described in PA09 Security Coordination.

continued on next page

BP 01.07
Obtain Agreement On Security

Obtain agreement that the specified security meets the customer's needs.

Description

The purpose of this base practice is to obtain concurrence between all applicable parties on the system's security needs and the specified security. In the case where a specific customer, rather than a generic group, is not identified, that the specified security satisfies the objectives set. The specified security should be a complete and consistent reflection of governing policy, laws, and customer needs. Issues should be identified and reworked until concurrence is gained.

Example Work Products

- approved security objectives
  stated intent to counter identified threats and/or comply with identified security policies (as approved by the customer)
- security related requirements baseline
  the minimum set of security related requirements as agreed to by all applicable parties (specifically the customer) at specified milestones

Notes

It is important to ensure that what agreed is truly understood by all concerned and that all have the same understanding. Particular care is required to ensure that the security requirements mean the same thing to all those involved in the process.

End of PA 01: Specify Security Needs

PA 02: Provide Security Input

Summary description	The purpose of Provide Security Input is to provide system architects, designers, implementers, or users with the security information they need. This information includes security architecture, design, or implementation alternatives and security guidance. The input is developed, analyzed, provided to and coordinated with the appropriate organization members based on the security needs identified in PA01 Specify Security Needs.
Goals	• Needed security input is identified. • Timely and accurate security input is provided to appropriate parties.
Process area notes	This process area provides security input to support system design and implementation activities. The focus is on how security is an integral part of system development and not an end unto itself. Each of the base practices uses input from the entire engineering organization, produces security specific results, and communicates those results back to the entire engineering organization. The processes identified are applicable to the development of new facilities or the operation and maintenance of existing ones. This process area covers security input to both development (designers and implementors) and operation (users and administrators). In addition, by combining the design and implementation security activities into a single process area, it emphasizes that these activities are very similar, but are at different levels of abstraction. The alternative solutions range in scope from full system architectures to individual components. Some aspects of security requirements impact the environment in which the system is developed rather than the system itself. All base practices within this process area can be iterative and all occur at multiple points through the system life cycle.

continued on next page

Base practices list

The following list contains the base practices that are essential elements of good systems security engineering:

BP.02.01	Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs.
BP.02.02	Determine the security constraints and considerations needed to make informed engineering choices.
BP.02.03	Identify alternative solutions to security related engineering problems.
BP.02.04	Analyze and prioritize engineering alternatives using security constraints and considerations.
BP.02.05	Provide security related guidance to the other engineering groups.
BP.02.06	Provide security related guidance to operational system users and administrators.

continued on next page

BP 02.01 Understand Security Input Needs

Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs.

Description

Security engineering is coordinated with other disciplines to determine the types of security input that are helpful to those disciplines. Security input includes any sort of guidance, designs, documents, or ideas related to security that should be considered by other disciplines. Input can take many forms, including documents, memoranda, e-mail, training, and consultation.

This input is based on the needs determined in PA01 Specify Security Needs. For example, a set of security rules may need to be developed for the software engineers. Some of the inputs are more related to the environment than the system.

Example Work Products

- agreements between security engineering and other disciplines
  definition of how security engineering will provide input to other disciplines (e.g., documents, memoranda, training, consulting)
- descriptions of input needed
  standard definitions for each of the mechanisms for providing security input

Notes

Assurance objectives may have an influence on the specific security needs, particularly in such aspects as dependencies. They may also provide additional justification to security needs. In this case, security engineering need to provide the other disciplines with guidance on how to produce the appropriate evidence.

continued on next page

BP 02.02 Determine Security Constraints and Considera-tions

Determine the security constraints and considerations needed to make informed engineering choices.

Description

The purpose of this base practice is to identify all the security constraints and considerations needed to make informed engineering choices. The security engineering group performs analysis to determine any security constraints and considerations on the requirements, design, implementation, configuration, and documentation. Constraints may be identified at all times during the system's life. They may be identified at many different levels of abstraction. Note that these constraints can be either positive (always do this) or negative (never do this).

Example Work Products

- security design criteria
  security constraints and considerations that are needed to make decisions regarding overall system or product design
- security implementation rules
  security constraints and considerations that apply to the implementation of a system or product (e.g., use of specific mechanisms, coding standards)
- documentation requirements
  identification of specific documentation needed to support security requirements (e.g., administrators manual, users manual, specific design documentation)

Notes

These constraints and considerations are used to identify security alternatives (BP.02.03) and to provide security engineering guidance (BP.02.05). A major source of the constraints and considerations is the security relevant requirements, identified in PA01 Specify Security Needs.

continued on next page

BP 02.03 Identify Security Alternatives

Identify solutions to security related engineering problems.

Description

The purpose of this base practice is to identify alternative solutions to security related engineering problems. This process is iterative and transforms security related requirements into implementations. These solutions can be provided in many forms, such as architectures, models, and prototypes. This base practice involves decomposing, analyzing, and recomposing security related requirements until effective alternative solutions are identified.

Example Work Products

- security views of system architecture
  describe at an abstract level relationships between key elements of the system architecture in a way that satisfies the security requirements
- security design documentation
  includes details of assets and information flow in the system and a description of the functions of the system that will enforce security or that relate to security
- security models
  a formal presentation of the security policy enforced by the system; it must identify the set of rules and practices that regulate how a system manages, protects, and distributes information; the rules are sometimes expressed in precise mathematical terms [NCSC88]
- security architecture
  focuses on the security aspects of a systems architecture, describing the principles, fundamental concepts, functions, and services as they relate to the security of the system
- reliance analysis (safeguard relationships and dependencies)
  a description of how the security services and mechanisms interrelate and depend upon one another to produce effective security for the whole system; identifies areas where additional safeguards may be needed

continued on next page

BP 02.03 Identify Security Alternatives (cont.)	*Notes* The solution alternatives include architecture, design, and implementation solutions. These security alternatives should be consistent with the constraints and considerations identified when determining security constraints and considerations (BP.02.02). The alternatives are also a part of the trade-off comparisons (BP.02.04). This activity is related to providing security engineering guidance (BP.02.05) in so much as once the preferred alternative has been selected, guidance to the other engineering disciplines is required.

continued on next page

BP 02.04 Analyze Security of Engineering Alternatives

Analyze and prioritize engineering alternatives using security constraints and considerations.

Description

The purpose of this base practice is to analyze and prioritize engineering alternatives. Using the security constraints and considerations identified when determining security constraints and considerations (BP.02.02), the design group can evaluate each engineering alternative and come up with a recommendation for the engineering group. The security engineering group should also consider the engineering guidance from other engineering groups.

These engineering alternatives are not limited to the security alternatives identified (BP.02.03), but can include alternatives from other disciplines as well.

Example Work Products

- trade-off study results and recommendations
  includes analysis of all engineering alternatives considering security constraints and considerations as provided in BP02.02
- end-to-end trade-off study results
  results of various decisions throughout the life cycle of a product, system, or process, focusing on areas where security requirements may have been reduced in order to meet other objectives (e.g., cost, functionality)

Notes

None.

continued on next page

BP 02.05 Provide Security Engineering Guidance

Provide security related guidance to the other engineering groups.

Description

The purpose of this base practice is to develop security related guidance and provide it to the engineering groups. Security engineering guidance is used by the engineering groups to make decisions about architecture, design, and implementation choices.

Example Work Products

- architecture recommendations
  includes principles or constraints that will support the development of a system architecture that satisfies the security requirements
- design recommendations
  includes principles or constraints that guide the design of the system
- implementation recommendations
  includes principles or constraints that guide the implementation of the system
- security architecture recommendations
  includes principles or constraints that define the security features of the system
- philosophy of protection
  high-level description of how security is enforced, including automated, physical, personnel, and administrative mechanisms
- design standards, philosophies, principles
  constraints on how the system is designed (e.g., least privilege, isolation of security controls)
- coding standards
  constraints on how the system is implemented

Notes

The amount of guidance required and the level of detail depends on the knowledge, experience and familiarity of the other engineering disciplines with security. In many cases much of the guidance may relate to the development environment rather than the system under development.

continued on next page

BP 02.06 Provide Operational Security Guidance

Provide security related guidance to operational system users and administrators.

Description

The purpose of this base practice is to develop security related guidance and provide it to system users and administrators. This operational guidance tells the users and administrators what must be done to install, configure, operate, and decommission the system in a secure manner. To ensure that this is possible, the development of the operational security guidance should start early in the life cycle.

Example Work Products

- administrators manual
  description of system administrator functions and privileges for installing, configuring, operating, and decommissioning the system in a secure manner
- users manual
  description of the security mechanisms provided by the system and guidelines for their use
- security profile
  security environment (threats, organizational policy); security objectives (e.g., threats to be countered); security functional and assurance requirements; rationale that system developed to these requirements will meet the objectives
- system configuration instructions
  instructions for configuration of the system to ensure its operation will meet the security objectives

Notes

The development environment is considered to be an operational environment for the development of systems.

End of PA 02: Provide Security Input

PA 03: Verify and Validate Security

Summary description

The purpose of Verify and Validate Security is to ensure that solutions verified and validated with respect to security. Solutions are verified against the security requirements, architecture, and design using observation, demonstration, analysis, and testing. Solutions are validated against the customer's operational security needs.

Goals

- Solutions meet security requirements.
- Solutions meet the customer's operational security needs.

Process area notes

This process area is an important part of system verification and validation and occurs at all levels of abstraction. Solutions include everything from operational concepts to architectures to implementations and span the entire information system, including environment and procedures.

In the interest of obtaining objective results, the verification and validation group should be a group that is different than the engineering groups; however, the group may be working side-by-side with the engineering groups. The results of both verification and validation may be fed back to the entire engineering groups at any time during the solution life cycle. Verification and validation are sometimes associated with the concepts of correctness and effectiveness.

Base practices list

The following list contains the base practices that are essential elements of good systems security engineering:

BP.03.01	Identify the solution to be verified and validated.
BP.03.02	Define the approach and level of rigor for verifying and validating each solution.
BP.03.03	Verify that the solution implements the requirements associated with the previous level of abstraction.
BP.03.04	Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer's operational security needs.
BP.03.05	Capture the verification and validation results for the other engineering groups.

continued on next page

BP 03.01 Identify Verification and Validation Targets

Identify the solution to be verified and validated.

Description

The purpose of this base practice is to identify the targets of the verification and validation activities, respectively. Verification demonstrates that the solution is correctly implemented, while validation demonstrates that the solution is effective. This involves coordination with the all the engineering groups throughout the life cycle.

Example Work Products

- verification and validation plans
  definition of the verification and validation effort (includes resources, schedule, work products to be verified and validated)

Notes

Many work products can be verified and validated, spanning a wide range of abstraction and complexity. These include requirements, designs, architectures, implementations, hardware items, software items, and test plans. Work products associated with operation and maintenance of a system can also be verified and validated, including system configuration, user documentation, training materials, and incident response plans.

continued on next page

BP 03.02 Define Verification and Validation Approach

Define the approach and level of rigor for verifying and validating each solution.

Description

The purpose of this base practice is to define the approach and level of rigor for verifying and validating each solution. Identifying the approach involves selecting how each requirement is verified and validated. The level of rigor should indicate how intense the scrutiny of the verification and validation effort should be and is influenced by the output of the assurance strategy from PA06 Build Assurance Argument. For example, some projects may require a cursory inspection for compliance with the requirements and others may require much more rigorous examination.

The methodology should also include a means to maintain traceability from customer's operational security needs to security requirements to solutions to validation and verification results.

Example Work Products

- test, analysis, demonstration, and observation plans
  definition of the verification and validation methods to be used (e.g., testing, analysis) and the level of rigor (e.g., informal or formal methods)
- test procedures
  definition of the steps to be taken in the testing of each solution
- traceability approach
  description of how verification and validation results will be traced to customer's security needs and requirements

Notes

The verification and validation approach should be compatible with the overall system verification and validation approach. This will require significant coordination and interaction. Activities related to coordination are described in PA09 Coordinate Security.

continued on next page

BP 03.03 Perform Verification

Verify that the solution implements the requirements associated with the previous level of abstraction.

Description
The purpose of this base practice is to verify that the solution is correct by showing that it implements the requirements associated with the previous level of abstraction including the assurance requirements identified as a result of PA06 Build Assurance Argument. There are many methods of verifying requirements, including testing, analysis, observation, and demonstration. The method to be used is identified in BP.03.02. Both the individual requirements and the overall system are examined.

Example Work Products
- raw data from test, analysis, demonstration, and observation
  results from any approaches used in verifying that the solution meets the requirements
- problem reports
  inconsistencies discovered in verifying that a solution meets the requirements

Notes
None.

continued on next page

BP 03.04 Perform Validation

Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer's operational security needs.

Description
The purpose of this base practice is to validate that the solution satisfies the needs associated with the previous level of abstraction. Validation demonstrates that the solution meets these needs effectively. There are many ways to validate that these needs have been met, including testing the solution in an operational or representative test setting. The method to be used is identified in BP.03.02.

Example Work Products
- problem reports
  inconsistencies discovered in validating that a solution meets the security need
- inconsistencies
  areas where the solution does not meet the security needs
- ineffective solutions
  solutions that do not meet the customer's security needs

Notes
This practice is related to traceability.

continued on next page

BP 03.05 Provide Verification and Validation Results

Capture the verification and validation results for the other engineering groups.

Description

The purpose of this base practice is to capture and provide the verification and validation results. The verification and validation results should be provided in a way that is easy to understand and use. The results should be tracked so that the traceability from needs, to requirements, to solution, and to test results is not lost.

Example Work Products

- test results
  documentation of outcome of testing
- traceability matrix
  mapping of security needs to requirements to solutions (e.g., architecture, design, implementation) to tests and test results

Notes

None.

End of PA 03: Verify and Validate Security

PA 04: Attack Security

Summary description

The purpose of Attack Security is to identify existing system vulnerabilities and validate their potential for exploitation. Vulnerabilities are discovered through active attacks against the system.

Goals

- System vulnerabilities are identified and their potential for exploitation is determined.

Process area notes

Discovery of system vulnerabilities by active tools and techniques is a method that supplements but does not replace the vulnerability analysis conducted in PA10 Determine Security Vulnerabilities. Attack Security may be viewed as a specialized form of vulnerability analysis. For example, this type of analysis can be useful when trying to validate the security vulnerability of a system after a significant system upgrade, or to identify security vulnerabilities when two systems are interconnected. Attack security is needed in some cases to validate the security posture of a system and to increase the perception and understanding of existing security vulnerabilities.

Attack Security, sometimes referred to as penetration testing, is a process in which security engineers attempt to circumvent the security features of the system. The security engineers typically work under the same constraints applied to ordinary users but may be assumed to use all design and implementation documentation. The process of attacking security is not exhaustive and it is constrained by time and money.

Base practices list

The following list contains the base practices that are essential elements of good systems security engineering:

BP.04.01	Identify the depth and breadth of the attack.
BP.04.02	Develop attack scenarios that can identify potential vulnerabilities.
BP.04.03	Perform attacks within the framework of the developed attack scenarios.
BP.04.04	Synthesize the results of the applied attacks.

continued on next page

BP 04.01
Scope Attack

Identify the depth and breadth of the attack.

Description

The purpose of identifying the depth and breadth of the attack is for the security engineers and the customer to determine the target system(s) and network(s) that are to be part of the exercise and comprehensive the exercise will be. Attacks should be performed within the framework of a known and recorded configuration environment during a pre-arranged and specified time period. The duration and available resources of the exercise should be determined as well as the visible effects (e.g., audit trail entries). Specific objectives for the attack should be clearly stated so that appropriate scenarios can be developed.

Example Work Products

- attack methodology and philosophy
  includes objectives and the approach for performing the attack testing
- attack procedures
  detailed steps for performing the attack testing
- attack plans
  includes resources, schedule, description of the attack methodology
- penetration study
  the analysis and implementation of attack scenarios targeted at identifying unknown vulnerabilities
- attack scenarios
  description of the specific attacks that will be attempted

Notes

The limitations of automated tools used to conduct certain types of attacks should be considered when determining the scope of the attack exercise.

continued on next page

BP 04.02 Develop Attack Scenarios

Develop attack scenarios that can identify potential vulnerabilities.

Description

The purpose of developing attack scenarios is to conduct security attacks in a systematic manner. Since there is no single method for developing attack scenarios, a methodology and philosophy for carrying out the attack must be developed and documented. One approach used is to analyze the system documentation to hypothesize security vulnerabilities. The list of hypothesized vulnerabilities is then ranked according to the security required by the customer and by an estimated probability of existence and potential for exploitation. Finally the prioritized list is used to develop the attack scenarios. The attack scenarios should document the expected result of the attack.

Example Work Products

- attack methodology and philosophy
  includes objectives and the approach for performing the attack testing
- attack procedures
  detailed steps for performing the attack testing
- attack plans
  includes resources, schedule, description of the attack methodology
- penetration study
  the analysis and implementation of attack scenarios targeted at identifying unknown vulnerabilities
- attack scenarios
  description of the specific attacks that will be attempted

Notes

An attack on system security should be repeatable. An attack should not be conducted in an ad hoc manner, although it does not have to be fully specified to include exploitation procedures.

continued on next page

BP 04.03 Perform Attacks

Perform attacks within the framework of the developed attack scenarios.

Description
Attack scenarios as developed in BP04.02 should be followed to the extent that expected vulnerabilities are validated. All system vulnerabilities including expected and unexpected, discovered during an attack should be noted.

Example Work Products
- penetration profile
  includes results of the attack testing (e.g., vulnerabilities)

Notes
Attacks which are not reproducible make the task of developing countermeasures difficult.

continued on next page

BP 04.04 Synthesize Attack Results

Synthesize the results of the applied attacks.

Description

Results of the attack exercise need to be analyzed and documented. Any vulnerabilities found and their potential for exploitation need to be identified. Vulnerabilities that were discovered during the attack must be documented in sufficient detail to allow the customer to make decisions about countermeasures. In some cases the security engineer may review the attack outcome through audit logs and alarms that were activated by the attack. Recommendations for resolving these vulnerabilities may also be included in the results.

Example Work Products

- attack reports

  documents the results and analysis of the results including vulnerabilities found, their potential for exploitation, and recommendations

Notes

Attack results can be conveyed in written report but attacks may also be demonstrated in a presentation.

End of PA 04: Attack Security

PA 05: Assess Operational Security Risk

Summary description	The purpose of Assess Operational Security Risk is to identify the security risks involved with relying on an operational system in a defined environment. This process area focuses on ascertaining these risks based on an established understanding of how operational capabilities and assets are vulnerable to threats. This includes activities that assess the operational impact that results from a successful exploitation of a vulnerability. This set of activities is performed any time during a system's life-cycle to support decisions related to developing, maintaining, or operating the system within a known environment.
Goals	• An understanding of the security risk associated with operating the system within a defined environment is reached.
Process area notes	The activities associated with this process area often depend on an established understanding of overall system vulnerabilities. Obtaining these technical understandings is the focus of PA 10 Determine Security Vulnerabilities. These understandings can be focused or prioritized for operationally significant threats or functions, whose importance is established by some of the activities of this process area. Determination and selection of countermeasures are practiced in accordance with PA01 Specify Security Needs and PA02 Provide Security Inputs. Threats and their operational importance can change, so the risk assessment activity can be, and typically is, iterative and can be conducted multiple times for an asset in a defined environment. In the case of products (as opposed to operational systems) this PA can be applicable considering an assumed environment, or this PA may not apply.

continued on next page

Base practices list

The following list contains the base practices that are essential elements of good systems security engineering:

BP.05.01	Select the methods, techniques, and criteria by which security risks for the system in a defined environment are analyzed, assessed, and compared.
BP.05.02	Identify, analyze, and prioritize operational, business, or mission capabilities and assets leveraged by the system as well as their associated values.
BP.05.03	Identify applicable threats (both natural and human-based) to both operational and security objectives.
BP.05.04	Assess potential operational impacts based on an analysis of prioritized operational capabilities and assets, identified threats, and established system vulnerabilities.

continued on next page

BP 05.01 Select Risk Analysis Method

Select the methods, techniques, and criteria by which security risks for the system in a defined environment are analyzed, assessed, and compared.

Description

This base practice consists of defining the method for establishing security risks for the system in a defined environment in a way that permits them to be analyzed, assessed, and compared. This should include a scheme for categorizing and prioritizing the risks based on threats, operational functions, established system vulnerabilities, potential loss, security requirements, or areas of concern.

Example Work Products

- risk assessment method
  defines the method for determining, categorizing, and prioritizing the security risks to a system in a way that allows them to be analyzed, assessed, and compared
- risk assessment formats
  describes the format in which risks will be documented and tracked, including a description, significance, and dependencies.

Notes

Method can be an existing one, tailored one, or one specific to the operational aspects and defined environment for the system.

continued on next page

BP 05.02 Prioritize Operational Capabilities and Assets

Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system and assets as well as their associated values.

Description

Identify, analyze, and prioritize operational, business, or mission capabilities and assets leveraged by the system. These can include information assets in addition to explicit capital or physical assets (hardware and software) associated with the operation. Each of these assets are defined by assessing the importance or value of the asset to the customer within the defined operational environment.

Example Work Products

- asset list

  documents the assets and capabilities leveraged by the system, such as capital, hardware, software, information assets, and operational capabilities, in terms of their significance, classification, sensitivity level, type, criticality, or other valuation.

- system capability profile

  describes the operational capabilities of a system and their importance to the objective of the system.

continued on next page

BP 05.02 Prioritize Operational Capabilities and Assets (cont.)

Notes

Functional and information assets can be interpreted to their value and criticality in the defined environment. Value can be the operational significance, classification, sensitivity level, or any other means of specifying the perceived value of the asset to the intended operation and use of the system. Criticality can be interpreted as the impact on the system operation, on human lives, on operational cost and other critical factors, when a leveraged function is compromised, modified, or unavailable in the operational environment

Assets are further defined in relation to their applicable security requirements. For example, assets may be defined as the confidentiality of a client list, the availability of interoffice communication, or the integrity of payroll information. Assets are further refined in PA10 Determine Security Vulnerabilities.

Many assets are intangible or implicit, as opposed to explicit. The risk assessment method selected should address how capabilities and assets are to be valued and prioritized.

continued on next page

BP 05.03 Identify Threats

Identify applicable threats (both natural and human-based) to both operational and security objectives.

Description
The purpose of this base practice is to identify and define threats to the system. Further identification of threats is accomplished through an association of threats to defined assets and a determination of the nature and likelihood of these events.

Example Work Products
- threat list

  the potential threats to operational and security objectives, detailing their likelihood of occurrence, likelihood of success, and their impact.

Notes
Threat assessment minimally includes a determination of the likelihood of each threat against the assets and the value of each asset to the threat (in the case of a human threat). This assessment also can include the development and analysis of multiple concurrent threats, where the likelihood of several threats applied in parallel is analyzed. Because threats to assets can change, the threat assessment activity can be iterative and can be conducted multiple times in the defined environments.

continued on next page

BP 05.04 Assess Operational Impacts

Assess potential operational impacts based on an analysis of prioritized operational capabilities and assets, identified threats, and established system vulnerabilities.

Description

Assess the potential operational impacts and ordered according to some combination of the likelihood of impact, potential impact, and threats. The analysis uses prioritized operational capabilities, identified threats, and specific vulnerabilities to categorize impacts.

Example Work Products

- risk assessment
  identifies and prioritizes the operational risks to the system based on the likelihood of successful exploitation of a vulnerability which leads to a harmful impact.
- risk comparisons
  documents the trade-offs possible in the risk reduction process.
- impact report
  details the effects of a successful attack on a vulnerability in terms of money, time, reputation, or other valuation, and in terms of all facets of security criticality.

Notes

Impact may be determined quantitatively or qualitatively or a combination of the two.

End of PA 05: Assess Operational Security Risk

PA 06: Build Assurance Argument

Summary description

The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.

This process includes identifying and defining assurance related requirements; evidence production and analysis activities; and additional evidence activities needed to support assurance requirements. Additionally, the evidence generated by these activities is gathered, packaged, and prepared for presentation.

Goals

- Ensure that the work products and processes clearly provide the evidence that the customer's security needs have been met.

Process area notes

Activities involved in building an assurance argument include managing the identification, planning, packaging, and presentation of security assurance evidence.

Base practices list

The following list contains the base practices that are essential elements of good systems security engineering:

BP.06.01	Identify the security assurance objectives.
BP.06.02	Define a security assurance strategy to address all assurance objectives.
BP.06.03	Identify and control security assurance evidence.
BP.06.04	Perform analysis of security assurance evidence.
BP.06.05	Provide a security assurance argument that demonstrates the customer's security needs are met.

continued on next page

BP 06.01 Identify Assurance Objectives

Identify the security assurance objectives.

Description

Assurance objectives as determined by the customer, identify the level of confidence needed in the system. The system security assurance objectives specify a level of confidence that the system security policy is enforced. Adequacy of the objectives is determined by the developer, integrator, customer, and the signature authority.

Identification of new, and modification to existing, security assurance objectives are coordinated with all security-related groups internal to the engineering organization and groups external to the engineering organization (e.g., customer, systems security certifier, signature authority, user).

The security assurance objectives are updated to reflect changes. Examples of changes requiring a modification in security assurance objectives include changes in the level of acceptable risk by the customer, system security certifier, signature authority, or user, or changes in the requirements or interpretations of the requirements.

Security assurance objectives must be communicated so as to be unambiguous. Applicable interpretations are included or developed if necessary.

Example Work Products

- statement of security assurance objectives

  identifies the customer's requirements for the level of confidence needed in a system's security features.

Notes

In cases where a specific claim is not mandated, it is helpful if the assurance objectives can be stated or related to a specific assurance claim to be achieved or met. This helps to reduce misunderstandings and ambiguity.

continued on next page

BP 06.02 Define Assurance Strategy

Define a security assurance strategy to address all assurance objectives.

Description

The purpose of a security assurance strategy is to plan for and ensure that the security objectives are implemented and enforced correctly. Evidence produced through the implementation of a security assurance strategy should provide an acceptable (to the system signature authority) level of confidence that the system security measures are adequate to manage the security risk. Effective management of the assurance related activities is achieved through the development and enactment of a security assurance strategy. Early identification and definition of assurance related requirements is essential to producing the necessary supporting evidence. Understanding and monitoring the satisfaction of customer assurance needs through continuous external coordination ensures a high quality assurance package.

Example Work Products

- security assurance strategy

  describes the plan for meeting the customer's security assurance objectives and identifies the responsible parties.

Notes

The security assurance strategy is coordinated with all affected internal engineering groups and external groups (e.g., customer, systems security certifier, signature authority, or user) as defined in PA09 Coordinate Security.

continued on next page

BP 06.03 Control Assurance Evidence

Identify and control security assurance evidence.

Description

Security assurance evidence is gathered as defined in the security assurance strategy through interaction with all security engineering process areas to identify evidence at various levels of abstraction. This evidence is controlled to ensure currency with existing work products and relevancy with security assurance objectives.

Example Work Products

- security assurance evidence repository (e.g., database, engineering notebook, test results, evidence log)

  stores all evidence generated during development, testing, and use. Could take the form of a database, engineering notebook, test results, or evidence log.

Notes

Assurance work products can be developed from the system, architecture, design, implementation, engineering process, physical development environment, and physical operational environment.

continued on next page

BP 06.04 Analyze Evidence

Perform analysis of security assurance evidence.

Description

Assurance evidence analysis is conducted to provide confidence that the evidence that is collected meets the security objectives, thus satisfying the customer's security needs. An analysis of the assurance evidence determines if system security engineering and security verification processes are adequate and complete enough to conclude that the security features and mechanisms are satisfactorily implemented. Additionally, the evidence is analyzed to ensure that the engineering artifacts are complete and correct with respect to the baseline system. In the event of insufficient or inadequate assurance evidence, this analysis may necessitate revisions to the system, security work products and processes that support the security objectives.

Example Work Products

- assurance evidence analysis results
  identifies and summarizes the strengths and weaknesses of evidence in the repository.

Notes

Some assurance evidence can only be generated from a consolidation of other system engineering artifacts or inferred from a consolidation of other assurance.

continued on next page

BP 06.05 Provide Assurance Argument

Provide a security assurance argument that demonstrates the customer's security needs are met.

Description
An overall assurance argument is developed to demonstrate compliance with security assurance objectives and provided to the customer. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple levels of abstraction. The assurance argument should be reviewed for deficiencies in the presentation of evidence as well as for deficiencies in meeting security assurance objectives.

Example Work Products
- assurance argument with supporting evidence
  a structured set of assurance objectives supported by various pieces of assurance evidence.

Notes
The high-level security assurance argument might be that objectives of the relevant criteria have been met. Other possible parts of the assurance argument might address how threats to system assets have been addressed. Each of the assurance objectives is supported by relevant and sufficient evidence to meet the applicable standard of proof. This argument may be used by the customer, systems security certifier, signature authority, and users.

End of PA 06: Build Assurance Argument

PA 07: Monitor System Security Posture

Summary description	The purpose of Monitor System Security Posture is to ensure that all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security are identified and reported. The external and internal environments are monitored for all factors that may have an impact on the security of the system.
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 the security objectives.
Process area notes	Security posture indicates the readiness of the system and its environment to handle current threats, and vulnerabilities and any impact to the system and its assets. This process area then, involves the activities in PA10 Determine Security Vulnerabilities and PA05 Assess Operational Security Risk. The data gathered about both the internal and external environment is analyzed both in its own context and in relation to other data that may result from events occurring before, in parallel with, or after an event in question. The process area addresses both the target environment intended for the system and the environment in which the system is developed. Any particular system has to function in conjunction with existing systems which can affect its overall security, thus these existing systems should be included in the monitoring.

continued on next page

Base practices list

The following list contains the base practices that are essential elements of good systems security engineering:

BP 07.01	Analyze event records to determine the cause of an event, how it proceeded, and likely future events.
BP 07.02	Monitor changes in threats, vulnerabilities, impacts, risks, and the environment.
BP 07.03	Identify security relevant incidents.
BP 07.04	Monitor the performance and functional effectiveness of security safeguards.
BP 07.05	Review the security posture of the system to identify necessary changes.
BP.07.06	Manage the response to security relevant incidents.
BP.07.07	Ensure that the artifacts related to security monitoring are suitably protected.

continued on next page

BP 07.01 Analyze Event Records

Analyze event records to determine the cause of an event, how it proceeded, and likely future events.

Description
Examine historical and event records (compositions of log records) for security relevant information. The events of interest should be identified along with the factors used to correlate events among multiple records. Multiple event records can then be fused into a single event record.

Example Work Products
- descriptions of each event
  identifies the source, impact, and importance of each detected event.
- constituent log records and sources
  security related event records from various sources.
- event identification parameters
  describe which events are and are not being collected by various parts of a system.
- listing of all current single log record alarm states
  identifies all requests for action based on single log records.
- listing of all current single event alarm states
  identifies all requests for action based on events which are formed from multiple log records.
- periodic report of all alarm states that have occurred
  synthesizes alarm listings from multiple systems and does preliminary analysis.
- log analysis and summaries
  performs analysis on the alarms that have occurred recently and reports the results for broad consumption.

continued on next page

BP 07.01 Analyze Event Records (cont.)

Notes

Many audit logs are likely to contain information related to a single event. This is particularly the case in a distributed/networked environment. Often an event leaves a trace in multiple locations across the network. To ensure that individual records are valuable and contribute to a complete understanding of the event and its behavior, the individual log records need to be combined or fused into a single event record.

Analysis can be performed on single records and on multiple records. Analysis of multiple records of the same type often uses statistical or trend analysis techniques. Analysis of multiple records of different types may be performed on log records and event (fused) records, although it is more normal to perform multiple event record analysis on the same type of events.

Alarms, i.e. requests for action based on a single occurrence, should be determined for both log records and fused event records. Log and event records from the development environment also need to be included in the analysis.

continued on next page

BP 07.02 Monitor Changes

Monitor changes in threats, vulnerabilities, impacts, risks, and the environment.

Description
Look for any changes that may impact the effectiveness of the current security posture, either positively or negatively.

The security implemented for any system should be in relation to the threats, vulnerabilities, impacts and risks as they relate to its environment both internal and external. None of these are static and changes influence both the effectiveness and appropriateness of the system's security. All must be monitored for change, and the changes analyzed to assess their significance with regard to the effectiveness of the security.

Example Work Products
- report of changes
  identifies any external or internal changes that may affect the security posture of the system.
- periodic assessment of significance of changes
  performs analysis on changes in security posture to determine their impact and need for response.

Notes
Both internal and external sources should be examined as well as the development and operational environments.

When changes are noted a response should be triggered, usually a review of the risk analysis or part thereof. See PA05 Assess Operational Security Risk.

continued on next page

BP 07.03 Identify Security Incidents

Identify security relevant incidents.

Description

Determine if a security relevant incident has occurred, identify the details, and make a report if necessary. Security relevant incidents may be detected using historical event data, system configuration data, integrity tools, and other system information. Since some incidents occur over a long period of time, this analysis is likely to involve comparison of system states over time.

Example Work Products

- incident list and definitions
  identifies common security incidents and describes them for easy recognition.
- incident response instructions
  describes the appropriate response to security incidents that arise.
- incident reports
  describes what incident occurred and all relevant details, including source of the incident, any damage, response taken, and further action required.
- reports related to each intrusion event detected
  describes each intrusion event detected and provides all relevant details, including the source, any damage, response taken, and further action required.
- periodic incident summaries
  provides a summary of recent security incidents, noting trends, areas that may require more security, and possible cost savings from lowering security.

continued on next page

BP 07.03 Identify Security Incidents (cont.)	*Notes* Security incidents can occur in both the development and operational environment. These incidents can impact the system being developed or the operational system in different ways. Deliberate technical attacks by hackers or malicious code (viruses, worms, etc.) necessitate a different approach than protection against random events. Analysis of the system configuration and state is required to detect the attacks. Appropriate response plans should be prepared, tested and put into action. Many technical attacks require rapid, predefined response to minimize the ongoing spread of the damage. In many cases uncoordinated responses can make the situation worse. In the cases that necessitate it, the response should be identified and defined (BP.07.06).

continued on next page

BP 07.04 Monitor Security Safeguards

Monitor the performance and functional effectiveness of security safeguards.

Description

Examine the performance of safeguards to identify changes in the performance of the safeguard.

Example Work Products

- periodic safeguard status
  describes the state of the existing safeguards in order to detect possible misconfiguration or other problems.
- periodic safeguard status summaries
  provides a summary of the state of existing safeguards, noting trends, needed improvements, and possible cost savings from lowering security.

Notes

Safeguards protecting the development and operational environments should be monitored. Many safeguards can be left in an inappropriate or non-effective state after use. Many safeguards provide indications of their current status, effectiveness and maintenance requirements. All three aspects need to be reviewed on a periodic basis.

continued on next page

BP 07.05 Review Security Posture

Review the security posture of the system to identify necessary changes.

Description

The security posture of a system is subject to change based on the threat environment, operational requirements, and system configuration. This practice re-examines the reasons why security was put in place and the requirements security places on other disciplines.

Example Work Products

- security review
  contains a description of the current security risk environment, the existing security posture, and an analysis of whether the two are compatible.
- risk acceptance review
  a statement by the appropriate approval authority that the risk associated with operating the system is acceptable.

Notes

A review of the security posture should be conducted in the light of the current operational environment and changes that have occurred. If other events, such as changes, have not triggered a complete review of security, a review should be triggered based on the time since the last review. Time triggered reviews should be in compliance with appropriate policy and regulations. The review should lead to a reassessment of the adequacy of current security and the appropriateness of the current level of risk acceptance. The review should be based on the organizations approach to security assessment, see PA05 Assess Security Risk. In the same manner that the operational environment is reviewed, the development environment in which the systems is created should also be periodically reviewed. In fact, the development environment can be considered as an operational environment for the development of systems.

continued on next page

BP 07.06 Manage Security Incident Response

Manage the response to security relevant incidents.

Description

In many cases, the continued availability of systems is critical. Many events can not be prevented, thus the ability to respond to disruption is essential. A contingency plan requires the identification of the maximum period of non-functionality of the system; the identification of the essential elements of the system for functionality; the identification and development of a recovery strategy and plan; testing of the plan; the maintenance of the plan.

In some cases contingencies may include incident response and active engagement of hostile agents (e.g. viruses, hackers etc.)

Example Work Products

- system recovery priority list
  contains a description of the order in which system functions will be protected and restored in the case of an incident causing failure.
- test schedule
  contains the dates for periodic testing of the system to ensure that security related functions and procedures are operational and familiar.
- test result
  describes the results of periodic testing and what actions should be taken to keep the system secure.
- maintenance schedule
  contains the dates for all system maintenance, both upgrades and preventative.
- incident reports
  describes what incident occurred and all relevant details, including source of the incident, any damage, response taken, and further action required.
- periodic reviews
  describes the procedure to be performed during periodic reviews of the security of the system, including who is to be involved, what checks will be made, and what the output will contain.

continued on next page

BP 07.06 Manage Security Incident Response (cont.)

Example Work Products (cont.)

- contingency plans

  identifies the maximum acceptable period of system downtime, the essential elements of the system, a strategy and plan for system recovery, business resumption, situation management, and procedures for testing and maintenance of the plan.

Notes

Future events can not be pre-determined, but, unless they are to cause chaos, they must be managed. If the situation falls outside the pre-identified scenarios, it is elevated to the appropriate business management decision level.

continued on next page

BP 07.07 Protect Security Monitoring Artifacts

Ensure that the artifacts related to security monitoring are suitably protected.

Description

If the products of monitoring activities can not be depended upon they are of little value. This activity includes the sealing and archiving of related logs, audit reports and related analysis.

Example Work Products

- a listing all archived logs and associated period of retention
  identifies where artifacts associated with security monitoring are stored and when they can be disposed of.
- periodic results of spot checks of logs that should be present in archive
  describes any missing reports and identifies the appropriate response.
- usage of archived logs
  identifies the users of archived logs, including time of access, purpose, and any comments.
- periodic results of testing the validity and usability of randomly selected archived logs
  analyzes randomly selected logs and determines whether they are complete, correct, and useful to ensure adequate monitoring of system security.

Notes

The majority of monitoring activities, including auditing, produce output. This output may be acted upon immediately or recorded for later analysis and further action. The contents of the logs should be designed to aid in the understanding of what occurred during an incident, and to detect changes in trends. The output log should be managed in compliance with applicable policy and regulations. Logs must be reliable and protected from tampering or accidental damage. When the log is full it must be replaced with a new one or emptied. When the log is changed any records that are not required should be removed and other reduction actions that may be required performed. Logs should be sealed, to prevent any changes from going undetected and should be archived for the proscribed period.

End of PA 07: Monitor System Security Posture

PA 08: Administer Security Controls

Summary description	The purpose of Administer Security Controls is to ensure that the intended security for the system that was integrated into the system design, is in fact achieved by the resultant system in its operational state.
Goals	• Security controls are properly configured and used.
Process area notes	This process area addresses those activities required to administer and maintain the security control mechanisms for a development environment and an operational system. Further this process area helps to ensure that, over time, the level of security does not deteriorate. The management of controls for a new facility should integrate with existing facility controls.
Base practices list	The following list contains the base practices that are essential elements of good systems security engineering: BP.08.01 Establish responsibilities and accountability for security controls and communicate them to everyone in the organization. BP.08.02 Manage the configuration of system security controls. BP.08.03 Manage security awareness, training, and education programs for all users and administrators. BP.08.04 Manage periodic maintenance and administration of security services and control mechanisms.

continued on next page

BP 08.01 Establish Security Responsibilities

Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.

Description

Some aspects of security can be managed within the normal management structure, while others require more specialized management.

The procedures should ensure that those charged with responsibility are made accountable and empowered to act. It should also ensure that whatever security controls are adopted are clear and consistently applied. In addition, they should ensure that whatever structure is adopted it is communicated, not only to those within the structure, but also the whole organization.

Example Work Products

- an organizational security structure chart
  identifies the organization members related to security and their role.
- documented security roles
  describes each of the organizational roles related to security and their responsibilities.
- documented security responsibilities
  describes each of the security responsibilities in detail, including what output is expected and how it will be reviewed and used.
- documented security accountabilities
  describes who is accountable for security related problems, ensuring that someone is responsible for all risks.
- documented security authorizations
  identifies what each member of an organization is allowed to do.

Notes

Some organizations establish a security engineering working group which is responsible for resolving security related issues. Other organizations identify a security engineering lead who is responsible for making sure that the security objectives are attained.

continued on next page

BP 08.02 Manage Security Configuration

Manage the configuration of system security controls.

Description

Security configuration of all devices requires management. This base practice recognizes that system security relies to a great extent on a number of interrelated components (hardware, software, and procedures) and that normal configuration management practices may not capture the interrelated dependencies required for secure systems.

Example Work Products

- records of all software updates
  tracks licenses, serial numbers, and receipts for all software and software updates to the system, including date, person responsible, and a description of the change.
- records of all distribution problems
  contains a description of any problem encountered during software distribution and a description of how it was resolved.
- system security configuration
  a database describing the current state of the system hardware, software, and communications, including their location, the individual assigned, and related information.
- system security configuration changes
  describes any changes to the system security configuration, including the name of the person making the change, a description of the change, the reason for the change, and when the change was made.
- records of all confirmed software updates
  includes a description of the change, the name of the person making the change, and the date made.
- periodic summaries of trusted software distribution
  describes recent trusted software distribution activity, noting any difficulties and action items.
- security changes to requirements
  tracks any changes to system requirement made for security reasons or having an effect on security, to help ensure that changes and their effects are intentional.

continued on next page

BP 08.02 Manage Security Configuration (cont.)

Example Work Products (cont.)

- security changes to design documentation
  tracks any changes to the system design made for security reasons or having an effect on security, to help ensure that changes and their effects are intentional.
- control implementation
  describes the implementation of security controls within the system, including configuration details.
- security reviews
  describe the current state of the system security controls relative to the intended control implementation.
- control disposal
  describes the procedure for removing or disabling security controls, including transition plans.

Notes

Maintaining currency of the configuration of security controls in any system is a complex task, particularly for a large distributed system. Some aspects of the configuration itself are of vital importance to the maintenance of security. Effective security requires the recording of certain information related to the security control mechanisms that make up the system and not normally used by other disciplines. Similarly, proposed changes to an existing system must be assessed to determine the impact on the overall system security posture.

Procedures are required, particularly in a distributed environment, to ensure that all copies of a particular module of software or application are the appropriate version are the same. In addition, particularly if the software is distributed over the network itself, it is essential to ensure that the software has not become corrupted in the distribution process. These requirements apply to all software.

This base practice should ensure that the software performs only those functions that are intended; a sealed reference version is maintained; all copies of the software are the same; updates are confirmed; and the security controls configuration is known and maintained.

continued on next page

BP 08.03 Manage Security Awareness, Training, and Education Programs

Manage security awareness, training, and education programs for all users and administrators.

Description
The security awareness, training and education of all staff requires management in the same way that other awareness, training and education needs to be managed.

Example Work Products
- user review of security training material
  describes the effectiveness, applicability, and relevance of the security awareness and training material.
- logs of all awareness, training and education undertaken, and the results of that training
  tracks user understanding of organizational and system security.
- periodic reassessments of the user community level of knowledge, awareness and training with regard to security
  reviews the organizational understanding of security and identifies possible areas to focus on in the future.
- records of training, awareness and educational material
  collection of security relevant training material which can be reused throughout an organization. Can be integrated with other organizational training materials.

Notes
In this context the term users is taken to include not only those individuals who work directly with the system, but also includes all individuals who receive information from the system, either directly or indirectly, plus all administration and management.

It is vitally important that users are aware of the reasons that security is in place and the reasons for a particular security mechanism or control. In addition, it is essential that the users understand how to use the mechanism or control correctly. Thus users require initial, periodic refresher, and revised sessions when new mechanisms and controls are introduced. All users require security awareness, some users require training in the use of security mechanisms, and a few users require much more in depth security knowledge and are thus candidates for security education.

continued on next page

BP 08.04 Manage Security Services and Control Mechanisms

Manage periodic maintenance and administration of security services and control mechanisms.

Description

The general management of security services and mechanisms is similar to other service and mechanism management. This includes their protection from corruption, accidental and deliberate, and archival in compliance with legal and policy requirements.

Example Work Products

- maintenance and administrative logs
  record of maintenance, integrity checks, and operational checks performed on system security mechanisms.
- periodic maintenance and administration reviews
  contains analysis of recent system security administration and maintenance efforts.
- administration and maintenance failure
  tracks problems with system security administration and maintenance in order to identify where additional effort is required.
- administration and maintenance exception
  contains descriptions of exceptions made to the normal administration and maintenance procedures, including the reason for the exception and the duration of the exception.
- sensitive information lists
  describes the various types of information in a system and how that information should be protected.
- sensitive media lists
  describes the various types of media used to store information in a system and how each should be protected.
- sanitization, downgrading, and disposal
  describes procedures for ensuring that no unnecessary risks are incurred when information is changed to a lower sensitivity or when media are sanitized or disposed.

continued on next page

BP 08.04 Manage Security Services and Control Mechanisms (cont.)

Notes

Some examples of these services are identification and authentication (I&A); access mediation/control; and key management.

Each of the security services must involve establishing appropriate security parameters, implementing those parameters, monitoring and analyzing performance, and adjusting the parameters.

These requirements are particularly applicable to such security services as Identification and Authentication for the maintenance of users and authentication data, and access control for the maintenance of permissions.

Information assets are defined as the hardware, software, and data that belong to an organization. Some information assets may require the sensitive portions to be removed so that the remainder can be used for less sensitive purposes. Sanitization ensures that information is released to individuals who have a need to know. This may be achieved by downgrading the information or by selective removal of specific sensitive information.

Electronic media can retain residual traces of information even when it is overwritten with other information. Some media may need to be sanitized before it can be used for other less sensitive purposes. Once the useful life of magnetic media is complete it should be disposed of in a manner appropriate to the sensitivity of the residual information, which may necessitate the destruction of the media. The specific details of sanitization, downgrading, and disposal requirements are dependent upon the specific community and applicable regulations.

End of PA 08: Administer Security Controls

PA 09: Coordinate Security

Summary description

The purpose of Coordinate Security is to ensure that all parties are aware of and involved with security engineering activities. This activity is critical as security engineering cannot succeed in isolation. This coordination involves maintaining open communications between security groups, other engineering groups, and external groups. Various mechanisms may be used to coordinate and communicate the security engineering decisions and recommendations between these parties, including memoranda, documents, e-mail, meetings, and working groups.

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.

Process area notes

This process area ensures that security is an integral part of the total engineering effort. Security engineers should be part of all major design teams and working groups. It is especially important that security engineering establishes relationships with other engineering teams early in the life cycle when critical design decisions are made. This process area can be equally applied to both development and operational organizations.

Base practices list

The following list contains the base practices that are essential elements of good systems security engineering:

BP.09.01	Define security engineering coordination objectives and relationships.
BP.09.02	Identify coordination mechanisms for security engineering.
BP.09.03	Facilitate security engineering coordination.
BP.09.04	Use the identified mechanisms to coordinate decisions and recommendations related to security.

continued on next page

BP 09.01 Define Coordination Objectives

Define security engineering coordination objectives and relationships.

Description

Many other groups need to be aware of and involved with security engineering activities. The objectives for sharing information with these groups is determined by examining the project structure, information needs, and project requirements. Relationships and commitments with the other groups are established. Successful relationships take many forms, but must be acknowledged by all the involved parties.

Example Work Products

- information sharing agreements
  describe a process for sharing information between groups, identifying the parties involved, media, format, expectations, and frequency.
- working group memberships and schedules
  describe the organization's working groups, including their membership, roles of members, purpose, agenda, and logistics
- organizational standards
  describe the processes and procedures for communicating security related information between the various working groups and with the customer.

Notes

Coordination objectives and relationships should be defined as early as possible in the project, to ensure that communication lines are well established. The other engineering groups should define roles for security engineers in the day to day operations (e.g. sit in on reviews, attend training, review designs). If this is not done, the risk of missing a key aspect of security increases.

continued on next page

BP 09.02 Identify Coordination Mechanisms

Identify coordination mechanisms for security engineering.

Description
There are many ways that the security engineering decisions and recommendations can be shared with other groups. This activity identifies the different ways that security is coordinated on a project.

It is not uncommon to have multiple security teams working on the same project. In these situations, all the teams should be working toward a commonly understood goal. Interface identification, security mechanism selection, training and development efforts need to be conducted in such a way as to ensure that each security component operates as expected when placed in the operational system. Additionally, the security engineering efforts must be understood by all other engineering teams and engineering activities so as to allow for clean integration of security into the system. The customer must also be aware of events and activities related to security to ensure that requirements are identified and addressed appropriately.

Example Work Products
- communication plans
  include the information to be shared, meeting times, processes and procedures to be used between members of working groups and with other groups.
- communication infrastructure requirements
  identify the infrastructure and standards needed to share information between working group members and with other groups effectively.
- templates for meeting reports, message, memoranda
  describe the format for various documents, to ensure standardization and efficient work.

Notes
None.

continued on next page

BP 09.03 Facilitate Coordination

Facilitate security engineering coordination.

Description
Successful relationships rely on good facilitation. Communication between different groups with different priorities may result in conflicts. This base practice ensures that disputes are resolved in an appropriate productive manner.

Example Work Products
- procedures for conflict resolution
  identifies the approach for efficiently resolving conflicts within and between organizational entities.
- meeting agendas, goals, action items
  describes the topics to be discussed at a meeting, emphasizing the goals and action items to be addressed.
- action item tracking
  identifies the plan for working and resolving an action item, including responsibility, schedule, and priority.

Notes
None.

continued on next page

BP 09.04 Coordinate Security Decisions and Recommendations

Use the identified mechanisms to coordinate decisions and recommendations related to security.

Description

The purpose of this base practice is to communicate security decisions and recommendations among the various security engineering groups, other engineering groups, external entities, and other appropriate parties.

Example Work Products

- decisions
  communication of security related decisions to affected groups via meeting reports, memoranda, working group minutes, e-mail, security guidance, or bulletin boards
- recommendations
  communication of security related recommendations to affected groups via meeting reports, memoranda, working group minutes, e-mail, security guidance, or bulletin boards

Notes

None.

End of PA 09: Coordinate Security

PA 10: Determine Security Vulnerabilities

Summary description

The purpose of Determine Security Vulnerabilities is to determine analytically the security vulnerabilities associated with a system. This process area includes such activities as analyzing system assets, defining specific susceptibilities and vulnerabilities, and providing an assessment of the overall system vulnerability.

The terms associated with security risk and vulnerability assessment are used differently in many contexts. For the purposes of this model, susceptibilities refer to exploitable vulnerabilities, security holes, or implementation bugs within a system that are likely to be attacked by a threat. These susceptibilities are independent of any threat instantiation or attack. Once these susceptibilities are associated with a specific threat and a likelihood of being exploited, they are referred to as vulnerabilities.

This set of activities is performed any time during a system's life-cycle to support the decision to develop, maintain, or operate the system within the known environment.

Goals

- An understanding of system security vulnerabilities is reached.

Process area notes

In the system case, the activities associated with this process area often depend on an established understanding of the operational threats and system functions of operational importance. Obtaining these operational understandings is the focus of PA05 Assess Security Risks. In the case of products, the activities of this process area are often conducted without such understandings; in this case, generic understandings are used. The analyses and practices associated with this process area are typically "paper-studies" and in this way differ from those associated with active attacks as in PA04 Attack Security. Activities associated with this PA may or may not use results from activities in PA04 Attack Security.

continued on next page

Base practices list

The following list contains the base practices that are essential elements of good systems security engineering:

BP.10.01	Select the methods, techniques, and criteria by which security vulnerabilities for the system in a defined environment are analyzed, assessed, and compared.
BP.10.02	Identify system assets that support the key operational capabilities or the security objectives of the system.
BP.10.03	Identify the potential attacks (both natural and human-based) to specific system assets.
BP.10.04	Identify vulnerabilities in the system.
BP.10.05	Assess the overall system vulnerability that results from the specific vulnerabilities, individually or in aggregate.

continued on next page

BP 10.01 Select Vulnerability Analysis Method

Select the methods, techniques, and criteria by which security vulnerabilities for the system in a defined environment are analyzed, assessed, and compared.

Description

This base practice consists of defining the method for establishing security vulnerabilities for the system in a defined environment in a way that permits them to be analyzed, assessed, and compared. This should include a scheme for categorizing and prioritizing the vulnerabilities based on susceptibilities, threats and their likelihood, operational functions, security requirements, or areas of concern when provided.

Example Work Products

- vulnerability analysis method
  identifies the approach for finding and addressing system security vulnerabilities, including the analysis, reporting, and tracking process.
- vulnerability analysis formats
  describes the format of the results of a vulnerability analysis to ensure a standardized approach.

Notes

The vulnerability analysis method can be an existing one, tailored one, or one specific to the operational aspects and defined environment for the system. It often is based on or compliments the risk analysis methodology selected in PA05 Assess Operational Security Risk. Note that understandings about threats and operational capabilities and operational value are not also provided, in which case the methodology must either narrow its scope or adopt some assumptions.

continued on next page

BP 10.02 Analyze System Assets

Identify system assets that support the key operational capabilities or the security objectives of the system.

Description

Identify system resources and data necessary to support the security objectives or the key operational capabilities (operational, business, or mission functions) of the system. Define each of these assets by assessing the significance of each asset in providing such support within a defined environment.

Example Work Products

- product asset analysis
  contains an identification of the product assets and their significance to the operation of the system.
- system asset analysis
  contains an identification of the system assets and their significance to the operation of the system.

Notes

Assets are typically categorized as data and resources. This includes not only information, but system ones as well (e.g., communication, data retrieval, applications, or printing resources). The importance of these assets can be interpreted as its significance to the value and criticality of the capabilities it supports in the defined environment. These assets need not be just security mechanisms; they can include non-security mechanisms that support a security function or work in concert with security mechanisms. In some cases, this practice is a review of the work from PA02 Provide Security Input and PA03 Verify and Validate Security.

continued on next page

BP 10.03 Identify Threats

Identify the potential threats (both natural and human-based) to specific system assets.

Description

The purpose of this base practice is to define specific threats to the system, i.e., postulated or known attacks as well as their likelihood of occurrence. Threats may be prioritized by their likelihood of attack or the amount of effort they are likely to expend.

Example Work Products

- threat analysis
  identifies the potential threats to the system.
- attack analysis
  prioritizes the threats by the likelihood of their being attacked.

Notes

In this practice, operational threats are translated into system threats and are analyzed to project attacks against the system. This assessment also can include the identification and analysis of multiple concurrent threats, where the likelihood of several threats applied in parallel or in tandem is analyzed. Because threats to assets can change, and often do as attackers learn new ways to attack the assets, the threat assessment activity can be iterative and can be conducted multiple times in the defined environments.

continued on next page

BP 10.04 Identify Vulnerabilities

Identify vulnerabilities in the system.

Description

System vulnerabilities may be found in both security and non-security refined assets (e.g., specific mechanisms). In many cases, non-security mechanisms that support security functions or work in concert with security mechanisms are found to have exploitable susceptibilities. These susceptibilities are analyzed based on the prioritized operational functions from PA05 Assess Operational Security Risk.

Example Work Products

- susceptibilities list

  describes the susceptibility of the system to various attacks, and can be organized by the likelihood of success.

Notes

In this practice, susceptibilities are seen as inherent to the system without consideration of the likelihood of any threats. The analyses of such susceptibilities may be prioritized in accordance with threat analysis.

continued on next page

BP 10.05 Synthesize System Vulnerability

Assess the overall system vulnerability that results from the specific vulnerabilities, individually or in aggregate.

Description

Analyze which vulnerabilities or combination of vulnerabilities result in operational problems for the system. Analysis should consider the additional characteristics of the vulnerability including: likelihood of threat attempting an exploitation of the vulnerability, chance for successful exploitation, and the risk of the threat agent.

Example Work Products

- vulnerability assessment report
  includes a quantitative or qualitative description of the vulnerabilities that result in an operational problem for the system, including the likelihood of attack, likelihood of success, and the impact of the attack.

Notes

The method used to analyze the vulnerabilities may be qualitative or quantitative, and should be included in the method for determining security vulnerability. Often analysis of vulnerabilities includes a reflection of likelihood.

End of PA 10: Determine Security Vulnerabilities

SSE-CMM Project and Organization PAs

Security considerations

The SSE-CMM adopts the Project and Organization PAs from the SE-CMM and interprets the SE-CMM PAs in the context of security engineering. Rather than change the SE-CMM PAs themselves, a SSE-CMM interpretation sheet is provided for each PA, listing security considerations for that PA. The interpretation sheet is to be used in conjunction with the SE-CMM PAs which are included in Appendix E.

Each PA interpretation sheet includes the following information:

Applicable SE-CMM PA. This section provides the reference to the SE-CMM PA.

Security considerations. This section indicates what needs to be changed in the SE-CMM PA when it is applied in the context of security engineering.

Security engineering relationships. This section provides references to SSE-CMM PAs.

Security considerations

In addition to the specific considerations on the interpretation sheet for each PA, the following are general considerations with respect to security engineering for all of the Project and Organization PAs:

Program vs. Security Risk. The Project and Organization PAs use the term "risk." In these cases, the reference to "Program Risk" is risk related to the successful completion of a project, addressing issues related to cost and schedule. The Engineering PAs address "Security Risk" activities as determining whether operational impacts due to residual security vulnerabilities are tolerable. Results of security risk assessments may provide input to, and influence program risk management activities, though project and Organization PAs do not address management of security risks referenced in the Engineering PAs.

Applicability to Operational Phase. Although the wording of the Project and Organization PAs seem to imply applicability to only development aspects, the PAs apply equally to the operation and maintenance phase of a life cycle. The PAs will need to be interpreted for an assessment or improvement purposes based on the view of the PAs that are applicable to an organization. The exceptions are noted in the SSE-CMM cover page.

Security Engineering vs. Systems Engineering. The term "Systems Engineering" is used throughout the Project and Organization PAs (for example, "Improve Organization's Systems Engineering Processes"). The use of these PAs, however, are broadly applicable. The term "Systems Engineering" should be substituted with the term "Security Engineering" when the PAs are applied in the context of security engineering. PAs also need to address the security engineering perspective by ensuring the integration of security engineering with other engineering disciplines.

Engineering Relationships. Systems engineering and security engineering relationships are indicated for each PA. Note there are many relationships between the various PAs (only the major relationships are identified).

SE-CMM PA Relationships. The SSE-CMM has adopted the Project and Organization PAs from the SE-CMM. These PAs have been integrated into the SSE-CMM and assigned an SSE-CMM PA number. The adopted SE-CMM PAs themselves are located in Appendix E and the SSE-CMM PA interpretation sheets are provided in the following pages of this section. PA references within each SE-CMM PA in Appendix E are references to the original SE-CMM PAs (they have not been modified).

PA 11: Ensure Quality

Applicable SE-CMM PA	SE-CMM PA 08 Ensure Quality [Appendix E, page E-1]
Security considerations	None.
Security engineering relationships	PA06 Build Assurance Argument is related to ensure quality. Assurance can be considered a specific type of security related quality.

PA 12: Manage Configurations

Applicable SE-CMM PA	SE-CMM PA 09 Manage Configurations [Appendix E, page E-8]
Security considerations	In BP02 the determination of the level of configuration units identified for a system/project should consider the level of detail required by the assurance objectives in PA06 Build Assurance Argument.
Security engineering relationships	Manage Configurations provides evidence to PA06 Build Assurance Argument. Also, the CM system selected should itself be managed according to PA08 Administer Security Controls.

PA 13: Manage *Program* Risk

Applicable SE-CMM PA	SE-CMM PA 10 Manage Risk [Appendix E, page E-14]
Security considerations	Manage Program Risk refers to risk related to the successful completion of the project, addressing issues related to cost and schedule. The Engineering PAs address "Security Risk" activities, that is determining whether operational impacts due to residual security vulnerabilities are tolerable. Results of security risk activities may provide input to and influence program risk management activities.
Security engineering relationships	PA09 Coordinate Security should be taken into account to ensure that security issues are addressed.

PA 14: Monitor and Control Technical Effort

Applicable SE-CMM PA	SE-CMM PA 11 Monitor and Control Technical Effort [Appendix E, page E-21]
Security considerations	None.
Security engineering relationships	PA07 Monitor System Security Posture and PA08 Administer Security Controls need to be taken into account both during the development effort and during the operation of the system. PA09 Coordinate Security should be taken into account to ensure that security issues are addressed.

PA 15: Plan Technical Effort

Applicable SE-CMM PA	SE-CMM PA 12 Plan Technical Effort [Appendix E, page E-27]
Security considerations	None.
Security engineering relationships	PA09 Coordinate Security should be taken into account, particularly during the performance of BP05 Identify Technical Activities for the entire life cycle of the project, and BP06 Define Project Interface to support effective interaction with the customers and suppliers.

PA 16: Define Organization's Security Engineering Process

Applicable SE-CMM PA	SE-CMM PA 13 Define Organization's System Engineering Process [Appendix E, page E-38]
Security considerations	In Define Organization's System Engineering Process, the term "Systems Engineering" is used. This PA however, is broadly applicable and the term "Systems Engineering" is substituted with the term "Security Engineering" when assessing an organization's security engineering capability. In addition, BPs need to address the integration of security engineering with systems engineering and other engineering disciplines.
Security engineering relationships	PA09 Coordinate Security should be taken into account when defining the organization's security engineering process.

PA 17: Improve Organization's Security Engineering Processes

Applicable SE-CMM PA	SE-CMM PA 14 Improve Organization's System Engineering Processes [Appendix E, page E-43]
Security considerations	In Improve Organization's Systems Engineering Processes, the term "Systems Engineering" is used. This PA however, is broadly applicable and the term Systems Engineering is substituted with the term "Security Engineering" when assessing an organization's security engineering capability. In addition, BPs need to address the integration of security engineering with systems engineering disciplines.
Security engineering relationships	None.

PA 18: Manage Security Product Line Evolution

Applicable SE-CMM PA	SE-CMM PA 15 Manage Product Line Evolution [Appendix E, page E-48]
Security considerations	Product lines consisting of security products have special requirements which include: stringent configuration management practices; personnel clearance requirements for the development of secure code; and obtaining certification and accreditation of secure products. All of these requirements add to the length of the product development cycle and life cycle costs.
Security engineering relationships	PA06 Build Assurance Argument is related to ensure that new or modified products continue to meet the customer's security needs.

PA 19: Manage Security Engineering Support Environment

Applicable SE-CMM PA	SE-CMM PA 16 Manage Systems Engineering Support Environment [Appendix E, page E-52]
Security considerations	The development of products in the COMSEC and trusted software development environments will present unique requirements in BP02, BP03 and BP04, such as assurance needs cleared personnel and chain of custody.
Security engineering relationships	The Security Engineering Support Environment should be included in the activities of PA05 Assess Operational Security Risk. PA06 Build Assurance Argument should be affirmed through a properly managed Security Engineering Support Environment.

PA 20: Provide Ongoing Skills and Knowledge

Applicable SE-CMM PA	SE-CMM PA 17 Provide Ongoing Skills and Knowledge [Appendix E, page E-60]
Security considerations	Training needs to be provided in the organization's security engineering process.
Security engineering relationships	None.

PA 21: Coordinate with Suppliers

Applicable SE-CMM PA	SE-CMM PA 18 Coordinate with Suppliers [Appendix E, page E-69]
Security considerations	None.
Security engineering relationships	The assessed organization acts as the customer when the supplier executes PA01 Specify Security Needs.

Appendix A: Change Request Form

Appendix A: Change Request Form

SECTION I: TO BE COMPLETED BY REVIEWER			
Name/Organization:	Phone:	Email:	
Problem Title:	p MODEL p Architecture p PAs p Terminology p _____	p APPLICATION p Appraisal Method p Pilots p Assurance p _____	p PROJECT p Sponsorship p Participation p Schedule p _____
Description of problem (use back if needed):			
Impact if the problem is not resolved:			
Possible solutions:			
SECTION II: TO BE COMPLETED BY SSE-CMM STEERING GROUP			
p Accepted p Rejected Priority: p High p Medium p Low Rationale:			
Action Required:			
Disposition:			
Assigned to: p Sponsorship & Adoption p Planning & Infrastructure p Author WG p Application WG p _____			
Due Date:			

Appendix B: Approved Model Requirements

Appendix B: Approved Model Requirements

1.0 Introduction

This appendix establishes the requirements for the Systems Security Engineering Capability Maturity Model (SSE-CMM). The requirements will be used by the SSE-CMM Author Working Group as the basis for development of the model. Any deviance from these requirements must have written approval from the SSE-CMM Steering Group.

1.1 Document Purpose

The purpose of this document is to identify the requirements for the SSE-CMM. The requirements are presented in three sections:

Section 2. identifies the requirements that apply to the SSE-CMM model document;
Section 3. identifies the requirements that apply to the model;
Section 4. identifies the requirements that apply to the process of developing the model.

1.2 Document Scopejwa[4]

This document identifies only those requirements that apply to the model and its development and revision. Requirements for the application of the model, i.e., in appraisals and with respect to its use for assurance, are not covered in this document.

1.3 Document Terminologyjwa[5]

Within this document the term ‘shall’ indicates a mandatory requirement.

continued on next page

1.4 Background **jwa**[6]

1.4.1 Project Structure **jwa**[7]

The SSE-CMM Project is organized into three main working groups. Implementation of the SSE-CMM Project direction and strategy is the responsibility of the Steering Group. Working groups responsible for producing the SSE-CMM work products include the SSE-CMM Author Group and the SSE-CMM Application Group. The Author Group is responsible for developing the model while the Application Group is responsible for producing the methods and tools for applying the model (e.g., appraisal methods, questionnaire).

1.4.2 Project Goal **jwa**[8]

Provide a SSE-CMM, as well as an associated appraisal method and other instruments (e.g., questionnaire, training plan) that:

1) support improvement of an organization's security engineering practice;
2) provide an industry-wide framework for the assessment of security engineering capabilities; and
3) provide a foundation for capability-based assurance.

1.5 Document Changes **jwa**[9]

The requirements within this document will be modified as necessary by direction of the SSE-CMM Steering Group upon recommendation from Steering Group members or either the SSE-CMM Author or Applications Working Groups. A Change Request Form shall be provided in the SSE-CMM document for community-suggested revisions to the model and model requirements.

continued on next page

2.0 Document Requirements

The requirements that apply to the contents and structure of the SSE-CMM document are identified in this section.

2.1 Document Contents	This section identifies the contents of "The Systems Security Engineering Capability Maturity Model." At a minimum, the following topics shall be covered within the document.
2.1.1 Executive Summary	The history, purpose, and goals of the model shall be presented. The summary shall provide a brief overview of the model, including a brief description of its structure and its relation to other efforts.
2.1.2 Introduction	A brief presentation of the history of the Project and the Project organization shall be given. Project work products shall be identified and their relationship to this document described. The document structure shall be described.
2.1.3 Security Engineering	The view of security engineering that is used within the model shall be presented. It shall include a description of the scope of the discipline. A high-level view of the process components of security engineering shall be provided.
2.1.4 Model Architecture	A description of the SSE-CMM shall be provided.
2.1.4.1 Relation to Foundation Models	The foundation models for the SSE-CMM shall be identified and described. The methodology used to relate the SSE-CMM to the foundation models shall be described.
2.1.4.2 Structure	The structure of the model, to include the capability level structure, the process categories, process areas, and any other components needed to understand the model shall be presented. Relationships between these components shall be described.

continued on next page

2.1.5 Process Areas and Practices	Each of the SSE-CMM Process Areas (PAs) shall be presented. The PAs shall include the base practices for security engineering. The structure of the PAs shall be based on the foundation model.

2.1.6 Glossary	A glossary of the security engineering terms used in the SSE-CMM shall be provided as an appendix.
2.2 Style Guide	The styles for SSE-CMM work shall be based on the format of the foundation model as specified in Section 3.2.1.

continued on next page

3.0 Model Requirements

	The requirements that apply to the SSE-CMM are identified in this section.
3.1 Scope of Model	
3.1.1 Independence	The practices defined in the model shall be independent from the implementation of a specifically defined process.
3.1.2 Coverage	
3.1.2.1 Engineering Aspects	The model shall address security engineering and management practices with regard to any and all aspects of developing secure systems/products or providing security engineering services. Examples include hardware, software, communications, developer certification support activities in a product, system, or enterprise context.
3.1.2.2 Levels of Abstraction	The model shall address security engineering and management practices with regard to all levels of abstraction, from concept definition to mechanism implementation.
3.1.2.3 Life Cycle	The model shall cover security engineering practices from concept definition through development, integration/test, operation and maintenance, and decommissioning. The model shall not cover security engineering activities performed by system acquisition, system certification, or product organizations.

continued on next page

3.1.3 Applicability	
3.1.3.1 Organizations	The model shall be applicable to organizations regardless of their size or structure. The model shall be applicable to commercial, government, and academic organizations that practice security engineering. The model shall be applicable to security engineering service organizations.
3.1.3.2 Projects	The model shall be applicable to all projects that have security implications within the organization regardless of type, size, and scope.
3.1.3.3 End-Products	The model shall be applicable to security engineering practices for secure systems, products, and components.
3.1.4 Purpose	The SSE-CMM shall be developed with the following intended uses: • as a tool for engineering organizations to evaluate and define improvements to their security engineering practices; • as a standard mechanism for customers to evaluate a provider's security engineering capability; and • as a basis for security engineering evaluation organizations (e.g., system certifiers and product evaluators) to establish capability-based confidences (as an ingredient to system or product assurance).
3.1.5 Application of Model	The SSE-CMM shall support three types of appraisals: as part of an SE-CMM appraisal; as a delta to a previously completed SE-CMM appraisal; by itself, without an SE-CMM appraisal.

continued on next page

3.2 The Model

3.2.1 Foundation Models	The Systems Engineering CMM (SE-CMM) [SEI94] shall be the basis for the structure of the SSE-CMM. The structure of the SE-CMM is based on the International Organization for Standardization (ISO) Software Process Improvement and Capability dEtermination (SPICE) Baseline Practices Guide. The content of the Security Engineering CMM Strawman [NSA94] shall be used as input to the security engineering PAs and practices of the SSE-CMM.
3.2.2 Dependence /Independence	Although based upon the foundations model identified in Section 3.2.1, the SSE-CMM shall be developed independently to address the maturity of security engineering, management, and organization aspects. The model provides the basis for measuring security as a specialty engineering discipline that is complementary to other engineering disciplines.

continued on next page

3.2.3 Content	The model shall define the necessary Organizational, Management, and Engineering process areas for security engineering.
3.2.4 Terminology	The SSE-CMM should provide a common language for communication about the domain of security engineering.
3.2.4.1 Process Improvement	Process improvement/measurement terminology shall, to the extent possible, be consistent with those in the Systems Engineering CMM. In the event of conflict, those defined within the SSE-CMM shall take precedence.
3.2.4.2 Security Engineering	Security engineering terminology shall be consistent with [NSTIS]. In the event of conflict, those defined within the SSE-CMM shall take precedence.

continued on next page

4.0 Process Requirements

The requirements that apply to the process of developing the SSE-CMM are identified in this section.

4.1 Incremental Development

The SSE-CMM shall be developed in increments that correspond to the Project Phases as follows:

Conceive:	Review Current Work; Research Model Development Security Engineering CMM Development Workbook
Develop I:	Form Working Groups; refine initial model into a Draft SSE-CMM.
Develop II:	Pilot and test the Draft SSE-CMM and SSE-CMM Appraisal Method.
Develop III:	Revise and publish SSE-CMM v1.0.
Operate and Maintain:	Continually apply and update the SSE-CMM version X.X.

4.2 Change Management

The process for changes to the SSE-CMM are documented in the Project Master Plan maintained by the Steering Group.

continued on next page

4.3 Validation

Model validation shall be through: 1) use of pilot appraisals; and 2) field experience.

4.3.1 Pilot Appraisals

To validate various aspects of the model and provide adequate input to SSE-CMM v1.0, pilot appraisals shall, to the extent possible, be accomplished on diverse organizations with regard to:

Size:	organizations of various sizes;
Focus:	both contract-driven system development and market-driven product development environments;
Assurance:	both high and low assurance developments;
Perceived Maturity:	at least one project or organization perceived to have a mature process capability;
Type of Organization:	both development and service provider organizations

4.3.2 Field Experience

To continue validation of the SSE-CMM v1.0, data on application of the model in diverse organizations as identified in Section 4.3.1 shall be collected as input to update the model.

continued on next page

Derivation of SSE-CMM Requirements

The requirements herein contained were produced using material garnered from project participants as recorded in the documents listed below.

Sources list

	SSE-CMM Author Group Meetings.
	SSE-CMM Steering Group Meetings.
[SEI94]	Systems Engineering CMM Project, "A Systems Engineering Capability Maturity Model, Version 1.0," CMU/SEI-94-HB-04, December 1994.
[NSA94]	National Security Agency, "Security Engineering CMM Development Workbook," November 1994.
[NSA95]	Security Engineering CMM Project, "Security Engineering CMM Project Master Plan," February 6, 1995.
[NSTIS]	NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary.

end of SSE-CMM Requirements

Appendix B: Approved Model Requirements

Appendix C: Bibliography

Appendix C: Bibliography

Bibliography

This bibliography includes references within the document and also other documents related to the subject area. The bibliography includes references in the following subject areas:

Security Engineering
Security Engineering Process Areas
Systems/Software Engineering
Systems/Software Process
Capability Maturity Models

Appendix C: Bibliography

C.1 Security Engineering

BAUER91 Bauer, R.K., Sachs, J., Weidner, M.L., Wilson, W.F., "A Framework for Developing Accreditable MLS AISs," *Proceedings of the 14th National Computer Security Conference,* October 1-4, 1991.

BENZEL89 Benzel, T. C. V., "Integrating Security Requirements and Software Development Standards," *Proceedings of the 12th National Computer Security Conference,* 10-13 October 1989.

CCEB96 Common Criteria Editorial Board, "Common Criteria for Information Technology Security Evaluation," Version 1.0, January 31, 1996.

CTCPEC93 Canadian Systems Security Centre, Communications Security Establishment, Government of Canada, "The Canadian Trusted Computer Product Evaluation Criteria," Version 3.0e, January 1993.

DAWSON93 Dawson M., Moses T., Maj Fletcher T.J. "A Method for Designing Secure System Architecture." *Proceedings, 5th Annual Canadian Computer Security Symposium,* 1993.

DOD85 Department of Defense, "Department of Defense Trusted Computer System Evaluation Criteria," DOD 5200.28-STD, December 1985.

GAMBEL93 Gambel, Daniel; Fowler, Joan, "Composing Trusted Systems Using Evaluated Products," *Proceedings of the Fifth Annual Canadian Computer Security Symposium,* 1993.

HINTON93 Hinton, Heather; Lee, E. Stewart, "Secure Composition Based on Environmental Considerations," *Proceedings of the Fifth Annual Canadian Computer Security Symposium,* 1993.

HOPKINSON95 Hopkinson, J. "Security Architecture Framework," *Proceedings of the Seventh Annual Canadian Computer Security Symposium,* 1995.

HOWE92 Howe, D. "Information System Security Engineering: Cornerstone to the Future," *Proceedings of the 15th National Computer Security Conference,* Baltimore, MD, Vol. 1, October 15, 1992. pp. 144-251.

ISO/IEC 11770 International Organization for Standardization, "Information Technology - Security Techniques - Key Management - Part 1: Framework.

ISO/IEC 13335 International Organization for Standardization, "Information Technology - Security Techniques - Guidelines for the Management of IT Security". (All Parts)

ISO/IEC 14516 International Organization for Standardization, "Information Technology - Security Techniques - Guidelines for the Use and Management of Trusted Third Parties". (All Parts)

ISO/IEC 15408 International Organization for Standardization, "Information Technology - Security Techniques - Evaluation Criteria for IT Security" (Common Criteria) (All parts).

ITSEC91 Information Technology Security Evaluation Criteria, Harmonized Criteria of France-Germany-the Netherlands-the United Kingdom (ITSEC), V1.2, June 1991.

ITSEM92 Information Technology Security Evaluation Manual (ITSEM), Draft V0.2, 2 April 1992.

JOYNES95 Joynes, M. "Architecture Integration with a service view," *Proceedings of the Seventh Annual Canadian Computer Security Symposium*, 1995.

LONGLEY Longley, Dennis; Shain, Michael; Caelli, William, *Information Security Dictionary of Concepts, Standards and Terms*.

MARMOR89 Marmor-Squires, A., Danner, B., McHugh, J., Nagy, L., Sterne, D., Branstad, M., Rougeau, P., "A Risk Driven Process Model for the Development of Trusted Systems," *Proceedings of the Fifth Annual Computer Security Applications Conference*, December 4-8, 1989.

NCSC88 National Computer Security Center, "Glossary of Computer Security Terms," 21 October 1988.

NIST National Institute of Standards and Technology, "An Introduction to Computer Security: The NIST Handbook".

NSA93C National Security Agency Central Security Service, "Information Systems Security Engineering Handbook," December 17, 1993.

NSTISSI92 National Security Telecommunications and Information Systems Security, "National Information Systems Security (INFOSEC) Glossary," NSTISSI No. 4009, June 5, 1992.

C.2 Security Engineering Process Areas

CSE	Communication Security Establishment, "A Framework for Security Risk Management for Information Technology Systems," Ottawa, GOC.
CSE95	Communication Security Establishment, "A Guide to Risk Management and Safeguard Selection for Information Technology Systems," Ottawa, GOC, 1995.
DOE90	National Institute of Standards and Technology, "Department of Energy Risk Assessment Methodology," NISTIR 4325, May 1990
DOD92b	Department of Defense, Strategic Defense Initiative Organization, "Trusted Software Methodology" Volumes 1 & 2, SDI-S-SD-000007, June 17, 1992.
DOJ90	National Institute of Standards and Technology, "Department of Justice Simplified Risk Analysis Guidelines," NISTIR 4387, August 1990.
KEMMERER83	Kemmerer, R.A., "Shared Resource Matrix Methodology: An approach to Identifying Storage and Timing Channels," *ACM Trans. on Computer Sys.*, Vol 1 No. 3, August 1983.
LINDE75	Linde, R.R, "Operating Systems Penetration," *AFIPS Conference Proceedings*, Vol. 44, 1975 National Computer Conference, AFIPS Press, Arlington VA, 1975.
NIST94a	National Institute of Standards and Technology, "A Head Start on Assurance: Proceedings of an Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness," NISTIR 5472, March 21-23, 1994.
NIST94b	National Institute of Standards and Technology, "Proceedings Report of the International Invitational Workshop on Developmental Assurance,", NISTIR 5590, June 16-17, 1994.
NORVELL89	Norvell, W., "Integration of Security into the Acquisition Life Cycle," *Proceedings of the 12th National Computer Security Conference*, 10-13 October 1989.
NSA93a	National Security Agency, "Rating Maintenance Phase Program Document" (DRAFT), Version 2.0, October 1993
NSA93c	National Security Agency Central Security Service, "Information Systems Security Engineering Handbook," December 17, 1993.
SDI92b	GE (for Strategic Defense Initiative Organization), "Trusted Software Key Process Area," Initial Issue, 30 September 1992.
SMITH90	Smith, S.T.; Jalbert, M.L., "LAVA/CIS Version 2.0: A Software System for Vulnerability and Risk Assessment," *Proceedings of the 13th National Computer Security Conference*, Volume II, 1 Oct 1990.

WICHERS94 Wichers, D.; Landoll, D., Sachs, J., "What Color is Your Assurance?," Proceedings of the 1994 National Computer Security Conference, October 11-14, 1994.

C.3 Systems/Software Engineering

BASS91 Bass, Len, and Coutaz, Joelle, *Developing Software for the User Interface*, 1991, 51046.

BROOKS95 Brooks, Frederick P., "The Mythical Man-Month," *Essays on Software Engineering, Anniversary Edition*, 1995, 83595.

CMU95 Carnegie Mellon University / Software Engineering Institute, "The Capability Maturity Model: Guidelines for Improving the Software Process," 1995, 54664.

GOLDBERG95 Goldberg, Adele, and Rubin, Kenneth S., *Succeeding With Objects: Decision Framework for Project Management*, 1995, 62878.

GOMAA93 Gomaa, Hassan, *Software Design Methods for Concurrent and Real-Time Systems*, 1993, 52577.

GRAHAM93 Graham, Ian, *Object-Orientated Methods*, Second Edition, 1993, 59371.

HUMPHREY95 Humphrey, Watts S., *A Discipline for Software Engineering*, 1995, 54610.

JACOBSON95a Jacobson, Ivar, et al., "The Object Advantage: Business Process Reengineering with Object Technology," *ACM Press*, 1995, 42289.

JACOBSON95b Jacobson, Ivar, et al., "The Object-Orientated Software Engineering," *ACM Press*, 1995, 42289.

LEVESON95 Leveson, Nancy G., *Safeware: System Safety and Computers*, 1995, 11972.

NEUMANN95 Neumann, Peter G., *Computer-Related Risks*, ACM Press, 1995.

SMITH90 Smith, Connie U., *Performance Engineering for Software Systems*, 1990, 53769.

WOODCOCK88 Woodcock, Jim, and Loomes Martin, *Software Engineering Mathematics*, 1988, 50424.

C.4 Systems/Software Process

ANSI87 American Society for Quality Control, "Quality Systems - Model for Quality Assurance in Design/Development, Production, Installation, and Servicing," ANSI/ASQC Q91-1987, 1987.

BERARD90 Berard, Edward, V., *Motivation for an Object-Oriented Approach to Software Engineering*, Berard Software Engineering, Inc., Germantown, Md., April 1990.

BOEHM89 Boehm, Barry, W., "A Spiral Model of Software Development and Enhancement," *Software Risk Management,* 1989, pp. 26-37.

CURTIS92 Curtis, Dr. Bill, "Software Process Improvement Seminar for Senior Executives," NIST Lecture Series on High-Integrity Systems, Gaithersburg, MD, December 1992.

DEMING86 Deming, W. Edwards, *Out of the Crisis*, Massachusetts Institute of Technology, Center for Advanced Engineering Study, Cambridge, MA, 1986.

DOD87 Office of the Under Secretary of Defense for Acquisition, Washington, D.C., "Report of the Defense Science Board Task Force on Military Software," September 1987.

DOD88a Department of Defense, "Defense System Software Development," DOD-STD-2167A, 29 February 1988.

DOD88b Department of Defense, "Life Cycle Management of Automated Information Systems (AISs)," DoDD 7920.1, June 20, 1988.

DOD92a Department of Defense, "Software Development and Documentation," Draft, MIL-STD-SDD, 22 December 1992.

DOD92b Department of Defense, "Systems Engineering," MIL-STD-499B, Draft, 6 May 1992.

FAGAN86 Fagan, M. E., "Advances in Software Inspections," *IEEE Transactions on Software Engineering*, Vol. 12, No. 7, July, 1986, pp. 744-751.

FEILER92 Feiler, P. H.; Humphrey, W. S., “Software Process Development and Enactment: Concepts and Definitions,” CMU/SEI-92-TR-4, ADA258465, March 1992.

FOWLER90 Fowler, P.; Rifkin, S., “Software Engineering Process Group Guide,” Software Engineering Institute, CMU/SEI-90-TR-24, ADA235784, September, 1990.

FREEDMAN90 Freedman, D. P.; Weinberg, G. M., *Handbook of Walkthroughs, Inspections, and Technical Reviews*, Third Edition, Dorset House, New York, NY, 1990.

Appendix C: Bibliography

HUMPHREY88	Humphrey, W. S., "Characterizing the Software Process," *IEEE Software*, Vol. 5, No. 2, March, 1988, pp. 73-79.
HUMPHREY89	Humphrey, W. S., *Managing the Software Process*, Addison-Wesley, Reading, MA, 1989.
IEEE-STD-610	ANSI/IEEE Std 610.12-1990, "IEEE Standard Glossary of Software Engineering Terminology," February 1991.
ISO91	International Organization for Standardization, "Quality Management and Quality Assurance Standards - Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply, and Maintenance of Software," ISO 9000-3, 1991.
ISO94	International Organization for Standardization, ISO 9001, "Quality Systems - Model for Quality Assurance in Design/Development, Production, Installation, and Servicing."
KITSON92	Kitson, D. H.; Masters, S., "An Analysis of SEI Software Process Assessment Results: 1987-1991," Software Engineering Institute, CMU/SEI-92-TR-24, July 1992.
MIL84	Military Standard, "System Safety Program Requirements," MIL-STD-882B, 30 March 1984.
OVER93	Over, J. W., "Motivation For Process-Driven Development," *CrossTalk - The Journal of Defense Software Engineering*, January 1993.
PERRY96	Perry, W., "What it Really, Really Means to Manage by Processes -- and How to Do it," NIST Lecture Series on High-Integrity Systems, Gaithersburg, MD, 13 May 1996.
RAO93	Rao, Bindu, R., C++ and the OOP Paradigm. McGraw-Hill, 1993.
SIEGEL90	Siegel, J. A. L., et al., "National Software Capacity: Near-Term Study," CMU/SEI-90-TR-12, ADA226694, May 1990.

C.5 Capability Maturity Models

FERRAIOLO93 Ferraiolo, K.; Sachs, J., "Determining Assurance Levels by Security Engineering Process Maturity," *Proceedings of the Fifth Annual Canadian Computer Security Symposium*, May 1993.

FERRAIOLO94A Ferraiolo, K.; Williams, J.; Landoll, D., "A Capability Maturity Model for Security Engineering," *Proceedings of the Sixth Annual Canadian Computer Security Symposium*, May 1994.

FERRAIOLO96 Ferraiolo,K.; Sachs, J., "Distinguishing Security Engineering Process Areas by Maturity Levels," *Proceedings of the Eighth Annual Canadian Computer Security Symposium*, May 1996.

GALLAGHER95 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.

GOODENOUGH93A Goodenough, J.; Klein, M., "Maturity Models for the Technical Aspects of Software Engineering," Draft, August 6, 1993.

GOODENOUGH93B Goodenough, J., "Maturity Models for the Technical Aspects of Software Engineering," Presentation at Software Engineering Symposium, September 1993.

HEFNER96 Hefner, R.; Hsiao, D.; Monroe, W., "Experience with the Systems Security Engineering Capability Maturity Model," *International Council on Systems Engineering Symposium*, July 1996.

HOSY95 Hosy, H.; Roussely, B., "Industrial Maturity and Information Technology Security," *Proceedings of the Seventh Annual Canadian Computer Security Symposium*, May 1995.

PAULK91 Paulk, M. C.; Curtis, B.; Chrissis, M. B; et al, “Capability Maturity Model for Software, Software Engineering Institute,” CMU/SEI-91-TR-24, ADA240603, August 1991.

PAULK93A Paulk, M. C.; Curtis, B.; Chrissis, M. B; Weber, C. V., “Capability Maturity Model for Software,” Version 1.1, Software Engineering Institute, CMU/SEI-93-TR-24, February 1993.

PAULK93B Paulk, M. C.; Weber, C. V.; Garcia, S.; Chrissis, Bush, M., “Key Practices of the Capability Maturity Model,” Version 1.1, Software Engineering Institute, CMU/SEI-93-TR-25, February 1993.

SEI94 Software Engineering Institute, “Benefits of CMM-BAsed Software Process Improvement: Initial Results," SEI-94-TR-013, 1994.

SEI95 Software Engineering Institute, “A Systems Engineering Capability Maturity Model,” Version 1.1, CMU/SEI-95-MM-003, November 1995.

Appendix C: Bibliography

SHERER94 — Sherer, W.; Cooper, J., Software Acquisition Maturity Model, tutorial presented at the Sixth Annual Software Technology Conference, Salt Lake City, Utah, 10 April 1994.

SPICE94 — ISO SPICE Project, SPICE Baseline Practices Guide (distributed to Systems Engineering CMM Workshop), 21 June 1994.

SSECMM97 — SSE-CMM Project, “SSE-CMM Appraisal Method Description,” Version 1.1, June 1997.

WEBER91 — Weber, C. V.; Paulk, M. C.; Wise, C. J.; Withey, J. V., “Key Practices of the Capability Maturity Model,” Software Engineering Institute, CMU/SEI-91-TR-25, ADA240604, August 1991.

ZIOR95 — Zior, M., "Community Response to CMM-Based Security Engineering Process Improvement," *Proceedings of the 1995 National Information System Security Conference*, October 1995.

Appendix D: Glossary

Appendix D: Glossary

Accountability	The property that ensures that the actions of an entity can be traced uniquely to the entity. [ISO 7498-2; 1988]
Accreditation	Formal declaration by a designated approving authority that a system is approved to operate in a particular security mode using a prescribed set of safeguards.
Assessment	An appraisal by a trained team of professionals to determine the state of an organizations current process, to determine the high-priority process-related issues facing an organization, and to obtain the organizational support for process improvement.
Asset	Anything that has value to the organization [ISO 13335-1: 1996]
Assurance	Degree of confidence that security needs are satisfied [NIST94a]
Assurance Argument	Structured reasoning supported by evidence that the claimed assurance satisfies assurance needs
Assurance Claim	An assertion or supporting assertion that a system meets its security needs. Claims address both direct threats (e.g., system data could be compromised by outsiders) and indirect threats (e.g., system code may contain flaws).
Assurance Evidence	Data on which a judgment or conclusion about an assurance claim may be based. The evidence may consist of observation, test results, analysis results, and appraisals providing support for the associated claims.
Authenticity	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information. [ISO 13335-1:1996]
Availability	The property of being accessible and useable upon demand by an authorized entity. [ISO 7498-2: 1988]
Baseline	A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. [IEEE-STD-610]
Certification	Comprehensive evaluation of security features and other safeguards of an AIS to establish the extent to which the design and implementation meet a set of specified security requirements.
Confidentiality	the property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO 7498-2:1988]
Consistency	The degree of uniformity, standardization, and freedom from contradiction among the documents or parts of a system or component. [IEEE-STD-610]
Correctness	A property of a representation of a system or product such that it accurately reflects the specified security requirements for that system or

	product.
Customer	The individual or organization that is responsible for accepting the product and authorizing payment to the service / development organization.
Data Integrity	The property that data has not been altered or destroyed in an unauthorized manner [ISO 7498-2:1988]
Effectiveness	A property of a system or product representing how well it provides security in the context of its proposed or actual operational use
Engineering Group	A collection of individuals (both managers and technical staff) which is responsible for project or organizational activities related to a particular engineering discipline (e.g. hardware, software, software configuration management, software quality assurance, systems, system test, system security).
Evidence	Directly measurable characteristics of a process and/or product that represent objective, demonstrable proof that a specific activity satisfies a specified requirement.
Group	The collection of departments, managers, and individuals who have responsibility for a set of tasks or activities. The size can vary from a single individual assigned part-time, to several part-time individuals assigned from different departments, to several dedicated full-time individuals.
Integrity	see data integrity and system integrity
Maintenance	The process of modifying a system or component after delivery to correct flaws, improve performance or other attributes, or adapt to a changed environment. [IEEE-STD-610]
Methodology	A collection of methods, procedures, and standards that define an integrated synthesis of engineering approaches to the development of a product or system.
Objective	Non-biased perspective
Penetration Profile	A delineation of the activities required to effect a penetration.
Procedure	A written description of a course of action to be taken to perform a given task. [IEEE-STD-610]
Process	A sequence of steps performed for a given purpose. [IEEE-STD-620]
Reliability	The property of consistent behavior and results. [IEEE 13335-1:1996]
Residual Risk	The risk that remains after safeguards have been implemented [IEEE 13335-1:1996]
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets [IEEE 13335-

	1:1996]
Risk Analysis	The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. [IEEE 13335-1:1996]
Risk Management	Process of assessing and quantifying risk and establishing acceptable level of risk for the organization. [IEEE 13335-1:1996]
Security Engineering	See Chapter 2, Section 3: Security Engineering
Security Policy	Rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its systems
Security Related Requirements	Requirements which have a direct effect on the secure operation of a system or enforce conformance to a specified security policy.
Signature Authority	Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.
System	A collection of components organized to accomplish a specific function or set of functions. [IEEE-STD-610] A system may include many products. A product can be the system .
Threat	Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to information or a system.
Validation	The process of assessing a system to determine whether it satisfies the specified requirements.
Verification	The process of assessing a system to determine whether the work products of a given development phase satisfy the conditions imposed at the start of that phase.
Vulnerability	Includes a weakness of an asset or group of assets which can be exploited by a threat [IEEE 13335-1:1996]
Work Product	Output of a process.

Appendix E: SE-CMM Project and Organization PAs

Appendix E: SE-CMM Project and Organization PAs

PA 08: Ensure Quality

Summary description

The purpose of Ensure Quality is to address not only the quality of the system, but also the quality of the process being used to create the system and the degree to which the project follows the defined process. The underlying concept of this process area is that high-quality systems can only be consistently produced on a continuous basis if a process exists to continuously measure and improve quality[10]. In addition, this process must be adhered to rigorously and throughout the system life cycle. Key aspects of the process required to develop high-quality systems are measurement, analysis, and corrective action.

Process area notes

A successful quality program requires integration of the quality efforts throughout the project team and support elements. Effective processes provide a mechanism for building in quality and reduce dependence on end-item inspections and rework cycles.

This is not meant to imply that those managing and/or assuring the quality of work products and processes are solely responsible for the quality of the work product outputs. On the contrary, the primary responsibility for "building in" quality lies with the builders. [11]A quality management process helps to ensure that all aspects of quality management are seriously considered and acted upon by the organization and reflected in its products. [12]This increases the confidence of developers, management, and customers in the system's quality.

The kinds of quality variances that may be addressed by this [13]process area include technical content, such as the particular values of derived or allocated requirements; and form issues, such as whether the customer prefers instructions on product use to be in paper or electronic form. Cost and schedule variances can also be considered defects and would be dealt with as are other defects.

Organizations may wish to determine the variances, from expected values, of technical and other issues in increments that correspond to the schedule commitments of the organization. For example, if the organization has committed to deliver or roll-out a product during a given week, then it would be wise to measure or determine its progress, by measuring variances, on a weekly basis. If the commitment is monthly, then monthly measurements would likely be appropriate.

continued on next page

Base practices list

The following list contains the base practices that are essential elements of good systems engineering:

BP.08.01	Ensure the defined system engineering process is adhered to during the system life cycle.
BP.08.02	Evaluate work product measures against the requirements for work product quality.
BP.08.03	Measure the quality of the systems engineering process used by the project.
BP.08.04	Analyze quality measurements to develop recommendations for quality improvement or corrective action as appropriate.
BP.08.05	Obtain employee participation in identifying and reporting quality issues.
BP.08.06	Initiate activities that address identified quality issues or quality improvement opportunities.
BP.08.07	Establish a mechanism or a set of mechanisms to detect the need for corrective actions to processes or products.

BP 08.01 Monitor Conformance to the Defined Process

Ensure the defined system engineering process is adhered to during the system life cycle.

Description

[14]Ensure that the project's execution follows the defined system engineering process. [15]Compliance should be checked at useful intervals. Deviations from the defined process and the impact of the deviation should be recorded.

Typical Work Products

- recorded deviations from defined systems engineering process
- recorded impact of deviations from defined systems engineering process
- quality handbook (paper on-line)

Notes

The defined process can be monitored in a number of ways. For example, a designated [16]auditor/reviewer can participate in or observe all (or a sample percentage of) process activities, or an [17]auditor/reviewer may inspect all (or a sample percentage of) in-process work products.

continued on next page

BP 08.02 Measure Quality of the Work Product

Evaluate work product measures against the requirements for work product quality.

Description

Measuring the characteristics of the work product provides an indication of the quality of the system. Measurements should be designed to assess whether the work product will meet customer and engineering requirements. Product measurements should also be designed to help isolate problems with the system development process.

Typical Work Products

- assessment of the quality of the product
- product quality certification

Notes

Example approaches to measurement of work product quality include

- statistical process control of product measurements at various points in the development process
- measurement of a complete set of work product requirements such as
  - specification value
  - planned value
  - tolerance band
  - demonstrated value
  - demonstrated technical variance
  - current estimate
  - predicted technical variance

continued on next page

BP 08.03 Measure Quality of the Process

Measure the quality of the systems engineering process used by the project.

Description

The process that is used to create a quality product is as important as the quality of the product. It is important to have a system development process that is checked by measurement so that degrading conditions are caught early, before the final work product is produced and found to not meet requirements. Thus, having a process that is measured [18]may lead to less waste and higher productivity.

Typical Work Products

- process quality certification

Notes

Examples of tools to use in measuring the process include

- process flow chart: can be used to determine which characteristics should be measured and to identify potential sources of variation, in addition to defining the process
- statistical process control on process parameters
- design of experiments

continued on next page

BP 08.04 Analyze Quality Measurements

Analyze quality measurements to develop recommendations for quality improvement or corrective action, as appropriate.

Description
Careful examination of all of the available data on product, process, and project performance can reveal causes of problems. This information will then enable improvement of the process and product quality.

Typical Work Products
- analysis of deviations
- failure analysis
- defect reports
- system quality trends
- corrective action recommendations
- cause and effect diagrams

Notes
Examples of measurements that support quality improvement include
- trend analysis, such as the identification of equipment calibration issues causing a slow creep in the product parameters
- standards evaluation, such as determining if specific standards are still applicable due to technology or process changes

continued on next page

BP 08.05 Obtain Participation

Obtain employee participation in identifying and reporting quality issues.

Description
The development of a quality work product, using a quality process that is adhered to, requires the focus and attention of all of the people involved. [19]Ideas for improving quality need to be encouraged, and a forum needs to exist that allows each employee to raise process-quality issues freely.

Typical Work Products
- environment that promotes quality
- captured inputs and resolutions from workers

Notes
A quality environment can be fostered by
- process action teams
- a quality assurance group with a reporting chain of command that is independent of the project
- an independent channel for reporting quality issues

BP 08.06 Initiate Quality Improvement Activities

Initiate activities that address identified quality issues or quality improvement opportunities.

Description
In order to continuously improve quality, specific actions must be planned and executed. Specific aspects of the system development process that jeopardize product or process quality need to be identified and corrected. This would include[20] minimizing cumbersome or bureaucratic systems.

Typical Work Products
- recommendations for improving the systems engineering process
- quality improvement plan
- process revisions

Notes
Effective implementation of quality improvement activities requires input and buy-in by the work product team.

continued on next page

BP 08.07 Detect Need for Corrective Actions

Establish a mechanism or a set of mechanisms to detect the need for corrective actions to processes or products.

Description

Such a mechanism must be available throughout the life cycle of the product (development through manufacturing through customer use). Mechanisms may include online reporting systems, workshops, periodic reviews, customer focus groups, etc. Mechanisms must be available to all affected groups, including design, manufacturing, customers, customer support, etc.

Typical Work Products

- ongoing database or repository containing identified needs, process improvements, and product improvements
- clearly described processes, methods, and avenues for getting identified needs into a database or repository
- identified needs for process improvement
- identified needs for product improvement
- trouble reports

Notes

This base practice is critical to the effective use of systems engineering in the production, operations, and maintenance life-cycle phases.

Needs for corrective action are detected in this base practice. Corrective actions are directed in the Monitor and Control Technical Effort process area (PA11).

Trouble reports also flow into this base practice from the Verify and Validate System process area (PA07).

End of PA 08: Ensure Quality

PA 09: Manage Configurations

Summary description

The purpose of Manage Configurations is to maintain data on and status of identified configuration units, and to analyze and control changes to the system and its configuration units. Managing the system configuration involves providing accurate and current configuration data and status to developers and customers.

This process area is applicable to all work products that are placed under configuration management. An example set of work products that may be placed under configuration management could include hardware and software configuration items, design rationale, requirements, product data files, or trade studies.

Process area notes

The configuration management function supports traceability by allowing the configuration to be traced back through the hierarchy of system requirements at any point in the configuration life cycle. Traceability is established as part of the practices in the Derive and Allocate Requirements process area (PA02).

When the practices of this process area are used to manage requirements, changes to those requirements need to be iterated through the Understand Customer Needs and Expectations process area (PA06) to communicate the impact of changes to the customer or their surrogate.

Base practices list

The following list contains the base practices that are essential elements of good systems engineering:

BP.09.01 Decide among candidate methods for configuration management.
BP.09.02 Identify configuration units that constitute identified baselines.
BP.09.03 Maintain a repository of work product baselines.
BP.09.04 Control changes to established configuration units.
BP.09.05 Communicate status of configuration data, proposed changes, and access information to affected groups.

continued on next page

BP 09.01 Establish Configuration Management Methodology

Decide among candidate methods for configuration management.

Description

Three primary trade-off [21]considerations will have an impact on the structure and cost of configuration management, including

- the level of detail at which the configuration units are identified
- when the configuration units are placed under configuration management
- the level of formalization required for the configuration management process

The Analyze Candidate Solutions process area (PA01) should be used as guidance to perform the trade studies.

Typical Work Products

- guidelines for identifying configuration units
- timeline for placing configuration units under configuration management
- selected configuration management process
- selected configuration management process description

Notes

Example criteria for selecting configuration units at the appropriate work product level[22] include

- [23]need to maintain interfaces at a manageable level
- unique user requirements such as field replaceable units
- new versus modified design
- expected rate of change

[24]These criteria will affect the level of visibility into the design effort.

Example criteria for determining when to place work products under configuration management include

- portion of the development life cycle that the project is in
- [25]if system element is ready for test
- degree of formalization selected
- cost and schedule limitations
- customer requirements

continued on next page

BP 09.01 Establish Configuration Management Methodology (cont.)

Example criteria for selecting a configuration management process include

- portion of the development life cycle
- impact of change in system on other work products
- impact of change in system on procured or subcontracted work products
- impact of change in system on program schedule and funding
- requirements management

BP 09.02 Identify Configuration Units

Identify configuration units that constitute identified baselines.

Description
A configuration unit is one or more work products that are baselined together. The selection of work products for configuration management should be based on criteria established in the selected configuration management strategy. Configuration units should be selected at a level that benefits the developers and customers, but that does not place an unreasonable administrative burden on the developers.

Typical Work Products
- baselined work product configuration
- identified configuration units

Notes
Configuration units in the area of requirements management could vary from individual requirements to groupings of requirements documents.

Configuration units for a system that has requirements on field replacement should have an identified configuration unit at the field-replaceable unit level.

continued on next page

BP 09.03 Maintain Work Product Baselines

Maintain a repository of work product baselines.

Description

This practice involves establishing and maintaining a repository of information about the work product configuration. Typically, this consists of capturing data or describing the configuration units. This could also include an established procedure for additions, deletions, and modifications to the baseline, as well as procedures for tracking/ monitoring, auditing, and the accounting of configuration data. Another objective of maintaining the configuration data is to provide an audit trail back to source documents at any point in the system life cycle.

Typical Work Products

- decision database
- baselined configuration
- traceability matrix

Notes

In the case of hardware configuration units, the configuration data would consist of specifications, drawings, trade study data, etc. Optimally, configuration data can be maintained in electronic format to facilitate updates and changes to supporting documentation.

Software configuration units typically include source code files, requirements and design data, and test plans and results.

continued on next page

BP 09.04 Control Changes

Control changes to established configuration units.

Description
Control is maintained over the configuration of the baselined work product. This includes tracking the configuration of each of the configuration units, approving a new configuration, if necessary, and updating the baseline.

[26]Identified problems with the work product or requests to change the work product are analyzed to determine the impact that the change will have on the work product, program schedule and cost, and other work products. If, based upon analysis, the proposed change to the work product is accepted, [27]a schedule is identified for incorporating the change into the work product and other affected areas.

Changed configuration units are released after review and formal approval of configuration changes. Changes are not official until they are released.

Typical Work Products
- new work-product baselines

Notes
Change control mechanisms can be tailored to categories of changes. For example, the approval process should be shorter for component changes that do not affect other components.

continued on next page

BP 09.05 Communicate Configuration Status

Communicate status of configuration data, proposed changes, and access information to affected groups.

Description

Inform affected groups of the status of configuration data whenever there are any status changes. The status reports should include information on when accepted changes to configuration units will be processed, and the associated work products[28] that are affected by the change. Access to configuration data and status should be provided to developers, customers, and other affected groups.

Typical Work Products

- status reports

Notes

Examples of activities for communicating configuration status include

- Provide access permissions to authorized users.
- Make baseline copies readily available to authorized users.

End of PA 09: Manage Configurations

PA 10: Manage Risk

Summary description

The purpose of Manage Risk is to identify, assess, monitor, and mitigate risks to the success of both the systems engineering activities and the overall technical effort. This process area continues throughout the life of the project. Similar to the Plan Technical Effort (PA12) and Monitor and Control Technical Effort (PA11) process areas, the scope of this process area includes both the systems engineering activities and the overall technical project effort, as the systems engineering effort on the project cannot be considered successful unless the overall technical effort is successful.

Process area notes

All system development efforts have inherent risks, some of which are not easily recognized. Especially early on, the likelihood of known risks and the existence of unknown risks should be sought out. Poor risk management is often cited as a primary reason for unsatisfied customers, and cost or schedule overruns. Early detection and reduction of risks avoid the increased costs of reducing risks at a more advanced state of system development.

It is important to note the distinction among risk types, analysis, and management approach. Good risk management operates on all three dimensions. For example, analyzing developer risk primarily deals with the management approach, i.e., profit and market building; whereas analyzing user risk primarily is concerned with types and analysis, i.e., mission and goal satisfaction.

Base practices list

The following list contains the base practices that are essential elements of good systems engineering:

- BP.10.01 Develop a plan for risk-management activities that is the basis for identifying, assessing, mitigating, and monitoring risks for the life of the project.
- BP.10.02 Identify project risks by examining project objectives with respect to the alternatives and constraints, and identifying what can go wrong.
- BP.10.03 Assess risks and determine the probability of occurrence and consequence of realization.
- BP.10.04 Obtain formal recognition of the project risk assessment.
- BP.10.05 Implement the risk-mitigation activities.
- BP.10.06 Monitor risk-mitigation activities to ensure that the desired results are being obtained.

continued on next page

BP 10.01 Develop Risk Management Approach

Develop a plan for risk-management activities that is the basis for identifying, assessing, mitigating, and monitoring risks for the life of the project.

Description

The purpose of this base practice is to develop an effective plan to guide the risk-management activities of the project. Elements of the plan should include identification of members of the risk-management team and their responsibilities; a schedule of regular risk-management activities, methods, and tools to be employed in risk identification and mitigation; and methods of tracking and controlling risk-mitigation activities. The plan should also provide for the assessment of risk-management results.

Typical Work Products

- risk-management plan

Notes

Examples of risk-management approaches include

- Use a spiral management approach where the objectives for the next cycle and the objectives for the overall project are clarified and documented periodically.
- Formally identify and review risks at the beginning of each cycle and develop mitigation approaches.
- At the end of each cycle, review progress made in reducing each risk.

continued on next page

BP 10.02
Identify Risks

Identify project risks by examining project objectives with respect to the alternatives and constraints, and identifying what can go wrong.

Description
Examine the project objectives, the project plans (including activity or event dependencies), and the system requirements in an orderly way to identify probable areas of difficulties and what can go wrong in these areas. Sources of risk based on past experience should be considered to identify potential risks. This activity is enacted during the Plan Technical Effort process area (PA12). Establishing critical development dependencies and providing tracking and corrective action is performed in the Monitor and Control Technical Effort process area (PA11).

Typical Work Products
- list of identified risks

Notes
Examples of activities to identify risks include
- Develop a common risk classification scheme or risk taxonomy to categorize risks. This taxonomy contains the history of risks for each category, including probabilities of occurrence (which system elements contribute most to risk), estimated cost of occurrence, and mitigation strategies. This practice is very useful in improving risk estimates and in reusing successful risk-mitigations [Charette 89].
- Focus mitigation resources and controls on system elements which contribute most to risk.
- Collect all the information specifying project and systems engineering objectives, alternative technical strategies, constraints, and success criteria. Ensure that the objectives for the project and the systems engineering effort are clearly defined. For each alternative approach suggested to meet the objectives, document items that may prevent attainment of the objectives: these items are risks. Following this procedure results in a list of risks per alternative approach. Note, some risks will be common across all the alternatives.
- Interview technical and management personnel to uncover assumptions and decisions leading to risk. Use historical data from similar projects to find out where problems have arisen in similar contexts.

continued on next page

BP 10.03
Assess Risks

Assess risks and determine the probability of occurrence and consequence of realization.

Description
Estimate the chance of potential loss (or gain) and the consequence [29]if the previously identified risks occur. Analyze the risks independently of one another and understand the relationships between different individual risks. The analysis methodology should take into account factors such as the probability of failure due to the maturity and complexity of the technology.

Typical Work Products
- risk assessment

Notes
Examples of activities to assess risks include
- Develop standards for estimating the probability and cost of risk occurrence. Possible standards range from a simple high-moderate-low qualitative scale to quantitative scales in dollars and probability to the nearest tenth of a percent.
- Establish a practical standard based on the project's size, duration, overall risk exposure, system domain, and customer environment [Charette 89].

continued on next page

BP 10.04 Review Risk Assessment

Obtain formal recognition of the project risk assessment.

Description
Review adequacy of the risk assessment and obtain a decision to proceed, modify, or cancel the effort based on risks. This review should include the potential risk-mitigation efforts and their probability of success.

Typical Work Products
- risk-mitigation strategy

Notes
Examples of activities to review the risk assessment include
- Hold a meeting of all stakeholders of the project internal to the company to present the risk assessment. To help communicate a sense of control over the risks, present possible mitigation strategies along with each risk.
- Obtain agreement from the attendees that the risk estimates are reasonable and that no obvious mitigation strategies are being overlooked.

continued on next page

BP 10.05 Execute Risk Mitigations

Implement the risk-mitigation activities.

Description

Risk-mitigation activities may address lowering the probability that the risk will occur or lowering the extent of the damage the risk causes when it does occur. For risks that are of particular concern, several risk-mitigation activities may be initiated at the same time.

Typical Work Products

- risk-mitigation plan

Notes

Examples of activities to mitigate risks include the following:

- To address the risk that the delivered system will not meet a specific performance requirement, build a prototype of the system or a model that can be tested against this requirement. This type of mitigation strategy lowers the probability of risk occurrence.
- To address the risk that the delivery schedule will slip due to a subsystem not being available for integration, develop alternative integration plans with different integration times for the risky subsystem. If the risk occurs (i.e., the subsystem is not ready on time), the impact of the risk on the overall schedule will be less. This type of mitigation strategy lowers the consequence of risk occurrence.
- Use predetermined baselines (risk referents) to trigger risk-mitigation actions [Charette 89].

continued on next page

BP 10.06 Track Risk Mitigations

Monitor risk-mitigation activities to ensure that the desired results are being obtained.

Description
On a regular basis, examine the results of the risk mitigations that have been put into effect, to measure the results, and determine whether the mitigations have been successful.

Typical Work Products
- risk status
- risk taxonomy

Notes
For a project with a development schedule of about six months, re-assess risks every two weeks. Re-estimate the probability and consequence of each risk occurrence.

End of PA 10: Manage Risk

PA 11: Monitor and Control Technical Effort

Summary description

The purpose of Monitor and Control Technical Effort is to provide adequate visibility of actual progress and risks. Visibility encourages timely corrective action when performance deviates significantly from plans.

Monitor and Control Technical Effort involves directing, tracking and reviewing the project's accomplishments, results, and risks against its documented estimates, commitments, and plans. A documented plan is used as the basis for tracking the activities and risks, communicating status, and revising plans.

Process area notes

Similar to the Plan Technical Effort process area (PA12), this process area applies to the project's technical activities as well as to the systems engineering effort.

Progress is primarily determined by comparing the actual effort, work product sizes, cost, and schedule to the plan when selected work products are completed and at selected milestones. When it is determined that the plans are not being met, corrective actions are taken. These actions may include revising the plans to reflect the actual accomplishments and replanning the remaining work, or taking actions to improve performance or reduce risks.

Base practices list

The following list contains the base practices that are essential elements of good systems engineering:

BP.11.01 Direct technical effort in accordance with technical management plans.
BP.11.02 Track actual use of resources against technical management plans.
BP.11.03 Track performance against the established technical parameters.
BP.11.04 Review performance against the technical management plans.
BP.11.05 Analyze issues resulting from [30]the tracking and review of technical parameters to determine corrective actions.
BP.11.06 Take corrective actions [31]when actual results deviate from plans.

continued on next page

BP 11.01 Direct Technical Effort

Direct technical effort in accordance with technical management plans.

Description
Carry out the technical management plans created in the Plan Technical Effort process area. This practice involves technical direction of all of the engineering activities of the project.

Typical Work Products
- matrix matrix of responsibilities
- matrix work authorizations

Notes
Effective technical direction includes the use of appropriate communication mechanisms and timely distribution of technical information to all affected parties. All technical direction must be captured to preserve the basis for decisions and actions.

BP 11.02 Track Project Resources

Track actual use of resources against technical management plans.

Description
[32]Provide current information on the use of resources during the project to help adjust the effort and plans when needed.

Typical Work Products
- [33]resource usage

Notes
Tracking cost includes comparing the [34]actual costs to the estimates documented in the project plan to identify potential overruns and underruns.

continued on next page

BP 11.03 Track Technical Parameters	**Track performance against the established technical parameters.** *Description* The actual performance of the project and its products is tracked by measuring the technical parameters established in the technical management plan. These measurements are compared to the thresholds established in the technical management plan so that warnings of problems can to ensure objective measurements. Periodically perform the benchmarking activity and compare the actual measurement with the planned values of the parameters.

continued on next page

BP 11.04 Review Project Performance

Review performance against the technical management plans.

Description

The performance of the project and its products is reviewed periodically and when technical parameter thresholds are exceeded. The results of analyzing the measurements of technical performance are reviewed, along with other indicators of technical performance, and corrective action plans are approved.

Typical Work Products

- change requests for the technical management plan
- approved corrective actions

Notes

Examples of reviewing performance include

- Holding a meeting of all stakeholders of the project internal to the organization to present analyses of performance and suggested corrective actions.
- Writing a status report which forms the basis of a project review meeting.

continued on next page

BP 11.05 Analyze Project Issues

Analyze issues resulting from [35]**the tracking and review of technical parameters to determine corrective actions.**

Description
New project issues surface frequently and continuously through the project life cycle. Timely identification, analysis, and tracking of issues is crucial to controlling project performance.

Typical Work Products
- analysis of project performance issues
- approved corrective actions

Notes
[36]New information is integrated with historical project data.
[37]Trends that are hurting the project are identified, along with new issues that indicate risks to the project's success. Obtain more detailed data, as needed, for issues and trends that are inconclusive. Analysis frequently requires modeling and simulation tools as well as outside expert opinions.

continued on next page

BP 11.06 Take Corrective Action

Take corrective actions when technical parameters indicate future problems or when actual results deviate from plans.

Description
When corrective actions are approved, take the corrective actions by reallocating resources, changing methods and procedures, or increasing adherence to the existing plans. When changes to the technical management plan are necessary, employ the practices of the Plan Technical Effort process area (PA12) to revise the plan.

Typical Work Products
- resource reallocations
- changes to methods and procedures
- change orders

Notes
This base practice covers whatever actions are needed to prevent anticipated problems or to correct the problems discovered. The possible actions taken under this base practice are varied and numerous.

End of PA 11: Monitor and Control Technical Effort

PA 12: Plan Technical Effort

Summary description

The purpose of Plan Technical Effort is to establish plans that provide the basis for scheduling, costing, controlling, tracking, and negotiating the nature and scope of the technical work involved in system development, manufacturing, use, and disposal. System engineering activities must be integrated into comprehensive technical planning for the entire project.

Plan technical effort involves developing estimates for the work to be performed, obtaining necessary commitments from interfacing groups, and defining the plan to perform the work.

Process area notes

Planning begins with an understanding of the scope of the work to be performed, along with the constraints, risks, and goals that define and bound the project. The planning process includes steps to estimate the size of work products, estimate the resources needed, produce a schedule, consider risks, and negotiate commitments. Iterating through these steps may be necessary to establish a plan that balances quality, cost, and schedule goals.

Base practices list

The following list contains the base practices that are essential elements of good systems engineering:

BP.12.01 Identify resources that are critical to the technical success of the project.

BP.12.02 Develop estimates for the factors that affect the magnitude and technical feasibility of the project.

BP.12.03 Develop cost estimates for all technical resources required by the project.

BP.12.04 Determine the technical process to be used on the project.

BP.12.05 Identify technical activities for the entire life cycle of the project.

BP.12.06 Define specific processes to support effective interaction with the customer(s) and supplier(s).

BP.12.07 Develop technical schedules for the entire project life cycle.

BP.12.08 Establish technical parameters with thresholds for the project and the system.

BP.12.09 Use the information gathered in planning activities to develop technical management plans that will serve as the basis for tracking the salient aspects of the project and the systems engineering effort.

BP.12.10 Review the technical management plans with all affected groups and individuals, and obtain group commitment.

continued on next page

BP 12.01 Identify Critical Resources

Identify resources that are critical to the technical success of the project.

Description
Critical resources are resources that are essential to the success of the project and that may not be available for the project. Critical resources may include personnel with special skills, tools, facilities, or data. Critical resources can be identified by analyzing project tasks and schedules, and by comparing this project with similar projects.

Typical Work Products
- identified critical resources

Notes
Example practice: Examine the project schedule and think of the types of resources required at each point in time. List resources that are not easily obtainable. Cross check and augment this list by thinking of engineering skills that are required to synthesize the system and work products.

continued on next page

BP 12.02 Estimate Project Scope

Develop estimates for the factors that affect the magnitude and technical feasibility of the project.

Description
The project's scope and size can be estimated by decomposing the system into component elements that are similar to those of other projects. The size estimate can then be adjusted for factors such as differences in complexity or other parameters.

Historical sources often provide the best available information to use for initial size estimates. These estimates will be refined as more information on the current system becomes available.

Typical Work Products
- estimates of the scope of the system
  - number of source lines of code
  - number of cards of electronics
  - number of large forgings
  - number of cubic yards of material to be moved

Notes
Example practice: Analyze the available project documentation, and interview project personnel to determine the main technical constraints and assumptions. Identify the possible highest level technical approaches and the factors that may keep the project or the systems engineering effort from being successful. Identify the major technical parameters and estimate the acceptable range for each parameter.

continued on next page

BP 12.03 Estimate Project Costs

Develop cost estimates for all technical resources required by the project.

Description
A detailed estimate of project costs is essential to good project management, whether or not it is required by a customer. Estimates of project costs are made by determining the labor costs, material costs, and subcontractor costs based on the schedule and the identified scope of the effort. Both direct costs and indirect costs (such as the cost of tools, training, special test and support items) are included. For labor costs, historical parameters or cost models are employed to convert hours to dollars based on job complexity, tools, available skills and experience, schedules, and direct and overhead rates. Appropriate reserves are established, based on identified risks.

Typical Work Products
- total labor cost by skill level and schedule
- cost of material by item, vendor, and schedule
- cost of subcontracts by vendor and schedule
- cost of tools
- cost of training
- supporting rationale

Notes
A considerable amount of project data such as scope, schedule, and material items must be collected prior to estimating costs. Checklists and historical data from other projects can be used to identify cost items which may otherwise be overlooked. Variance reports and "lessons-learned" documents are typically good sources of this type of information.

continued on next page

BP 12.04 Determine Project's Process

Determine the technical process to be used on the project.

Description

At the highest level, the technical process should follow a life-cycle model based on the characteristics of the project, the characteristics of the organization, and the organization's standard process. Typical life-cycle models include waterfall, evolutionary spiral, and incremental. In the process definition, include process activities, inputs, outputs, sequences, and quality measures for process and work products.

Typical Work Products

- selected systems engineering process for the project

Notes

Establish and maintain an integrated management plan that defines the project's interaction with all internal and external organizations (e.g., the subcontractor) performing the technical effort. Include the planned project life-cycle model for the project and specific project activities.

continued on next page

BP 12.05 Identify Technical Activities

Identify technical activities for the entire life cycle of the project.

Description
Project and systems engineering activities may be selected from applicable standards, known best practice within the industry segment, reference models such as the SE-CMM, or the organization's historical experience.

Typical Work Products
• identified technical activities

Notes
Use historical records from similar projects, where possible, to develop the list of activities and to gain confidence that the list is complete. Use the "rolling wave" paradigm for planning. The "rolling wave" paradigm is used to define near-term activities more precisely than activities that start later in the project.

For example, the systems engineering activities would be decomposed into activities planned for the next three months until each activity is approximately two weeks in duration. Activities 3 to 12 months away should be planned at approximately a month in duration. Activities starting more than a year away can be described at a very high level, approximately two months in duration. For the nonsystems-engineering technical activities, use this same method while working with other disciplines according to the Integrate Disciplines process area (PA04).

continued on next page

BP 12.06 Define Project Interface

Define specific processes to support effective interaction with customer(s) and supplier(s).

Description
Project interfaces include all those with organizations and individuals who are necessary to successful project execution, whether they are inside or outside the project group. Types of interaction include information exchange, tasking, and deliveries. Methods and processes (including controls) for interaction are established as appropriate for the parties that are interacting.

Typical Work Products
- defined processes for project interfaces

Notes
For the project, identify the groups internal and external to your organization that the project needs to interact with in order to be successful. For each group, perform the base practices of the Integrate Disciplines process area (PA04) to define and implement each interface in terms of interaction mechanisms, interaction frequency, and problem resolution mechanisms.

continued on next page

BP 12.07 Develop Project Schedules

Develop technical schedules for the entire project life cycle.

Description
Project schedules include system and component development, obtaining procured items, training, and preparing the engineering support environment. Schedules are based on verifiable effort models or data for identified tasks, and they must allow for task interdependencies and the availability of procured items. Schedules should also include slack time appropriate for identified risks. All affected parties must review and commit to the schedule.

Typical Work Products
- project schedules

Notes
Schedules typically include both customer and technical milestones.

Example: Within project constraints (contractual, market timing, customer-provided inputs, etc.), define system increments consistent with the overall technical approach. Each increment should provide more system capability from the user's point of view. Estimate the additional staff hours required to develop each increment.

To create a schedule that uses resources at a level rate, select dates for completion of each increment proportional to the amount of work required to develop the increment. Derive detailed schedules for technical activities within each increment by sequencing the activities from the start of the increment and taking into account dependencies between activities.

For an event-driven schedule, the loading is typically not level. For noncritical-path activities, it may be necessary to adjust the activity duration, activity sequencing, or activity start dates to avoid unacceptable resource peaking.

continued on next page

BP 12.08 Establish Technical Parameters

Establish technical parameters with thresholds for the project and the system.

Description
Establish key technical parameters that can be traced over the life of the project and that will serve as in-progress indicators for meeting the ultimate technical objectives. Key technical parameters can be identified through interaction with the customer, customer requirements, market research, prototypes, identified risks, or historical experience on similar projects. Each technical parameter to be tracked should have a threshold or tolerance beyond which some corrective action would be expected. Key technical parameters should have pre-planned assessments scheduled at useful points in the project schedule.

Typical Work Products
- technical parameters
- technical parameter thresholds

Examples of technical parameters include
- payload capacity of cargo aircraft
- sensor resolution
- portable stereo weight
- automobile gas mileage
- video monitor distortion

Notes
Example: Identify aspects of the system that are primary drivers of system performance. Develop a metric for each aspect that can be tracked over time while the system is being developed.

continued on next page

BP 12.09 Develop Technical Management Plan

Use the information gathered in planning activities to develop technical management plans that will serve as the basis for tracking the salient aspects of the project and the systems engineering effort.

Description
Establish and maintain an integrated management plan that defines project interaction with all internal and external organizations (e.g., the subcontractor) performing the technical effort.

Typical Work Products
- technical management plan

Notes
Technical management plans typically include
- plans for developing the system
- plans for interacting with other organizations (e.g., subcontractors) performing the technical effort

continued on next page

BP 12.10 Review and Approve Project Plans

Review the technical management plans with all affected groups and individuals, and obtain group commitment.

Description

The objective of project plan reviews is to ensure a bottom-up, common understanding of the process, resources, schedule, and information requirements by affected groups and individuals throughout the project. Inputs on the project plan are solicited from all responsible organizational elements and project staff. [38]Whenever possible, these inputs are incorporated to build team ownership of the plans. [39]If an input is rejected or modified, feedback is provided to the individual who gave the input. Interim and completed project plans are distributed for review. A commitment to the project plans should be obtained from all groups comprising the project team.

Typical Work Products

- interface issues between disciplines/groups
- risks
- project plan inputs
- project plan comments
- project plan issues and resolutions

Notes

Affected groups and individuals typically include

- software engineering
- hardware engineering
- manufacturing
- management
- customers
- users
- partners
- subcontractors

Example activity: Identify questions that each group should answer as part of their review. (The questions may be different for different groups.) Communicate to the groups how the review will be conducted. Provide the technical management plans to the groups and, at the pre-arranged time, meet with them to discuss their comments. Produce a list of issues from the reviewers' comments and work on each issue until it is resolved.

End of PA 12: Plan Technical Effort

PA 13: Define Organization's Systems Engineering Process

Summary description

The purpose of Define Organization's Systems Engineering Process is to create and manage the organization's standard systems engineering processes, which can subsequently be tailored by a project to form the unique processes that it will follow in developing its systems or products.

Define Organization's Systems Engineering Process involves defining, collecting, and maintaining the process that will meet the business goals of the organization, as well as designing, developing, and documenting [40]systems-engineering process assets. [41]Assets include example processes, process fragments, process-related documentation, process architectures, process-tailoring rules and tools, and process measurements.

Process area notes

This process area covers the initial activities required to collect and maintain process assets, including the organization's standard systems engineering process. The improvement of the process assets and the organization's standard systems engineering process are covered in the process area Improve Organization's Systems Engineering Processes (PA14).

Base practices list

The following list contains the base practices that are essential elements of good systems engineering:

BP.13.01 Establish goals for the organization's systems engineering process from the organization's business goals.

BP.13.02 Collect and maintain systems-engineering process assets.

BP.13.03 Develop a well-defined standard systems engineering process for the organization.

BP.13.04 Define guidelines for tailoring the organization's standard systems engineering process for project use in developing the project's defined process.

continued on next page

BP 13.01 Establish Process Goals

Establish goals for the organization's systems engineering process from the organization's business goals.

Description
The systems engineering process operates in a business context, and this must be explicitly recognized in order to institutionalize the organization's standard practice. The process goals should consider the financial, quality, human resource, and marketing issues important to the success of the business.

Typical Work Products
- goals of the organization's systems engineering process
- requirements for the organization's standard systems engineering process
- requirements for the organization's process asset library
- process asset library

Notes
Establishing goals may include determining the tradeoff criteria for process performance based on time-to-market, quality, and productivity business issues.

continued on next page

BP 13.02 Collect Process Assets

Collect and maintain systems-engineering process assets.

Description

The information generated by the process definition activity, both at the organization and project levels, needs to be stored (e.g., in a process asset library), made accessible to those who are involved in tailoring and process design efforts, and maintained so as to remain current.

Typical Work Products

- instructions for use of a process asset library
- design specifications for a process asset library
- process assets

Notes

The purpose of a process asset library is to store and make available process assets that projects will find useful in defining the process for developing the system. It should contain examples of processes that have been defined, and the measurements of the process. When the organization's standard systems engineering process has been defined, it should be added to the process asset library, along with guidelines for projects to tailor the organization's standard systems engineering process when defining the project's process.

Process assets typically include

- the organization's standard systems engineering process
- the approved or recommended development life cycles
- project processes together with measurements collected during the execution of the processes
- guidelines and criteria for tailoring the organization's standard systems engineering process
- process-related reference documentation
- measurements of the project's process

continued on next page

BP 13.03 Develop Organization's Systems Engineering Process

Develop a well-defined standard systems engineering process for the organization.

Description

The organization's standard systems engineering process is developed using the facilities of the process asset library. New process assets may be necessary during the development task and should be added to the process asset library. The organization's standard systems engineering process should be placed in the process asset library.

Typical Work Products

- organization's standard systems engineering process
- inputs to training
- inputs to systems engineering process improvement

Notes

The standard systems engineering process should include the interfaces to the organization's other defined processes. In addition, references used to define the systems engineering process (e.g., military standards, IEEE standards) should be cited and maintained.

To develop the standard systems engineering process, an organization can identify all the process elements or activities of the organization's system engineering process. The organization must evaluate the process elements for consistency of inputs and outputs, redundant activities, and missing activities. Inconsistencies must be resolved between process elements and provision made for appropriate sequencing and verification features. The resulting process should be well defined.

A well-defined process includes

- readiness criteria
- inputs
- standards and procedures
- verification mechanisms
  - peer reviews
  - outputs
  - completion criteria [SPICE]

continued on next page

BP 13.04 Define Tailoring Guidelines

Define guidelines for tailoring the organization's standard systems engineering process for project use in developing the project's defined process.

Description
Since the organization's standard systems engineering process may not be suitable for every project's situation, guidelines for tailoring it are needed. The guidelines should be designed to fit a variety of situations, while not allowing [42]projects to bypass standards that must be followed or substantial and important practices prescribed by organization policy.

Typical Work Products
- tailoring guidelines for the organization's standard systems engineering process

Notes
Guidelines should enable the organization's standard systems engineering process to be tailored to address contextual variables such as the domain of the project; the cost, schedule, and quality tradeoffs; the experience of the project's staff; the nature of the customer; the technical difficulty of the project, etc.

End of PA 13: Define Organization's Systems Engineering Process

PA 14: Improve Organization's Systems Engineering Processes

Summary description

The purpose of Improve Organization's Systems Engineering Processes is to gain competitive advantage by continuously improving the effectiveness and efficiency of the systems engineering processes used by the organization. It involves developing an understanding of the organization's processes in the context of the organization's business goals, analyzing the performance of the processes, and explicitly planning and deploying improvements to those processes.

Process area notes

This process area covers the continuing activities to measure and improve the performance of systems engineering processes in the organization. The initial collection of the organization's process assets and the definition of the organization's standard system engineering process is covered in the process area Define Organization's Systems Engineering Process (PA13).

Guidance on improving the standard process may be obtained from several sources, including lessons learned, application of the generic practices, and appraisals of the standard process against the SE-CMM. The resulting profile of capability levels against process areas will point to the most needed areas for improvement. Incorporating the generic practices in these process areas will be useful.

Base practices list

The following list contains the base practices that are essential elements of good systems engineering:

- BP.14.01 Appraise the existing processes being performed in the organization to understand their strengths and weaknesses.
- BP.14.02 Plan improvements to the organization's processes based on analyzing the impact of potential improvements on achieving the goals of the processes.
- BP.14.03 Change the organization's standard systems engineering process to reflect targeted improvements.
- BP.14.04 Communicate process improvements to existing projects and to other affected groups, as appropriate.

continued on next page

BP 14.01 Appraise the Process

Appraise the existing processes being performed in the organization to understand their strengths and weaknesses.

Description
Understanding the strengths and weaknesses of the processes currently being performed in the organization is a key to establishing a baseline for improvement activities. Measurements of process performance and lessons learned should be considered in the appraisal. Appraisal can occur in many forms, and appraisal methods should be selected to match the culture and needs of the organization.

Typical Work Products
- process maturity profiles
- process performance analyses
- appraisal findings
- gap analyses

Notes
An example appraisal scenario: Appraise the organization's current systems engineering processes using the SE-CMM and its associated appraisal method. Use the results of the appraisal to establish or update process performance goals.

If delays and queues occur in the execution of the existing systems engineering process, then an organization may focus on them as starting points for cycle-time reduction. Recheck such process features as readiness criteria, inputs, and verification mechanisms.

continued on next page

BP 14.02
Plan Process Improve-ments

Plan improvements to the organization's processes based on analyzing the impact of potential improvements on achieving the goals of the processes.

Description
Appraising the process provides momentum for change. This momentum must be harnessed by planning improvements that will provide the most payback for the organization in relation to its business goals. The improvement plans provide a framework for taking advantage of the momentum gained in appraisal. The planning should include targets for improvement that will lead to high-payoff improvements in the process.

Organizations may take this opportunity to "mistake-proof" the process and eliminate wasted effort. It is important to make the process *stable*–that is, performed consistently by everyone. Deployment is commonly a challenge. In making improvements, be careful to avoid optimizing locally, and thereby creating problems in other areas.

Typical Work Products
- process improvement plan

Notes
Perform tradeoffs on proposed process improvements against estimated returns in cycle time, productivity, and quality. Use the techniques of the Analyze Candidate Solutions process area (PA01).

continued on next page

BP 14.03 Change the Standard Process

Change the organization's standard systems engineering process to reflect targeted improvements.

Description

Improvements to the organization's standard systems engineering process, along with necessary changes to the tailoring guidelines in the process asset library, will preserve the improved process and encourage projects to incorporate the improvements for new products.

Typical Work Products

- organization's standard systems engineering process
- tailoring guidelines for the organization's standard systems engineering process

Notes

As improvements to the standard systems engineering process are implemented and evaluated, the organization should adopt the successful improvements as permanent changes to the standard systems engineering process.

continued on next page

BP 14.04 Communicate Process Improvements

Communicate process improvements to existing projects and to other affected groups, as appropriate.

Description

Some process improvements may be useful to existing projects, and they can incorporate the useful improvements into their current project's process depending upon the status of the project. Others who are responsible for training, quality assurance, measurement, etc., should be informed of the process improvements.

Typical Work Products

- instructions for use of the process asset library
- tailoring guidelines for the organization's standard systems engineering process
- enumeration and rationale for changes made to the systems engineering process
- schedule for incorporating the process changes

Notes

Process improvements, as well as the rationale and expected benefits of the changes, should be communicated to all affected projects and groups. The organization should develop a deployment plan for the updated processes and monitor conformance to that deployment plan.

End of PA 14: Improve Organization's Systems Engineering Processes

PA 15: Manage Product Line Evolution

Summary description

The purpose of Manage Product Line Evolution is to introduce services, equipment, and new technology to achieve the optimal benefits in product evolution, cost, schedule, and performance over time as the product line evolves toward its ultimate objectives.

An organization must first determine the evolution of a product. Then the organization has to decide how it will design and build those products including critical components, cost-effective tools, and efficient and effective processes.

Process area notes

The Manage Product Line Evolution process area is needed ". . . to ensure that product development efforts converge to achieve strategic business purposes, and to create and improve the capabilities needed to make research and product development a competitive advantage over the long term." from p. 34 of [Wheelwright 92].

This process area covers the practices associated with managing a product line, but not the engineering of the products themselves.

Base practices list

The following list contains the base practices that are essential elements of good systems engineering:

BP.15.01 Define the types of products to be offered.

BP.15.02 Identify new product technologies or enabling infrastructure that will help the organization acquire, develop, and apply technology for competitive advantage.

BP.15.03 Make the necessary changes in the product development cycle to support the development of new products.

BP.15.04 Ensure critical components are available to support planned product evolution.

BP.15.05 Insert new technology into product development, marketing, and manufacturing.

continued on next page

BP 15.01 Define Product Evolution

Define the types of products to be offered.

Description
Define the product lines that support the organization's strategic vision. Consider the organization's strengths and weaknesses, the competition, potential market size, and available technologies.

Typical Work Products
- product line definition

Notes
Defined product lines enable a more effective reuse approach and allow investments with high potential payoff.

BP 15.02 Identify New Product Technologies

Identify new product technologies or enabling infrastructure that will help the organization acquire, develop, and apply technology for competitive advantage.

Description
Identify new product technologies for potential introduction into the product line. Establish and maintain sources and methods for identifying new technology and infrastructure improvements, such as facilities or maintenance services.

Typical Work Products
- reviews of product-line technology
- improvements recommended by process teams

Notes
This practice involves identifying, selecting, evaluating, and pilot testing new technologies. By maintaining an awareness of technology innovations and systematically evaluating and experimenting with them, the organization selects appropriate technologies to improve the quality of its product lines and the productivity of its engineering and manufacturing activities. Pilot efforts are performed to assess new and unproven technologies before they are incorporated into the product line. Infrastructure improvements such as facilities upgrades or enhancements to the service of the distribution chain may also provide opportunities for evolving a product line toward its future objectives.

continued on next page

BP 15.03 Adapt Development Processes

Make the necessary changes in the product development cycle to support the development of new products.

Description
Adapt the organization's product development processes to take advantage of components intended for future use.

Typical Work Products
• adapted development processes

Notes
This practice can include establishing a library of reusable components, which includes the mechanisms for identifying and retrieving components.

BP 15.04 Ensure Critical Component Availability

Ensure critical components are available to support planned product evolution.

Description
The organization must determine [43]the critical components of the product line and plan for their availability.

Typical Work Products
• product-line components

Notes
The availability of critical components can be ensured by incorporating considerations for the future use of these components into the product line requirements. Appropriate resources must be allocated by the organization to maintain the components on a continuous basis.

continued on next page

BP 15.05 Insert Product Technology

Insert new technology into product development, marketing, and manufacturing.

Description
Manage the introduction of new technology into the product lines, including both modifications of existing product-line components and the introduction of new components. Identify and manage risks associated with product design changes.

Typical Work Products
- new product-line definition

Notes
The objective of this practice is to improve product quality, increase productivity, decrease life-cycle cost, and decrease the cycle time for product development.

End of PA 15: Manage Product Line Evolution

PA 16: Manage Systems Engineering Support Environment

Summary description

The purpose of Manage Systems Engineering Support Environment is to provide the technology environment needed to develop the product and perform the process. Development and process technology is inserted into the environment with a goal of minimizing disruption of development activities while upgrading to make new technology available.

The technology needs of an organization change over time, and the efforts described in this process area must be re-executed as the needs evolve.

Process area notes

This process area addresses issues pertaining to the systems engineering support environment at both a project level and at an organizational level. The elements of a support environment consist of all the surroundings of the systems engineering activities, including

- computing resources
- communications channels
- analysis methods
- the organization's structures, policies and procedures
- machine shops
- chemical process facilities
- environment stress facilities
- systems engineering simulation tools
- software productivity tools
- proprietary systems engineering tools
- work space

continued on next page

PA 16: Manage Systems Engineering Support Environment, Continued

Base practices list

The following list contains the base practices that are essential elements of good systems engineering:

BP.16.01 Maintain awareness of the technologies that support the organization's goals.

BP.16.02 Determine requirements for the organization's systems engineering support environment based on organizational needs.

BP.16.03 Obtain a systems engineering support environment that meets the requirements established in Determine Support Requirements by using the practices in the Analyze Candidate Solutions process area.

BP.16.04 Tailor the systems engineering support environment to individual project's needs.

BP.16.05 Insert new technologies into the systems engineering support environment based on the organization's business goals and the projects' needs.

BP.16.06 Maintain the systems engineering support environment to continuously support the projects dependent on it.

BP.16.07 Monitor the systems engineering support environment for improvement opportunities.

continued on next page

BP 16.01 Maintain Technical Awareness

Maintain awareness of the technologies that support the organization's goals.

Description
Awareness of the current state of the art or state of the practice is a necessary element for assessing improvement options. Therefore, to insert new technology, a sufficient awareness of new technology must be present in the organization. Such awareness may be maintained internally or acquired.

Typical Work Products
- reviews of support environment technology

Notes
Maintaining awareness may be accomplished by reading industry journals, participating in professional societies, and establishing and maintaining a technical library.

BP 16.02 Determine Support Requirements

Determine requirements for the organization's systems engineering support environment based on organizational needs.

Description
An organization's needs are primarily determined by assessing competitiveness issues. For example, does the organization's support environment hinder the organization's competitive position? Does each major element of the organization's support environment allow systems engineering to operate with sufficient speed and accuracy?

Typical Work Products
- requirements for systems engineering support environment

Notes
Determine the organization's needs for computer network performance, improved analysis methods, computer software, and process restructuring.

continued on next page

BP 16.03 Obtain Systems Engineering Support Environment

Obtain a systems engineering support environment that meets the requirements established in Determine Support Requirements by using the practices in the Analyze Candidate Solutions process area.

Description
Determine the evaluation criteria and potential candidate solutions for the needed systems engineering support environment. Then, select a solution using the practices in the Analyze Candidate Solutions process area (PA01). Finally, obtain and implement the chosen systems engineering support environment.

Typical Work Products
- systems engineering support environment

Notes
The systems engineering support environment may include many of the following: software productivity tools, tools for simulating systems engineering, proprietary in-house tools, customized commercially available tools, special test equipment, and new facilities.

continued on next page

BP 16.04 Tailor Systems Engineering Support Environment

Tailor the systems engineering support environment to individual project's needs.

Description

The total support environment represents the needs of the organization as a whole. An individual project, however, may have unique needs for selected elements of this environment. In this case, tailoring the elements of the systems engineering support environment elements can allow the project to operate more efficiently.

Typical Work Products

- tailored systems engineering support environment

Notes

Tailoring allows an individual project to customize its systems engineering support environment. For example, project A does not involve signal processing, so signal processing automation tools are tailored out of (i.e., not provided to) this project's automation tool set. Conversely, project B is the only project in the organization that has a need for automated requirements tracing, so the appropriate tools are tailored into (i.e., provided in addition to) this project's automated tool set.

continued on next page

BP 16.05 Insert New Technology

Insert new technologies into the systems engineering support environment based on the organization's business goals and the projects' needs.

Description
The organization's systems engineering support environment must be updated with new technologies as they emerge and are found to support the organization's business goals and the projects' needs.

Training in the use of the new technology in the systems engineering support environment must be provided.

Typical Work Products
- new systems engineering support environment

Notes
Inserting new technologies into the organization's support environment presents several difficulties. To minimize these difficulties, follow the steps below:
1. Test the new technology thoroughly.
2. Decide whether to insert the improvement across the entire organization or in selected portions of the organization.
3. Provide early notification of the impending change to those who will be affected.
4. Provide any necessary "how to use" training for the new technology.
5. Monitor the acceptance of the new technology.

continued on next page

BP 16.06 Maintain Environment

Maintain the systems engineering support environment to continuously support the projects dependent on it.

Description
Maintain the systems engineering support environment at a level of performance consistent with its expected performance. Maintenance activities could include computer system administration, training, hotline support, availability of experts, evolving/expanding a technical library, etc.

Typical Work Products
- performance report for the systems engineering support environment

Notes
Maintenance of the systems engineering support environment could be accomplished several ways, including
- hire or train computer system administrators
- develop expert users for selected automation tools
- develop methodology experts who can be used on a variety of projects
- develop process experts who can be used on a variety of projects

continued on next page

BP 16.07 Monitor Systems Engineering Support Environment

Monitor the systems engineering support environment for improvement opportunities.

Description

Determine the factors that influence the usefulness of the systems engineering support environment, including any newly inserted technology. Monitor the acceptance of the new technology and of the entire systems engineering support environment.

Typical Work Products

- reviews of the technology used in the systems engineering support environment

Notes

Design some monitoring to be an automated, background activity, so that users of the support environment do not need to provide data consciously. Also provide a way for users of the systems engineering support environment to consciously provide inputs on the usefulness of the current systems engineering support environment and to suggest improvements.

End of PA 16: Manage Systems Engineering Support Environment

PA 17: Provide Ongoing Skills and Knowledge

Summary description

[44]The purpose of Provide Ongoing Skills and Knowledge is to ensure that projects and the organization have the necessary knowledge and skills to achieve project and organizational objectives. To ensure the effective application of these critical resources that are predominantly available only from people, the knowledge and skill requirements within the organization need to be identified, as well as the specific project's or organization's needs (such as those relating to emergent programs or technology, and new products, processes, and policies).

[45]Needed skills and knowledge can be provided both by training within the organization and by timely acquisition from sources external to the organization. Acquisition from external sources may include customer resources, temporary hires, new hires, consultants, and subcontractors. In addition, knowledge may be acquired from subject matter experts.

Process area notes

[46]The choice of training or external sourcing for the need skill and knowledge is often determined by the availability of training expertise, the project's schedule, and business goals. Successful training programs result from an organization's commitment. [47] In addition, they are administered in a manner that optimizes the learning process, and that is repeatable, assessable, and easily changeable to meet new needs of the organization. Training is not limited to "classroom" events: it includes the many vehicles that support the enhancement of skills and the building of knowledge. When training is not a viable approach due to schedule or availability of training resources, external sources of the needed skills and knowledge are pursued.

continued on next page

PA 17: Provide Ongoing Skills and Knowledge, Continued

Base practices list

The following list contains the base practices that are essential elements of good systems engineering:

[48]BP.17.01 Identify needed improvements in skill and knowledge throughout the organization using the projects' needs, organizational strategic plan, and existing employee skills as guidance.

BP.17.02 Evaluate and select the appropriate mode of acquiring knowledge or skills with respect to training or other sources.

BP.17.03 Ensure that appropriate skill and knowledge are available to the systems engineering effort.

BP.17.04 Prepare training materials based upon the identified training needs.

BP.17.05 Train personnel to have the skills and knowledge needed to perform their assigned roles.

BP.17.06 Assess the effectiveness of the training to meet the identified training needs.

BP.17.07 Maintain records of training and experience.

BP.17.08 Maintain training materials in an accessible repository.

continued on next page

BP 17.01 Identify Training Needs

Identify needed improvements in skill and knowledge throughout the organization using the projects' needs, organizational strategic plan, and existing employee skills as guidance.

Description
This base practice determines the improvements that are needed in skill and knowledge within the organization. The needs are determined using inputs from existing programs, the organizational strategic plan, and a compilation of existing employee skills. Project inputs help to identify existing deficiencies which may be remedied through training or acquisition of skills and knowledge by other means. The organizational strategic plan is used to help identify emerging technologies, and the existing skill level is used to assess current capability.

Identification of skill and knowledge needs should also determine training that can be consolidated to achieve efficiencies of scale, and increase communication via the use of common tools within the organization. Training should be offered in the organization's systems engineering process and in tailoring the process for specific projects.

Typical Work Products
- organization's training needs
- project skill or knowledge

Notes
The organization should identify additional training needs as determined from appraisal findings and as identified by the defect prevention process. The organization's training plan should be developed and revised according to a documented procedure. Each project should develop and maintain a training plan that specifies its training needs.

continued on next page

[49]**BP 17.02 Select Mode of Knowledge or Skill Acquisition**

Evaluate and select the appropriate mode of acquiring knowledge or skills with respect to training or other sources.

Description

The purpose of this practice is to ensure that the most effective method is chosen to make needed skill and knowledge available to projects in a timely manner. Project and organizational needs are analyzed, and the methods of the Analyze Candidate Solutions process area (PA01) are employed to choose among alternatives such as consultants, subcontracts, knowledge acquisition from identified subject matter experts, or training.

Typical Work Products

- survey of needed skills or knowledge
- trade-study results indicating the most effective mode of skill or knowledge acquisition

Notes

Example criteria which may be used to determine the most effective mode of acquiring knowledge or skill acquisition include

- time available to prepare for project execution
- business objectives
- availability of in-house expertise
- availability of training

continued on next page

[50]**BP 17.03 Assure Availability of Skill and Knowledge**

Ensure that appropriate skill and knowledge are available to the systems engineering effort.

Description

This practice addresses acquisition of the full range of skill and knowledge which must be made available to the project systems engineering effort. Through deliberate assessment and preparation, plans can be developed and executed to make available the range of required knowledge and skills, including functional engineering skills, application problem-domain knowledge, interpersonal skills, multidisciplinary skills, and process-related skills. After the needed skills have been identified, evaluations of the appropriate mode of knowledge or skill acquisition can be used to select the most effective approach.

Typical Work Products

- assessment of skill types needed by skill category
- project knowledge acquisition plan
- training plan
- list of identified and available subject matter experts

Notes

Appropriate coverage of the full range of skill and knowledge types can be addressed with a checklist of knowledge types (e.g., functional engineering, problem domain, etc.) against each element of the work breakdown structure.

An example of ensuring the availability of the appropriate application-problem domain knowledge (e.g., satellite weather data processing), would be a plan to interview identified subject matter experts in connection with requirements interpretation or system design. Such an approach would be appropriate when an organization does not have the required expertise available (as with the first program in a new line of business).

continued on next page

BP 17.04 Prepare Training Materials

Prepare training materials based upon the identified training needs.

Description
Develop the training material for each class that is being developed and facilitated by people within the organization, or obtain the training material for each class that is being procured.

Typical Work Products
- course descriptions and requirements
- training material

Notes
Course description should include
- intended audience
- preparation for participation
- training objective
- length of training
- lesson plans
- criteria for determining the students' satisfactory completion

Prepare
- procedures for periodically evaluating the effectiveness of the training and special considerations, such as piloting and field testing the training course
- needs for refresher training, and opportunities for follow-up training
- materials for training a specific practice to be used as part of the process (e.g., method technique)
- materials for training a process
- materials for training in process skills such as statistical techniques, statistical process control, quality tools and techniques, descriptive process modeling, process definition, and process measurement

Review the training material with some or all of the following instructional experts, subject matters experts, and students from the pilot programs.

continued on next page

BP 17.05
Train Personnel

Train personnel to have the skills and knowledge needed to perform their assigned roles.

Description
Personnel are trained in accordance with the training plan and developed material.

Typical Work Products
- trained personnel

Notes
Offer the training in a timely manner (just-in-time training) to ensure optimal retention and the highest possible skill level.
- A procedure should exist to determine the skill level of the employee prior to receiving the training to determine if the training is appropriate (i.e., if a trainer waiver or equivalent should be administered to the employee).
- A process exists to provide incentives and motivate the students to participate in the training.
- Online training/customized instruction modules accommodate different learning styles and cultures, in addition to transferring smaller units of knowledge.

continued on next page

BP 17.06 Assess Training Effectiveness

Assess the effectiveness of the training to meet the identified training needs.

Description

A key aspect of training is determining its effectiveness. Methods of evaluating effectiveness need to be addressed concurrent with the development of the training plan and training material; in some cases, these methods need to be an integral part of the training material. The results of the effectiveness assessment must be reported in a timely manner so that adjustments can be made to the training.

Typical Work Products

- analysis of training effectiveness
- modification to training

Notes

A procedure should exist to determine the skill level of the employee after receiving the training to determine the success of the training. This could be accomplished via formal testing, on-the-job skills demonstration, or assessment mechanisms embedded in the courseware.

continued on next page

BP 17.07 Maintain Training Records

Maintain records of training and experience.

Description
Records are maintained to track the training that each employee has received and the employee's skills and capabilities.

Typical Work Products
- training and experience records

Notes
Records are kept of all students who successfully complete each training course or other approved training activity. Also, records of successfully completed training are made available for consideration in the assignment of the staff and managers.

BP 17.08 Maintain Training Materials

Maintain an accessible repository.

Description
Courseware material is maintained in a repository for future access by employees and for maintaining traceability in changes in course material.

Typical Work Products
- baselined training materials
- revisions to training materials

Notes
Maintain a repository of training materials and make it available to all employees. (For example, the organization's library could make books, notebooks, videotapes, etc., available; soft-copy training materials could be maintained in a public file server.) Incorporate lessons learned into process training materials and the training program. Update process training materials with all process changes and improvements.

End of PA 17: Provide Ongoing Skills and Knowledge

PA 18: Coordinate with Suppliers

Summary description

The purpose of Coordinate with Suppliers is to address the needs of organizations to effectively manage the portions of product work that are conducted by other organizations. Decisions made as a part of this process area should be made in accordance with the Analyze Candidate Solutions process area (PA01). The general term *supplier* is used to identify an organization that develops, manufactures, tests, supports, etc., a component of the system. Suppliers may take the form of vendors, subcontractors, partnerships, etc., as the business organization warrants.

In addition to coordination of schedules, processes, and deliveries of work products, affected organizations must have a shared a vision of the working relationship. Relationships can range from integrated developer / supplier product teams, to prime-contractor / subcontractor, to vendors, and more. A successful relationship between an organization and a supplier depends on the capability of both organizations, and on a mutual understanding of the relationship and expectations.

Process area notes

When suppliers deliver products that do not meet an organization's needs, the organization has the option to change to another supplier, lower its standards and accept the delivered products, or help the supplier or vendor meet the organization's needs.

The organization acts as the customer when the supplier executes the Understand Customer Needs and Expectations process area (PA06). The organization should help the supplier to achieve full understanding. If the supplier does not have the processes to execute this process area, the organization should coach the supplier in getting the necessary information.

continued on next page

PA 18: Coordinate with Suppliers, Continued

Base practices list

The following list contains the base practices that are essential elements of good systems engineering:

BP.18.01 Identify needed system components or services that must be provided by other/outside organizations.

BP.18.02 Identify suppliers that have shown expertise in the identified areas.

BP.18.03 Choose suppliers in accordance with the Analyze Candidate Solutions process area (PA01).

BP.18.04 Provide to suppliers the needs, expectations, and measures of effectiveness held by the organization for the system components or services that are to be delivered.

BP.18.05 Maintain timely two-way communication with suppliers.

continued on next page

BP 18.01 Identify Systems Components or Services

Identify needed system components or services that must be provided by other/outside organizations.

Description

Rarely does an organization make every component of the system. Make-vs.-buy analyses and decisions determine which items will be procured. System needs that will be satisfied outside the organization are generally those in which the organization has little expertise or interest.

Typical Work Products

- make-vs.-buy trade study
- list of system components
- sub set of system components for outside organizations to address
- list of potential suppliers
- beginnings of criteria for completion of needed work

Notes

Example practices include

- Perform trade study.
- Examine own organization to determine missing expertise needed to address system requirements.

continued on next page

BP 18.02 Identify Competent Suppliers or Vendors

Identify suppliers that have shown expertise in the identified areas.

Description
The capabilities of the supplier should be complementary and compatible with those of the organization. Issues that may be of concern include competent development processes, manufacturing processes, responsibilities for verification, on-time delivery, life-cycle support processes, and ability to communicate effectively over long distances (video teleconferencing, electronic file transfers, e-mail and the like).

Typical Work Products
- list of suppliers
- advantages and disadvantages of each supplier
- potential ways of working over physical distances with suppliers

Notes
Example practices include
- Read trade journals.
- Use available library services.
- Use organizational knowledge-base (perhaps an online system).

continued on next page

BP 18.03 Choose Supplier or Vendors

Choose suppliers in accordance with the Analyze Candidate Solutions process area (PA01).

Description

Suppliers are selected in a logical and equitable manner to meet product objectives. The characteristics of a supplier which would best complement the organization's abilities are determined, and qualified candidates are identified. The practices of the Analyze Candidate Solutions process area (PA01) are applied to select the appropriate supplier.

Typical Work Products

- organization weaknesses which might be mitigated by a supplier
- characteristics of the desired working relationships with the supplier
- supplier requirements
- customer requirements to be "flowed down" to supplier
- selected supplier
- captured rationale for selected supplier

Notes

An important consideration in the selection of the supplier is the expected working relationship. This could range from a highly integrated product team to a classical "meet the requirements" relationship. The selection criteria are likely different, depending of the desired relationship.

continued on next page

BP 18.04 Provide Expectations

Provide to suppliers the needs, expectations, and measures of effectiveness held by the developing organization for the system components or services that are to be delivered.

Description
The contracting organization must clearly identify and prioritize its needs and expectations, as well as any limitations on the part of the suppliers. The organization works closely with suppliers to achieve a mutual understanding of product requirements, responsibilities, and processes which will be applied to achieve program objectives.

Typical Work Products
- needs statement
- technical performance parameters
- verification specifications

Notes
Examples of techniques and forums for providing needs, expectations, and measures of effectiveness to suppliers or vendors include
- trade studies
- formal contracts
- in-process reviews
- joint meetings
- payment milestones

continued on next page

BP 18.05 Maintain Communications

Maintain timely two-way communications with suppliers.

Description

The organization and supplier establish a mutual understanding of expected and needed communications. Characteristics of communications that are established include the types of information that are considered open and subject to no restrictions, the types of information subject to restrictions (e.g., policy or contractual relationships), the expected timeliness of information requests and responses, tools and methods to be used for communications, security, privacy, and distribution expectations. The need for "face-to-face" versus "at-a-distance" communications, and the need and mechanism for archiving communications are also considered.

Typical Work Products

- contractually required communication
- communications tools
- communications plans
- communications distribution lists

Notes

An effective communications environment between the organization and supplier is highly desirable. E-mail and voice-mail tools are effective for simple communications where two-way communication is not required.

Communications that affect schedule cost or scope should be restricted to authorized parties.

End of PA 18: Coordinate with Suppliers