

---

---

**Information technology — Systems  
Security Engineering — Capability Maturity  
Model (SSE-CMM®)**

*Technologies de l'information — Ingénierie de sécurité système — Modèle  
de maturité de capacité (SSE-CMM®)*

IECNORM.COM : Click to view the full PDF of ISO/IEC 21827:2002

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

IECNORM.COM : Click to view the full PDF of ISO/IEC 21827:2002

© ISO/IEC 2002

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.ch](mailto:copyright@iso.ch)  
Web [www.iso.ch](http://www.iso.ch)

Printed in Switzerland

## Contents

Foreword .....	v
Introduction .....	vi
1 Scope .....	1
2 Normative references .....	1
3 Terms and definitions .....	2
4 Background .....	5
4.1 Reason for Development .....	5
4.2 The Importance of Security Engineering .....	6
4.3 Consensus .....	6
5 Structure of the Document .....	7
6 Model Architecture .....	7
6.1 Security Engineering .....	7
6.2 Security Engineering Process Overview .....	9
6.3 SSE-CMM® Architecture Description .....	12
6.4 Summary Chart .....	20
7. Security Base Practices .....	20
7.1 PA01 - Administer Security Controls .....	21
7.2 PA02 - Assess Impact .....	24
7.3 PA03 - Assess Security Risk .....	28
7.4 PA04 - Assess Threat .....	31
7.5 PA05 - Assess Vulnerability .....	34
7.6 PA06 - Build Assurance Argument .....	37
7.7 PA07 - Coordinate Security .....	40
7.8 PA08 - Monitor Security Posture .....	42
7.9 PA09 - Provide Security Input .....	47
7.10 PA10 - Specify Security Needs .....	50
7.11 PA11 - Verify and Validate Security .....	54
Annex A(normative)Generic Practices .....	57
A.1 General .....	57
A.2 Capability Level 1 - Performed Informally .....	57
A.3 Capability Level 2 - Planned and Tracked .....	58
A.4 Capability Level 3 - Well Defined .....	63
A.5 Capability Level 4 - Quantitatively Controlled .....	68
A.6 Capability Level 5 - Continuously Improving .....	70

**ISO/IEC 21827:2002(E)**

Annex B(normative)Project and Organizational Base Practices ..... 73

- B.1 General ..... 73
- B.2 General Security Considerations ..... 73
- B.3 PA12 - Ensure Quality ..... 73
- B.4 PA13 - Manage Configurations ..... 78
- B.5 PA14 - Manage Project Risks ..... 81
- B.6 PA15 - Monitor and Control Technical Effort ..... 85
- B.7 PA16 - Plan Technical Effort ..... 88
- B.8 PA17 - Define Organization's Systems Engineering Process ..... 93
- B.9 PA18 - Improve Organization's Systems Engineering Processes ..... 96
- B.10 PA19 - Manage Product Line Evolution ..... 99
- B.11 PA20 - Manage Systems Engineering Support Environment ..... 101
- B.12 PA21 - Provide Ongoing Skills and Knowledge ..... 105
- B.13 PA22 - Coordinate with Suppliers ..... 110

Annex C(informative)Capability Maturity Model Concepts ..... 114

- C.1 General ..... 114
- C.2 Process Improvement ..... 114
- C.3 Expected Results ..... 115
- C.4 Common Misunderstandings ..... 115
- C.5 Key Concepts ..... 116

Bibliography ..... 120

IECNORM.COM : Click to view the full PDF of ISO/IEC 21827:2002

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 21827 was prepared by the International Systems Security Engineering Association (ISSEA) (formerly the Systems Security Engineering — Capability Maturity Model<sup>®1)</sup> Project) and was adopted, under the PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Annexes A and B form a normative part of this International Standard. Annex C is for information only.

---

1) ©CMM and Capability Maturity Model are Service Marks of Carnegie Mellon University

Not-for-profit corporation

5000 Forbes Avenue, Pittsburgh, PA 15213

## Introduction

A wide variety of organizations practice security engineering in the development of computer programs, whether as operating systems software, security managing and enforcing functions, software, middleware of applications programs. Appropriate methods and practices are therefore required by product developers, service providers, system integrators, system administrators, and even security specialists. Some of these organizations deal with high-level issues (e.g., ones dealing with operational use or system architecture), others focus on low-level issues (e.g., mechanism selection or design), and some do both. Organizations may specialize in a particular type of technology, or a specialized context (e.g. at sea).

The SSE-CMM® is designed for all these organizations. Use of the SSE-CMM should not imply that one focus is better than another is or that any of these uses are required. An organization's business focus need 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 examples below illustrate ways in which the SSE-CMM® may be applied to software, systems, facilities development and operation by a variety of different organizations.

### **Security Service Providers**

To measure the process capability of an organization that performs risk assessments, several groups of practices come into play. During system development or integration, 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.

### **Countermeasure Developers**

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 that provides the service of developing countermeasures needs to understand the relationships between these practices.

### **Product Developers**

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.

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®:

- Type of customer base (products, systems, or services);
- Assurance requirements (high vs. low);
- 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.

### **Specific Industry Segments**

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.

### **How Should the SSE-CMM® 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;
- Method by which security engineering evaluation organizations such as certifiers and evaluators can establish confidence in the organizational capability as one input to system or product security assurance;
- Standard mechanism for customers to evaluate a provider's security engineering capability.

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. Additional information on using process assessment can be found in ISO/IEC CD 15504-4 Software Engineering — Process Assessment — Part 4: Guidance on use for Process Improvement and Process Capability Determination.

### **Benefits of Using the SSE-CMM®**

The trend for security is a shift from protecting classified government data to a broader spectrum of concerns including financial transactions, contractual agreements, personal information, and the Internet. A corresponding proliferation of products, systems, and services that maintain and protect information has emerged. These security products and systems typically come to market in one of two ways: through lengthy and expensive evaluation or without evaluation. In the former case, trusted products often reach the market long after their features are needed and secure systems are being deployed that no longer address current threats. In the latter, acquirers and users must rely solely on the security claims of the product or system developer or operator. Further, security engineering services traditionally were often marketed on this caveat emptor basis.

This situation calls for organizations to practice security engineering in a more mature manner. Specifically, the following qualities are needed in the production and operation of secure systems and trusted products:

- Continuity - knowledge acquired in previous efforts is used in future efforts;
- Repeatability - a way to ensure that projects can repeat a successful effort;
- Efficiency - a way to help both developers and evaluators work more efficiently;
- Assurance - confidence that security needs are being addressed.

To provide for these requirements, a mechanism is needed to guide organizations in understanding and improving their security engineering practices. To address these needs, the SSE-CMM® is being developed to advance the state of the practice of security engineering with the goal of improving the quality and availability of and reducing the cost of delivering secure systems, trusted products, and security engineering services. In particular, the following benefits are envisioned:

#### *To Engineering Organizations:*

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

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

#### *To Acquiring Organizations:*

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

- Reusable 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.

## ISO/IEC 21827:2002(E)

### *To Evaluation Organizations:*

Evaluation organizations include System Certifiers, System Accreditors, Product Evaluators, and Product Assessors. Benefits of the SSE-CMM® to these organizations include:

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 21827:2002

# Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)

## 1 Scope

The SSE-CMM® is a process reference model. It is focussed upon the requirements for implementing security in a system or series of related systems that are the ITS domain. Within the ITS domain the SSE-CMM® Model is focussed on the processes used to achieve ITS, most specifically on the maturity of those processes. There is no intent within the SSE-CMM® Model to dictate a specific process to be used by an organization, let alone a specific methodology. Rather the intent is that the organization making use of the SSE-CMM® Model should use its existing processes, be those processes based upon any other ITS guidance document. The scope encompasses:

- the system security engineering activities for a secure product or a trusted system addressing the complete lifecycle of: concept definition, requirements analysis, design, development, integration, installation, operation, maintenance and de-commissioning;
- requirements for product developers, secure systems developers and integrators, organizations that provide computer security services and computer security engineering;
- applies to all types and sizes of security engineering organizations from commercial to government and the academe.

While the SSE-CMM® is a distinct model to improve and assess security engineering capability, this should not imply that security engineering should be practised 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 and 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.

This International Standard has a relationship to TR 15504, particularly part 2, as both are concerned with process improvement and capability maturity assessment. However, TR 15504 is specifically focussed on software processes, whereas the SSE-CMM is focussed on security.

This International Standard has a closer relationship with the new versions of 15504, particularly CD 15504-2, and is compatible with its approaches and requirements.

## 2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 12207, *Information technology — Software life cycle processes*

ISO/IEC TR 13335-1, *Information technology — Guidelines for the management of IT Security — Part 1: Concepts and models for IT Security*

ISO/IEC 15288, *Systems engineering — System life cycle processes*

## ISO/IEC 21827:2002(E)

ISO/IEC TR 15504-2, *Information technology — Software process assessment — Part 2: A reference model for processes and process capability*

ISO/IEC TR 15504-4, *Information technology — Software process assessment — Part 4: Guide to performing assessments*

ISO/IEC 17799: 2000, *Information technology — Code of practice for information security management*

### 3 Terms and definitions

For the purposes of this International Standard, the following terms and definitions apply.

#### 3.1 Accountability

The property that ensures that the actions of an entity can be traced uniquely to the entity. [ISO 7498-2:1988]

#### 3.2 Accreditation

In the context of this document: 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.

Note: This definition is generally accepted within the security community; within ISO the more generally used definition is: Procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks. [ISO/IEC Guide 2].

#### 3.3 Assessment

Verification of a product, system, or service against a standard using the corresponding assessment method to establish compliance and determine the assurance. [ISO/IEC 15443-1].

#### 3.4 Asset

Anything that has value to the organization [ISO 13335-1:1996].

#### 3.5 Assurance

In the context of this document: Grounds for confidence that a deliverable meets its security objectives. [ISO/IEC 15408-1].

Note: This definition is generally accepted within the security community; within ISO the more generally used definition is: Activity resulting in a statement giving confidence that a product, process or service fulfills specified requirements. [ISO/IEC Guide 2]

#### 3.6 Assurance Argument

A set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied.

#### 3.7 Assurance Claim

An assertion or supporting assertion that a system meets a security need. Claims address both direct threats (e.g., system data are protected from attacks by outsiders) and indirect threats (e.g., system code has minimal flaws).

#### 3.8 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.

#### 3.9 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].

#### 3.10 Availability

The property of being accessible and useable upon demand by an authorized entity. [ISO 7498-2: 1988].

**3.11 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].

**3.12 Certification**

In the context of this document, the process producing written results of performing a comprehensive evaluation of security features and other safeguards of a system to establish the extent to which the design and implementation meet a set of specified security requirements.

Note: This definition is generally accepted within the security community; within ISO the more generally used definition is: Procedure by which a third party gives written assurance that a product, process or service conforms to specified requirements. [ISO/IEC Guide 2]

**3.13 Confidentiality**

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO 7498-2:1988].

**3.14 Consistency**

The degree of uniformity, standardization, and freedom from contradiction among the documents or parts of a system or component. [IEEE-STD-610].

**3.15 Correctness**

For specified security requirements, the representation of a product or system that shows the implementation of the requirement is correct.

**3.16 Customer**

Recipient of a product provided by the supplier.

NOTE 1: In a contractual situation, the customer is called the purchaser.

NOTE 2: The customer may be, for example, the ultimate consumer, user, beneficiary or purchaser.

NOTE 3: The customer can be either external or internal to the organization. [ISO 8402] [ISO/IEC TR 15504]

**3.17 Effectiveness**

A property of a system or product representing how well it provides security in the context of its proposed or actual operational use.

**3.18 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).

**3.19 Evidence**

Directly measurable characteristics of a process and/or product that represent objective, demonstrable proof that a specific activity satisfies a specified requirement.

**3.20 Integrity**

Integrity is defined as safeguarding the accuracy and completeness of information and processing methods.

**3.21 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].

**3.22 Methodology**

A collection of standards, procedures and supporting methods that define the complete approach to the development of a product or system.

## ISO/IEC 21827:2002(E)

### 3.23 Penetration Profile

A definition of the activities required to effect a penetration.

### 3.24 Procedure

A written description of a course of action to be taken to perform a given task. [IEEE-STD-610].

### 3.25 Process

A set of interrelated activities, which transform inputs into outputs. [ISO/IEC 15288].

### 3.26 Reliability

The property of consistent behaviour and results. [ISO 13335-1:1996].

### 3.27 Residual Risk

The risk that remains after safeguards have been implemented [ISO 13335-1:1996].

### 3.28 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 [ISO 13335-1:1996].

### 3.29 Risk Analysis

The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. [ISO 13335-1:1996].

### 3.30 Risk Management

Process of assessing and quantifying risk and establishing acceptable level of risk for the organization. [ISO 13335-1:1996].

### 3.31 Security Policy

Within the context of this document; rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its systems, particularly those which impact the systems and associated elements.

### 3.32 Security Related Requirements

Requirements which have a direct effect on the secure operation of a system or enforce conformance to a specified security policy.

### 3.33 System

A discrete, distinguishable entity with a physical existence and a defined purpose, completely composed of integrated, interacting components, each of which does not individually comply with the required overall purpose. [ISO/IEC 15288].

Note 1: In practice, a system is 'in the eye of the beholder' and the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g. product system, aircraft system. Alternatively the word system may be substituted simply by a context dependent synonym, e.g. product, aircraft, though this may then obscure a system principles perspective.

Note 2: The system may need other systems during its life cycle to meet its requirements. Example - an operational system may need a system for conceptualization, development, production, operation, support or disposal.

### 3.34 Threat

Capabilities, intentions and attack methods of adversaries, or any circumstance or event, whether originating externally or internally, that has the potential to cause harm to information or a program or system or cause those to harm others.

### 3.35 Threat Agent

The originator and/or the initiator of deliberate or accidental man-made threats.

**3.36 Validation**

Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled. [ISO/IEC 15288].

**3.37 Verification**

Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled. [ISO/IEC CD 15288].

**3.38 Vulnerability**

Includes a weakness of an asset or group of assets which can be exploited by a threat [ISO 13335-1:1996].

**3.39 Work Product**

An artefact associated with the execution of a process. [ISO/IEC TR 15504-9].

Note: A work product might be used, produced or changed by a process.

**4 Background**

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 prescribe 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;
- 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 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. The SSE-CMM® Appraisal Method describes the process and tools for evaluating an organization's security engineering capability against the SSE-CMM®.

**4.1 Reason for Development**

Both customers and suppliers are interested in improving the development of security products, systems, and services. The field of security engineering has several generally 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.

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. This does not conflict with the premise that security engineering is done in context with systems engineering. In fact, having well-defined and accepted systems engineering activities will allow security engineering to be practised effectively in all contexts.

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:

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

### 4.2 The Importance of Security Engineering

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 expanded from one primarily concerned with safeguarding classified government data to broader applications including financial transactions, contractual agreements, personal information, and the Internet. These trends have elevated the importance of security engineering.

### 4.3 Consensus

The SSE-CMM® Model was developed by over 50 organization, many of them multi-national corporations. The Project had representatives from several Nations, notably Australia, Canada, Europe and the US. In addition, the SSE-CMM® project continually sought participation through various venues, including presentations and booths at conferences and through the public website [www.sse-cmm.org](http://www.sse-cmm.org).

The participants were organized into a Steering Group, and a number of Working Groups. The majority of the development was performed by the Working Groups, while the Steering Group was responsible for overall project progress and approval of Project deliverables.

The SSE-CMM® model was developed by a consensus process. All member organizations could send representatives to the working group meetings, and the majority did. Contributions were sent electronically to all members of the working group in the intervening period between meetings. Meetings were held on a monthly basis where input suggestions were discussed, revised and agreed. The results of any votes that were necessary were recorded in the working group meeting minutes issued for each meeting. These records have been maintained.

Each version of the SSE-CMM® Model was first approved by the working group tasked with development. It was then reviewed and approved by the Steering Group. After the Steering Group had approved the version it was then sent to a group of "Key reviewers" drawn from the ITS community at large for their review and comment. Each version was then released for public review and feedback. Based on the feedback from the Key reviewers and the community at large, the Steering Group made a determination of the final release of that version of the SSE-CMM® Model.

The SSE-CMM® Model has been approved first at the working group level; second at the Steering Group level, third at the Key Reviewer level, and finally at the community level. Thus, in essence, four levels of approval have been obtained.

Additional approval and consensus has been achieved during the Pilot Appraisals through the impact of application of the Model to different application domains. The Alternative Assurance Working Group (AAWG) of the Common Criteria Project has reviewed the SSE-CMM® Model for applicability as an alternative to the generation of assurance by evaluation and provided IT systems security community consensus feedback to the project.

Each major release of the Model was reviewed by a set of independent reviewers who had not been involved in its development. Their comments were consolidated, reviewed and incorporated in the Model. Finally, each version of the document was subjected to public review, the CDR and the two public workshops, and the comments received, addressed.

## 5 Structure of the Document

Clause 4 discusses some of the background of the document and the reasons for its development. Clause 6 addresses the architecture of the SSE-CMM Model and the role of systems security engineering. Clause 7 describes the systems security engineering process areas and base practices in detail. Annex A describes the capability maturity levels and generic practices, while Annex B describes the project and organization process areas and base practices. Annex C discusses the concepts of capability maturity models. ISO/IEC TR 15504-4 can also be applied to the use of the SSE-CMM®.

## 6 Model Architecture

The SSE-CMM® is a compilation of the best-known security engineering practices. To understand this model, some background in security engineering is required. This section provides a high level description of security engineering, and then describes how the architecture of the model reflects this basic understanding.

### 6.1 Security Engineering

#### 6.1.1 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 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.

#### 6.1.2 Description of Security Engineering

Security engineering is an evolving discipline. As such, a precise definition with community consensus does not exist today. However, some generalizations are possible. Some goals of security engineering are to:

- Gain understanding of the security risks associated with an enterprise;
- Establish a balanced set of security needs in accordance with identified risks;
- 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 or assurance in the correctness and effectiveness of security mechanisms;
- Determine 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.

#### 6.1.3 Security Engineering Organizations

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

- Developers;
- Product vendors;

## ISO/IEC 21827:2002(E)

- Integrators;
- Acquirers (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.

### 6.1.4 Security Engineering Life Cycle

Security engineering activities are practised during all life cycle phases, including:

- Concept stage;
- Development stage;
- Production stage;
- Utilization stage;
- Support stage;
- Retirement stage.

### 6.1.5 Security Engineering and Other Disciplines

Security engineering activities interface with many other disciplines, including:

- Enterprise engineering;
- Systems engineering;
- Software engineering;
- Human factors engineering;
- Communications engineering;
- Hardware engineering;
- Test engineering;
- System administration.

Note 1: With respect to systems engineering, further information can be found in ISO/IEC 15288 which views security from a systems perspective.

Note 2: With respect to software engineering, further information can be found in ISO/IEC 12207:1995 which views security from a software perspective.

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, acquirer, 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.

### 6.1.6 Security Engineering Specialties

While Security Engineering and Information Technology Security are very often the driving disciplines in the current security and business environment, other more traditional security disciplines, such as Physical Security and Personnel Security should not be overlooked. Security Engineering will need to draw upon these and many other specialist sub-disciplines if they are to achieve the most efficient and effective results in the performance of their work. The list below gives a few examples of specialty security sub-disciplines likely to be required, along with a short description of each. Examples of security specialty sub-disciplines include:

- Operations Security targets the security of the operating environment, and the maintenance of a secure operating posture;
- Information Security pertains to information and the maintenance of security of the information during its manipulation and processing;
- Network Security involves the protection of network hardware, software, and protocols, including information communicated over networks;
- Physical Security focuses on the protection buildings and physical locations;
- Personnel Security is related to people, their trustworthiness and their awareness of security concerns;
- Administrative Security is related to the administrative aspects of security and security in administrative systems;

- Communications Security is related to the communication of information between security domains, specifically the protection of information while it is being moved through the transport medium;
- Emanation Security deals with undesired signals generated by all machines that can transmit information outside the security domain;
- Computer Security deals specifically with the security computing devices of all types.

## 6.2 Security Engineering Process Overview

The SSE-CMM® divides security engineering into three basic areas: risk, engineering, and assurance, see figure 1. While these areas are by no means independent from one another, it is possible to consider them separately. At the simplest level, the risk process identifies and prioritizes dangers inherent to the developed product or system. The security engineering process works with the other engineering disciplines to determine and implement solutions to the problems presented by the dangers. Finally, the assurance process establishes confidence in the security solutions and conveys this confidence to the customers.

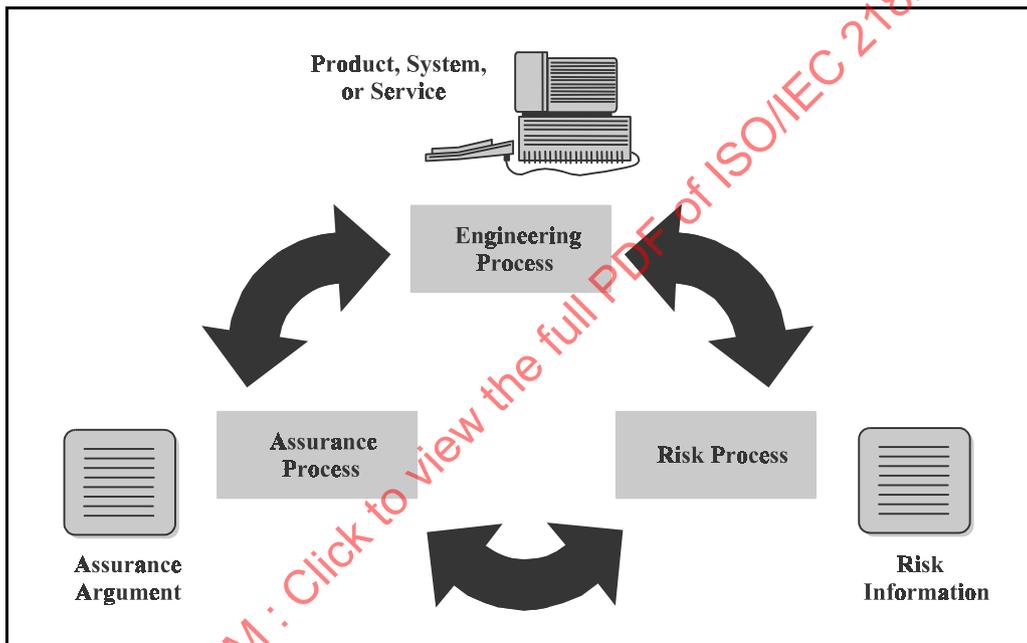


Figure 1 - The security engineering process has three main areas.

Together, these three areas work together with the goal of ensuring that the security engineering process results achieve the goals described above.

### 6.2.1 Risk

A major goal of security engineering is the reduction of risk. Risk assessment is the process of identifying problems that have not yet occurred. Risks are assessed by examining the likelihood of the threat and vulnerability and by considering the potential impact of an unwanted incident, see figure 2. 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. Because the factors may have a large amount of uncertainty as to the accuracy of the predictions associated with them, planning and the justification of security can be very difficult. One way to partially deal with this problem in a cost-effective manner is to implement techniques to detect the occurrence of an unwanted incident.

An unwanted incident is made up of three components: threat, vulnerability, and impact. Vulnerabilities are properties of the asset that may be exploited by a threat and include weaknesses. If either the threat or the vulnerability is not present there can be no unwanted incident and thus no risk. Risk management is the process of assessing and

quantifying risk, and establishing an acceptable level of risk for the organization. Managing risk is an important part of the management of security.

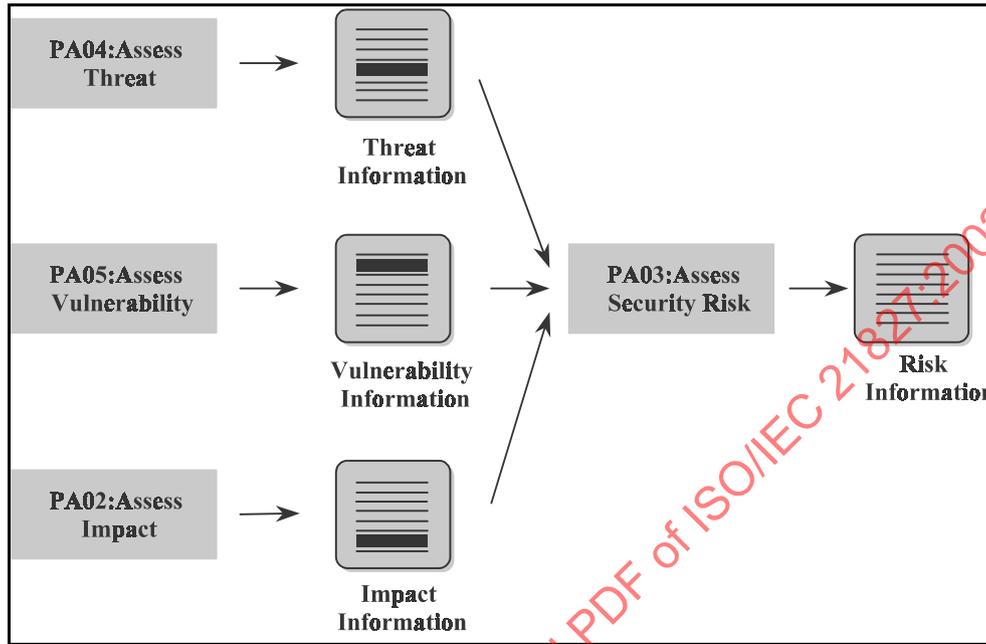


Figure 2 - The security risk process involves threats, vulnerabilities, and impact.

Risks are mitigated by the implementation of safeguards, which may address the threat, the vulnerability, the impact, or the 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® process areas include activities that ensure that the provider organization is analyzing threats, vulnerabilities, impacts, and associated risk.

### 6.2.2 Engineering

Security engineering, like other engineering disciplines, is a process that proceeds through concept, design, implementation, test, deployment, operation, maintenance, and decommission. Throughout this process, security engineers must work closely with the other parts of the system engineering team. The SSE-CMM® emphasizes that security engineers are part of a larger team and need to coordinate their activities with engineers from other disciplines. This helps to ensure that security is an integral part of the larger process, and not a separate and distinct activity.

Using the information from the risk process described above, and other information about system requirements, relevant laws, and policies, security engineers work with the customer to identify security needs, see figure 3. Once needs are identified, security engineers identify and track specific requirements.

The process of creating solutions to security problems generally involves identifying possible alternatives and then evaluating the alternatives to determine which is the most promising. The difficulty in integrating this activity with the rest of the engineering process is that the solutions cannot be selected on security considerations alone. Rather, a wide variety of other considerations, including cost, performance, technical risk, and ease of use must be addressed. Typically, these decisions should be captured to minimize the need to revisit issues. The analyses produced also form a significant basis for assurance efforts.

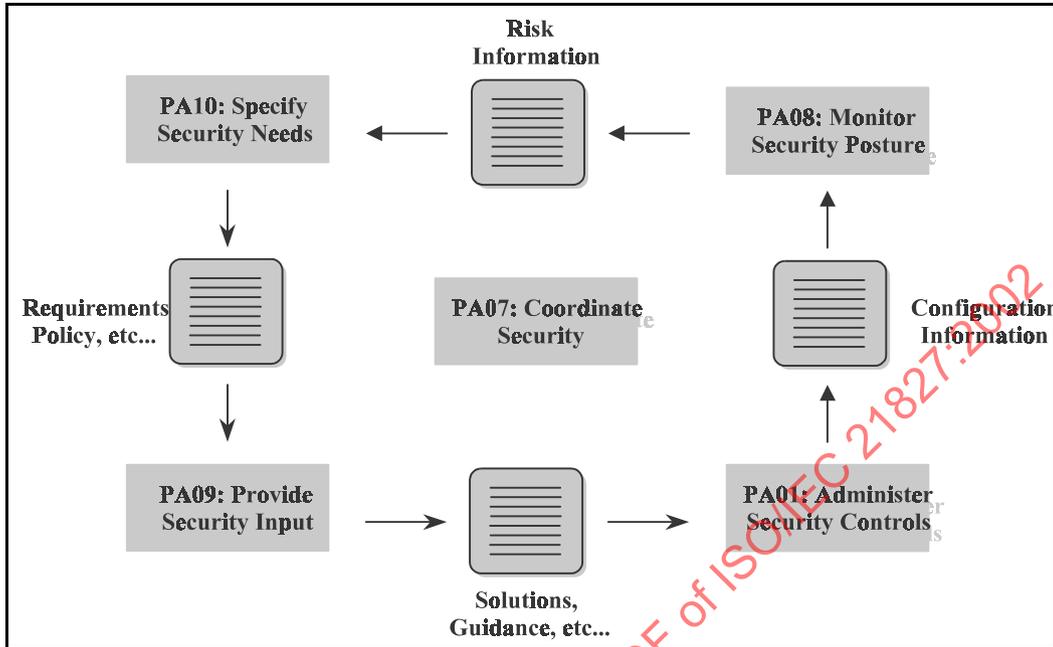


Figure 3 - Security is an integral part of the overall engineering process.

Later in the lifecycle, the security engineer is called on to ensure that products and systems are properly configured in relation to the perceived risks, ensuring that new risks do not make the system unsafe to operate.

### 6.2.3 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 repeatability 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, see figure 4. The detailed relationship between different forms of assurance is the subject of ongoing research.

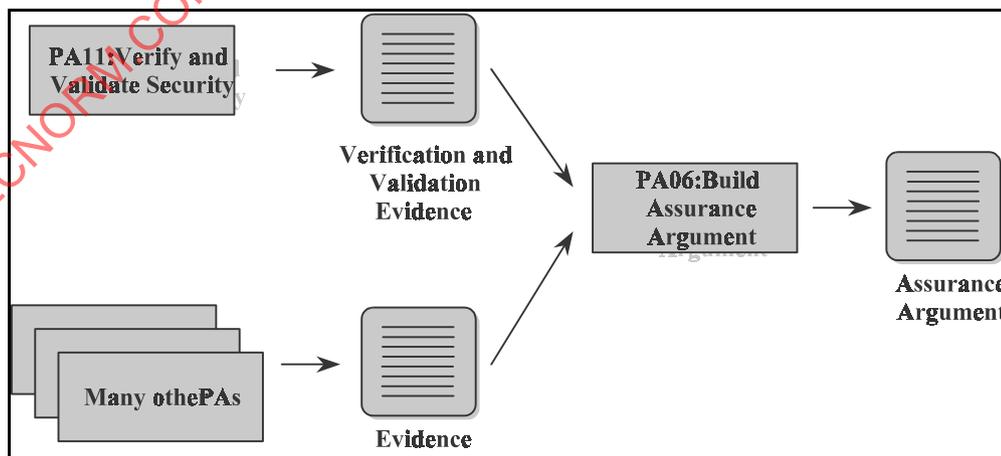


Figure 4 - The assurance process builds an argument establishing confidence.

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 communicated in the form of an argument. The argument includes a set of claims about properties of the system. These claims are supported by evidence. The evidence is frequently in the form of documentation developed during the normal course of security engineering activities.

The SSE-CMM® activities themselves involve the production of assurance relevant evidence. For example, process documentation can indicate that the development has followed a well-defined and mature engineering process that is subject to continuous improvement. Security verification and validation play a large role in establishing the trustworthiness of a product or system.

Many of the example work products included within the process areas 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 focussing on the process used to produce them. The maturity of the organizational practices will influence and contribute to the process.

### 6.3 SSE-CMM® Architecture Description

The SSE-CMM® architecture is designed to enable a determination of a security engineering organization's process maturity across the breadth of security engineering. The goal of the architecture is to clearly separate basic characteristics of the security engineering process from its management and institutionalization characteristics. In order to ensure this separation, the model has two dimensions, called "domain" and "capability" which are described below.

Importantly, the SSE-CMM® does not imply that any particular group or role within an organization must do any of the processes described in the model. Nor does it require that the latest and greatest security engineering technique or methodology be used. The model does require, however, that an organization have a process in place that includes the basic security practices described in the model. The organization is free to create their own process and organizational structure in any way that meets their business objectives.

#### 6.3.1 The Basic Model

The SSE-CMM® has two dimensions, "domain" and "capability." The domain dimension is perhaps the easier of the two dimensions to understand. This dimension simply consists of all the practices that collectively define security engineering. These practices are called "base practices." The structure and content of these base practices are discussed below.

The capability dimension represents practices that indicate process management and institutionalization capability. These practices are called "generic practices" as they apply across a wide range of domains. The generic practices represent activities that should be performed as part of doing a base practices.

Figure 5 illustrates the relationship between base practices and generic practices. A fundamental part of security engineering is the identification of security vulnerabilities. This activity is captured in the SSE-CMM® in Base Practice 05.02, "Identify System Security Vulnerabilities."

One way to determine an organization's ability to do something is to check whether they have a process for allocating resources to the activities they claim to be doing. This "characteristic" of mature organizations is reflected in the SSE-CMM® in Generic Practice 2.1.1, "Allocate Resources."

Putting the base practice and generic practice together provides a way to check an organization's capability to perform a particular activity. Here an interested party might ask, "does your organization allocate resources for identifying system security vulnerabilities?" If the answer is "yes," the interviewer learns a little about the organization's capability.

Answering all the questions raised by combining all the base practices with all the generic practices will provide a good picture of the security engineering capability of the organization in question.

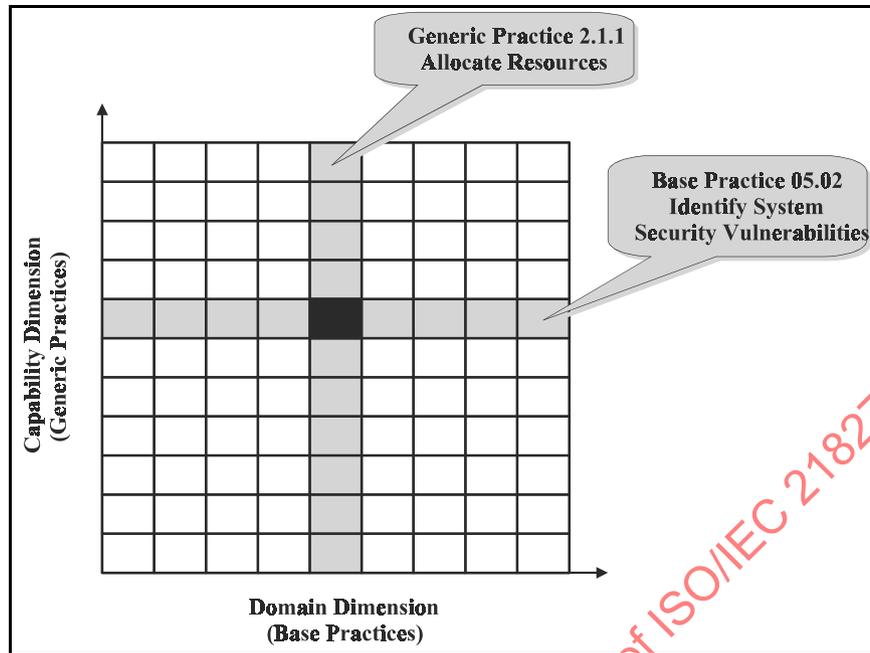


Figure 5 - The model evaluates each process area against each common feature.

### 6.3.2 The Base Practices

The SSE-CMM® contains 129 base practices, organized into 22 process areas. Of these 61 base practices, organized in 11 process areas, cover all major areas of security engineering. The remaining 68 base practices, organized in 11 process areas, address the project and organization domains. They have been drawn from the Systems Engineering and Software CMM®. They are required to provide a context and support for the Systems Security Engineering process areas. The base practices for security were gathered from a wide range of existing materials, practice, and expertise. The practices selected represent the best existing practice of the security engineering community, not untested practices.

Identifying 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. However, an organization cannot be considered to have achieved a base practice if it is only performed during the design phase or at a single level of abstraction. Therefore, the SSE-CMM® ignores these distinctions and identifies the basic set of practices that are essential to the practice of good security engineering.

A base practice:

- Applies across the life cycle of the enterprise;
- Does not overlap with other Base Practices;
- Represents a "best practice" of the security community;
- Does not simply reflect a state-of-the-art technique;
- Is applicable using multiple methods in multiple business contexts;
- Does not specify a particular method or tool.

The base practices have been organized into process areas in a way that meets a broad spectrum of security engineering organizations. There are many ways to divide the security engineering domain into process areas. One might try to model the real world, creating process areas that match security engineering services. Other strategies attempt to identify conceptual areas that form fundamental security engineering building blocks. The SSE-CMM® compromises between these competing goals in the current set of process areas.

Each process area has a set of goals that represent the expected state of an organization that is successfully performing the process area. An organization that performs the base practices of the process area should also achieve its goals.

A process area:

- Assembles related activities in one area for ease of use;
- Relates to valuable security engineering services;
- Applies across the life cycle of the enterprise;
- Can be implemented in multiple organization and product contexts;
- Can be improved as a distinct process;
- Can be improved by a group with similar interests in the process;
- Includes all base practices that are required to meet the goals of the process area.

The eleven systems security engineering process areas of the SSE-CMM® are listed below. Note that they are listed in alphabetical order to discourage the notion that there the process areas are ordered by lifecycle phase or area. These process areas and the base practices that define them are described in Clause 6., and listed below:

- PA01 Administer Security Controls;
- PA02 Assess Impact;
- PA03 Assess Security Risk;
- PA04 Assess Threat;
- PA05 Assess Vulnerability;
- PA06 Build Assurance Argument;
- PA07 Coordinate Security;
- PA08 Monitor Security Posture;
- PA09 Provide Security Input;
- PA10 Specify Security Needs;
- PA11 Verify and Validate Security.

The SSE-CMM® also includes eleven process areas related to project and organizational practices. These process areas were adapted from the SE-CMM®. These process areas and the base practices that define them are described in Annex B, and listed below:

- PA12 - Ensure Quality;
- PA13 - Manage Configuration;
- PA14 - Manage Project Risk;
- PA15 - Monitor and Control Technical Effort;
- PA16 - Plan Technical Effort;
- PA17 - Define Organization's Systems Engineering Process;
- PA18 - Improve Organization's Systems Engineering Process;
- PA19 - Manage Product Line Evolution;
- PA20 - Manage Systems Engineering Support Environment;
- PA21 - Provide Ongoing Skills and Knowledge;
- PA22 - Coordinate with Suppliers.

Note: These PAs have been placed in an annex to facilitate future enhanced alignment with 15288.

### 6.3.3 The Generic Practices

Generic practices are activities that apply to all processes. They address the management, measurement, and institutionalization aspects of a process. In general, they are used during an appraisal to determine the capability of an organization to perform a process.

Generic practices are grouped into logical areas called "Common Features" which are organized into five "Capability Levels" which represent increasing organizational capability. Unlike the base practices of the domain dimension, the generic practices of the capability dimension are ordered according to maturity. Therefore, generic practices that indicate higher levels of process capability are located at top of the capability dimension.

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. The lowest common feature is 1.1 Base Practices are Performed. This common features simply checks whether an organization performs all the base practices in a process area.

Subsequent common features have generic practices that help to determine how well a project manages and improves each process area as a whole. The generic practices, described in Clause 5, are grouped to emphasize any major shift in an organization's characteristic manner of doing security engineering. Table 3.1 lists some principles captured in the generic practices.

**Table 1 — Capability dimension principles**

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 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 emphasized the cultural shifts that will sustain the gains made.

The common features below represent the attributes of mature security engineering necessary to achieve each level. These common features and the generic practices that define them are described in Clause 5.

Level 1:

- 1.1 Base Practices are Performed;

Level 2:

- 2.1 Planning Performance;
- 2.2 Disciplined Performance;
- 2.3 Verifying Performance;
- 2.4 Tracking Performance;

Level 3:

- 3.1 Defining a Standard Process;
- 3.2 Perform the Defined Process;
- 3.3 Coordinate the Process;

Level 4:

- 4.1 Establishing Measurable Quality Goals;
- 4.2 Objectively Managing Performance;

Level 5:

- 5.1 Improving Organizational Capability;
- 5.2 Improving Process Effectiveness.

The SSE-CMM® also does not imply specific requirements for performing the generic practices. An organization is generally free to plan, track, define, control, and improve their processes in any way or sequence they choose. However, because some higher level generic practices are dependent on lower level generic practices, organizations are encouraged to work on the lower level generic practices before attempting to achieve higher levels.

#### 6.3.4 The Capability Levels

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, an organization that performs all but one of the Level 2 generic practices for some process area should receive a Level 1 rating. 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.

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.

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.

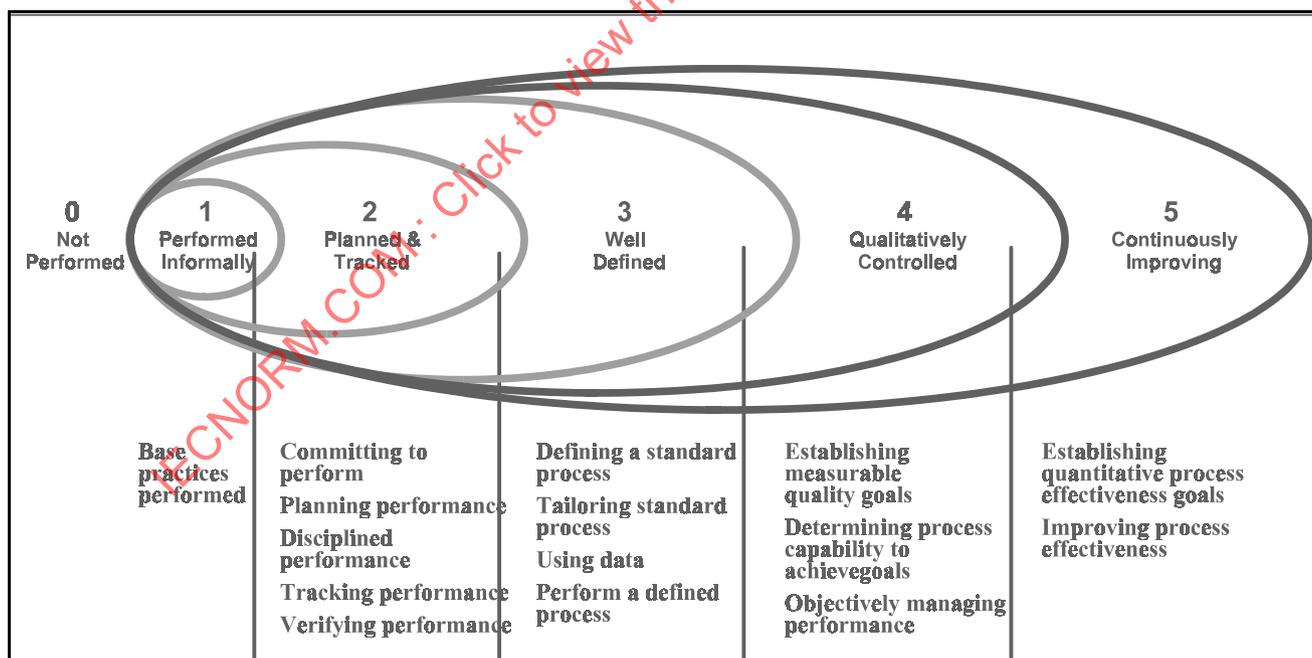


Figure 6 - Capability levels represent the maturity of security engineering organizations.

The SSE-CMM® contains five levels, which are depicted in Figure 6.

These five levels are informally described below, and detailed in Annex A.

- Level 1, "Performed Informally," focuses on whether an organization or project performs a process that incorporates the base practices. This level can be characterized by the statement, "you have to do it before you can manage it."
- Level 2, "Planned and Tracked," focuses on project-level definition, planning, and performance issues. This level can be characterized by the statement, "understand what's happening on the project before defining organization-wide processes."
- Level 3, "Well Defined," focuses on disciplined tailoring from defined processes at the organization level. This level can be characterized by the statement, "use the best of what you've learned from your projects to create organization-wide processes."
- Level 4, "Quantitatively Controlled," focuses on measurements being tied to the business goals of the organization. Although it is essential to begin collecting and using basic project measures early, measurement and use of data is not expected organization wide until the higher levels have been achieved. This level can be characterized by the statements, "you can't measure it until you know what 'it' is" and "managing with measurement is only meaningful when you're measuring the right things."
- Level 5, "Continuously Improving," gains leverage from all the management practice improvements seen in the earlier levels, then emphasizes the cultural shifts that will sustain the gains made. This level can be characterized by the statement, "a culture of continuous improvement requires a foundation of sound management practice, defined processes, and measurable goals."

**6.3.5 Capability Dimension / Measurement Framework Mapping**

The capability dimension of the SSE-CMM® and the measurement framework of ISO/IEC 15504-2 differ somewhat in terms of structure, but very little in terms of the detail and intent. In the case of the SSE-CMM® the capability dimension is organized into a number of "capability levels". Each capability level is made up of a number of "common features", which in turn are made up of one or more "generic practices"; see figure 10. In the case of ISO/IEC 15504-2 measurement framework, this is made up of a number of "levels" with each level consisting of a number of process attributes (PA)s. The table below sets out a mapping of the capability levels of the SSE-CMM® to the levels of 15504-2.

**Table 2 - Capability Dimension to Measurement Framework Mapping**

SSE-CMM® Capability Dimension	15504-2 Measurement Framework
<i>[Not explicitly defined in the SSE-CMM®, but implicitly inferred].</i>	Level 0: Incomplete process
Capability Level 1 - Performed Informally	Level 1: Performed process
Common Feature 1.1 Base Practices are performed	PA 1.1 Process performance attribute
Capability Level 2 - Planned and Tracked	Level 2: Managed process
Common Feature 2.1 Planning Performance Common Feature 2.4 Tracking Performance	PA 2.1 Performance management attribute
Common Feature 2.2 Disciplined Performance Common Feature 2.3 Verifying Performance	PA 2.2 Work product management attribute
Capability Level 3 - Well Defined	Level 3: Established process
Common Feature 3.1 Defining a Standard Process Common Feature 3.2 Performing the Defined Process	PA 3.1 Process definition attribute
<i>[Not specifically addressed at this point, however these aspects are addressed earlier in the following GPs].</i> GP 2.1.1 - Allocate Resources GP 2.1.2 - Assign Responsibilities GP 2.1.5 - Ensure Training	PA 3.2 Process resource attribute
Common Feature 3.3 Coordinate Security Practices	<i>[No direct equivalent].</i>

Capability Level 4 - Quantitatively Controlled	Level 4: Predictable process
Common Feature 4.1 Establishing Measurable Quality Goals	PA 4.1 Measurement attribute
Common Feature 4.2 Objectively Managing Performance	PA 4.2 Process control attribute
Capability Level 5 - Continuously Improving	Level 5: Optimizing process
Common Feature 5.1 Improving Organization Capability	PA 5.1 Continuously improving attribute
Common Feature 5.2 Improving Process Effectiveness	PA 5.2 Process change attribute

**6.3.6 Relationship to ISO/IEC CD 15288 - System Life Cycle Processes.**

this International Standard the SSE-CMM® has been developed outside the normal ISO/IEC environment. This means that some differences in the use of terminology and detail exist between ISO/IEC 21827 and ISO/IEC 15288. In addition, ISO/IEC 21827 is targeted at a different domain and discipline, systems security engineering, which inevitably, gives rise to some differences. These differences are minor and are note where applicable. However, the underlying concepts and approaches used by both ISO/IEC 21827 and ISO/IEC 15288 are very similar.

Some examples of relationships include:

- ISO/IEC 21827 Process Areas relate directly to ISO/IEC 15288 Processes;
- ISO/IEC 21827 Base Practices relate directly to ISO/IEC 15288 Activities; and
- ISO/IEC 21827 Work Products relate directly to ISO/IEC 15288 Outcomes; and
- ISO/IEC 21827 Process Descriptions are identical ISO/IEC 15288 process descriptions.

Table 3, below, maps the major relationships of the Process Areas of ISO/IEC 21827 to the processes of ISO/IEC 15288.

Note 1: A row containing multiple “x” indicates that the particular process of ISO/IEC CD 15288 is covered in more than one process area of ISO/IEC PAS DIS 21827.

Note 2: A column containing multiple “x” indicates that the particular process area of ISO/IEC PAS DIS 21827 is covered in more than one process of ISO/IEC CD 15288.

Table 3 - 21827 Process Areas to 15288 Processes Relationship

15288 Processes	21827 Process areas																				Rmk		
	PA01	PA02	PA03	PA04	PA05	PA06	PA07	PA08	PA09	PA10	PA11	PA12	PA13	PA14	PA15	PA16	PA17	PA18	PA19	PA20		PA21	PA22
Acquisition																						X	
Supply Environment Mgt	X																					X	
Investment Mgt																							NRE
System L-C Mgt																							
Resource Mgt																							
Project Planning																							
Project Assessment																							
Project Control																							
Decision Making																							
Risk Mgt																							
Configuration Mgt																							
Information Mgt																							
Stakeholder																							
Requ Def.																							
Requirements Analysis																							
Architecture Design																							
Implementation																							NRE
Integration																							NRE
Verification																							
Transition																							
Validation																							
Operation																							
Maintenance																							
Disposal																							
Rmks																							
Legend:																							

IECNORM.COM : Click to view the full PDF of ISO/IEC 21827:2002



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 8. The summary description contains a brief overview of the purpose of the process area. Each process area is decomposed into a set of base practices. The base practices 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 process area summary. Goals identify the desired end result of implementing the process area.

PA01 - Process Area Title (in verb-noun form)
Summary Description – An overview of the process area
Goals – A list indicating the desired results of implementing this process area
Base Practices List – A list showing the number and name of each base practice
Process Area Notes – Any other notes about this process area
BP.01.01 - Base Practice Title (in verb-noun form)
Descriptive Name – A sentence describing the base practice
Description – An overview of this base practice
Example Work Products – A list of examples illustrating some possible output
Notes – Any other notes about this base practice
BP.01.02 . . .

Figure 9 - Process Area Format

## 7.1 PA01 - Administer Security Controls

### 7.1.1 Process Area

#### 7.1.1.1 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.

#### 7.1.1.2 Goals

- Security controls are properly configured and used.

#### 7.1.1.3 Base Practice List

BP.01.01	Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.
BP.01.02	Manage the configuration of system security controls.
BP.01.03	Manage security awareness, training, and education programs for all users and administrators.
BP.01.04	Manage periodic maintenance and administration of security services and control mechanisms.

#### 7.1.1.4 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.

### 7.1.2 BP.01.01 - Establish Security Responsibilities

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

### 7.1.2.1 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.

### 7.1.2.2 Example Work Products

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

### 7.1.2.3 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.

## 7.1.3 BP.01.02 - Manage Security Configuration

Manage the configuration of system security controls.

### 7.1.3.1 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.

### 7.1.3.2 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 - a database describing 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 - a database tracking software updates which 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.
- 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.

### 7.1.3.3 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.

### 7.1.4 BP.01.03 - Manage Security Awareness, Training, and Education Programs

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

#### 7.1.4.1 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.

#### 7.1.4.2 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.

#### 7.1.4.3 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.

### 7.1.5 BP.01.04 - Manage Security Services and Control Mechanisms

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

### 7.1.5.1 Description

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

### 7.1.5.2 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.

### 7.1.5.3 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 analysing 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, a subset of 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.

## 7.2 PA02 - Assess Impact

### 7.2.1 Process Area

#### 7.2.1.1 Summary Description

The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible, such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.

### 7.2.1.2 Goals

- The security impacts of risks to the system are identified and characterized.

### 7.2.1.3 Base Practice List

BP.02.01	Identify, analyse, and prioritize operational, business, or mission capabilities leveraged by the system.
BP.02.02	Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system.
BP.02.03	Select the impact metric to be used for this assessment,
BP.02.04	Identify the relationship between the selected metrics for this assessment and metric conversion factors if required,
BP.02.05	Identify and characterize impacts.
BP.02.06	Monitor ongoing changes in the impacts.

### 7.2.1.4 Process Area Notes

Impact is the consequence of an unwanted incident, caused either deliberately or accidentally, which affects the assets. The consequences could be the destruction of certain assets, damage to the IT system, and loss of confidentiality, integrity, availability, accountability, authenticity or reliability. Possible indirect consequences include financial losses, and the loss of market share or company image. The measurement of impacts permits a balance to be made between the results of an unwanted incident and the cost of the safeguards to protect against the unwanted incident. The frequency of occurrence of an unwanted incident needs to be taken into account. This is particularly important when the amount of harm caused by each occurrence is low but where the aggregate effect of many incidents over time may be harmful. The assessment of impacts is an important element in the assessment of risks and the selection of safeguards.

The impact information produced by this process area is intended for use in PA03, along with the threat information from PA04 and vulnerability information from PA05. While the activities involved with gathering threat, vulnerability, and impact information have been grouped into separate process areas, they are interdependent. The goal is to find combinations of threat, vulnerability, and impact that are deemed sufficiently risky to justify action. Therefore, the search for impacts should be guided to a certain extent, by the existence of corresponding threats and vulnerabilities.

Since impacts are subject to change, they must be periodically monitored to ensure that the understanding generated by this process area is maintained at all times.

## 7.2.2 BP.02.01 - Prioritize Capabilities

Identify, analyse, and prioritize operational, business, or mission capabilities leveraged by the system.

### 7.2.2.1 Description

Identify, analyse, and prioritize operational, business, or mission directives. The influence of the business strategies should also be considered. These will influence and moderate the impacts to which the organization may be subjected. This in turn is likely to influence the sequence in which risks are addressed in other base practices and process areas. It is therefore important to factor in these influences when the potential impacts are being examined. This base practice is related to the activities of PA01 Specify Security Needs.

### 7.2.2.2 Example Work Products

- system priority lists and impact modifiers
- system capability profile - describes the capabilities of a system and their importance to the objective of the system.

### 7.2.2.3 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 may also be 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. 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.

### 7.2.3 BP.02.02 - Identify System Assets

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

#### 7.2.3.1 Description

Identify system resources and data necessary to support the security objectives or the key 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.

#### 7.2.3.2 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

#### 7.2.3.3 Notes

Assets are broadly construed to include the people, environment, technology and infrastructure in a system. Assets also include data and resources. This includes not only information, but also systems (e.g., communication, data retrieval, applications, or printing resources). The importance of these assets can be interpreted as their significance to the value and criticality of the capabilities they support in the defined environment. 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.

### 7.2.4 BP.02.03 - Select Impact Metric(s)

Select the impact metric(s) to be used for this assessment.

#### 7.2.4.1 Description

A number of metrics can be used to measure the impact of an event. It is advantageous to predetermine which metrics will be used for the particular system under consideration.

#### 7.2.4.2 Example Work Products

- selected impact metrics.

#### 7.2.4.3 Notes

A limited set of consistent metrics minimizes the difficulty in dealing with divergent metrics. Quantitative and qualitative measurements of impact can be achieved in a number of ways, such as:

- establishing the financial cost;
- assigning an empirical scale of severity, e.g., 1 through 10; and
- the use of adjectives selected from a predefined list, e.g., low, medium, high.

### 7.2.5 BP.02.04 - Identify Metric Relationship

Identify the relationship between the selected metrics for this assessment and metric conversion factors if required.

### 7.2.5.1 Description

Some impacts may need to be assessed using different metrics. The relationship between different metrics needs to be established to ensure a consistent approach for all exposures throughout the impact assessment. In some cases it will be necessary to combine metrics to be able to produce a single consolidated result. Thus an approach for consolidation needs to be established. This will usually vary on a system to system basis. When qualitative metrics are in use, rules also need to be established to guide the combination of qualitative factors during the consolidation phase.

### 7.2.5.2 Example Work Products

- impact metric relationships lists - describes the relationships between the metrics;
- impact metric combination rules - describes the rules for combining impact metrics.

### 7.2.5.3 Notes

As an example if the exposure was to a meteor destroying a house, one potential impact might be the cost to rebuild the house, 100,000 US dollars. Another impact might be the loss of shelter until the house can be rebuilt, 6 months. These two impacts can be combined if the cost of shelter per month is established, 250 US dollars per month. The total impact for this exposure would then be 101,500 US dollars.

## 7.2.6 BP.02.05 - Identify and Characterize Impacts

Identify and characterize the unwanted impacts of unwanted incidents with either multiple metrics or consolidated metrics as appropriate.

### 7.2.6.1 Description

Starting with the assets and capabilities identified in BP.02.01 and BP.02.02, identify the consequences that would cause harm. For each asset, these might include corruption, disclosure, obstruction, or disappearance. Unwanted impacts to capabilities might include interruption, delay, or weakening.

Once a relatively complete list has been created, the impacts can be characterized using the metrics identified in BP.02.03 and BP.02.04. This step may require some research into actuarial tables, almanacs, or other sources. The uncertainty in the metrics should also be captured and associated with each impact.

### 7.2.6.2 Example Work Products

- exposure impact lists - a list of potential impacts and the associated metrics.

### 7.2.6.3 Notes

The impact assessment is performed based on the impact metrics determined in BP.02.03 and the impacts are combined based on the rules established in BP.02.04. In most cases there will be some uncertainty associated with the metrics and likelihood that a specific impact will occur within the specified environment. It is generally more effective to keep the factors of uncertainty separate so that when actions are taken to refine the working data it can be seen whether the refinement is a result to data itself or the uncertainty associated with the data.

## 7.2.7 BP.02.06 - Monitor Impacts

Monitor ongoing changes in the Impacts.

### 7.2.7.1 Description

The impacts applicable to any location and situation are dynamic. New impacts can become relevant. It is therefore important to monitor both existing impacts and to check for the potential for new impacts on a regular basis. This base practice is closely linked to the generalized monitoring activity in BP.07.02.

### 7.2.7.2 Example Work Products

- impact monitoring reports - describes the results of monitoring impacts;
- impact change reports - describes changes to impacts.

### 7.2.7.3 Notes

Because impacts can change, the impact assessment activity can be iterative and can be conducted multiple times in the defined environments. However, impact assessment repetition should not supplant impact monitoring.

## 7.3 PA03 - Assess Security Risk

### 7.3.1 Process Area

#### 7.3.1.1 Summary Description

The purpose of Assess Security Risk is to identify the security risks involved with relying on a system in a defined environment. This process area focuses on ascertaining these risks based on an established understanding of how capabilities and assets are vulnerable to threats. Specifically, this activity involves identifying and assessing the likelihood of the occurrence of exposures. "Exposure" refers to a combination of a threat, vulnerability, and impact that could cause significant harm. 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.

#### 7.3.1.2 Goals

- An understanding of the security risk associated with operating the system within a defined environment is achieved;
- Risks are prioritized according to a defined methodology.

#### 7.3.1.3 Base Practice List

BP.03.01	Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analysed, assessed, and compared.
BP.03.02	Identify threat/vulnerability/impact triples (exposures),
BP.03.03	Assess the risk associated with the occurrence of an exposure.
BP.03.04	Assess the total uncertainty associated with the risk for the exposure.
BP.03.05	Order risks by priority.
BP.03.06	Monitor ongoing changes in the risk spectrum and changes to their characteristics.

#### 7.3.1.4 Process Area Notes

Security risk is the likelihood that the impact of an unwanted incident will be realized. While related to project risks involving cost and schedule, security risk deals specifically with protection against impacts to the assets and capabilities of a system.

Risk estimates always include 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 risk information produced by this process area depends on the threat information from PA04, vulnerability information from PA05, and impact information from PA02. While the activities involved with gathering threat, vulnerability, and impact information have been grouped into separate process areas, they are interdependent. The goal is to find combinations of threat, vulnerability, and impact that are deemed sufficiently risky to justify action. This

information forms the basis for the definition of security need in PA01 and the security input provided by PA02.

Since risk environments are subject to change, they must be periodically monitored to ensure that the understanding of risk generated by this process area is maintained at all times.

### 7.3.2 BP.03.01 - Select Risk Analysis Method

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

#### 7.3.2.1 Description

This base practice consists of defining the method for identifying security risks for the system in a defined environment in a way that permits them to be analysed, 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.

#### 7.3.2.2 Example Work Products

- risk assessment method - describes the approach for identifying and characterizing risks;
- risk assessment formats - describes the format in which risks will be documented and tracked, including a description, significance, and dependencies.

#### 7.3.2.3 Notes

Method can be an existing one, tailored one, or one specific to the operational aspects and defined environment for the system. The methodology used for the risk assessment should interface with the methodologies selected for the threat, vulnerability, and impact assessments.

### 7.3.3 BP.03.02 - Exposure Identification

Identify threat/vulnerability/impact triples (exposures).

#### 7.3.3.1 Description

The purpose of identifying the exposures is to recognize which of the threats and vulnerabilities are of concern and to identify the impact of an occurrence of the threat and vulnerability. These are the exposures that will need to be considered in the selection of safeguards to protect the system.

#### 7.3.3.2 Example Work Products

- system exposure lists - describes the exposures of the system.

#### 7.3.3.3 Notes

This base practice depends on the outputs of the threat, vulnerability, and risk process areas.

### 7.3.4 BP.03.03 - Assess Exposure Risk

Assess the risk associated with each exposure.

#### 7.3.4.1 Description

Identify the likelihood of the occurrence of an exposure.

#### 7.3.4.2 Example Work Products

- exposure risk list - a list of the calculated risks;
- exposure priority table - a prioritized table of the calculated risks.

### 7.3.4.3 Notes

The likelihood of an exposure is a combination of the likelihood of the exposure, which results from the likelihood of the threat and the likelihood of the vulnerability. In many cases the likelihood of a specific or generalized magnitude or severity of impact must also be factored in. In all cases there will be uncertainty associated with metrics. It is more effective to keep the factors of uncertainty separate so that when actions are taken to refine the working data it can be seen whether the refinement is a result of the data or the uncertainty associated with the data. This can often impact the strategies adopted to address the risks. This base practice makes use of the likelihood data gathered in BP.04.05 "Assess the likelihood of an occurrence of a threat event," BP.05.03 "Gather data related to the properties of the vulnerabilities," and BP.02.05 Assess impact of the realization of an exposure with either multiple metrics or consolidated metrics as appropriate.

### 7.3.5 BP.03.04 - Assess Total Uncertainty

Assess the total uncertainty associated with the risk for the exposure.

#### 7.3.5.1 Description

Each risk will have uncertainty associated with it. The total risk uncertainty is a cumulation of the uncertainties that have been identified for the threats, vulnerabilities, and impacts and their characteristics in BP.04.05 "Assess the likelihood of an occurrence of a threat event;" BP.05.03, Gather data related to the properties of the vulnerabilities; and BP.02.05, Assess impact of the realization of an exposure. This base practice is closely associated with the activities of PA06 Build Assurance Argument as assurance can be used to modify, and in some cases reduce uncertainty.

#### 7.3.5.2 Example Work Products

- exposure risk with associated uncertainty - a list of risks showing the measure of risk along with a measure of the uncertainty.

#### 7.3.5.3 Notes

If uncertainty is not kept separate from the likelihood of an occurrence of an exposure then safeguards may well be implemented that will not achieve the benefit perceived or risk may be mitigated when in fact there was not need to do so.

### 7.3.6 BP.03.05 - Prioritize Risks

Order risks by priority.

#### 7.3.6.1 Description

The risks that have been identified should be ordered based on the organization priorities, likelihood of occurrence, uncertainty associated with them and funds available. A risk can be mitigated, avoided, transferred or accepted. Combinations of these can also be used. The mitigation can address the threat, vulnerability, impact, or the risk itself. Actions should be selected with due regard to the stakeholders needs as identified in PA01 Specify Security Needs, business priorities, and the overall system architecture.

#### 7.3.6.2 Example Work Products

- risk priority lists - a list prioritizing the risks;
- safeguard requirement lists - lists of potential safeguards that can help mitigate the risks;
- rationale for prioritization - a description of the prioritization scheme.

#### 7.3.6.3 Notes

This step can be highly complex and often requires multiple iteration. Safeguards may address multiple risks, or multiple threats, vulnerabilities and impacts. This aspect can have the effect of changing the effective ordering of the risks to be addressed. Therefore, this process area is closely related to PA01 Specify Security Needs and PA02 Provide Security Input.

### 7.3.7 BP.03.06 - Monitor Risks and Their Characteristics

Monitor ongoing changes in the risk spectrum and changes to their characteristics.

#### 7.3.7.1 Description

The risk spectrum applicable to any location and situation is dynamic. New risks can become relevant and the characteristics of existing risks can change. It is therefore important to monitor both existing risks and their characteristics, and to check for new risks on a regular basis. This base practice is closely linked to the generalized monitoring activity in BP.07.02 Monitor changes in threats, vulnerabilities, impacts, risks and the environment.

#### 7.3.7.2 Example Work Products

- risk monitoring reports - reports describing the current risk spectrum;
- risk change reports - describes the operational capabilities of a system and their importance to the objective of the system.

#### 7.3.7.3 Notes

Because risks can change, the risk assessment activity can be conducted multiple times in the defined environments. However, risk assessment repetition should not supplant risk monitoring.

## 7.4 PA04 - Assess Threat

### 7.4.1 Process Area

#### 7.4.1.1 Summary Description

The purpose of the Assess Threat process area is to identify security threats and their properties and characteristics.

#### 7.4.1.2 Goals

- Threats to the security of the system are identified and characterized.

#### 7.4.1.3 Base Practice List

BP.04.01	Identify applicable threats arising from a natural source.
BP.04.02	Identify applicable threats arising from man-made sources, either accidental or deliberate.
BP.04.03	Identify appropriate units of measure, and applicable ranges, in a specified environment.
BP.04.04	Assess capability and motivation of threat agent for threats arising from man-made sources.
BP.04.05	Assess the likelihood of an occurrence of a threat event.
BP.04.06	Monitor ongoing changes in the threat spectrum and changes to their characteristics.

#### 7.4.1.4 Process Area Notes

Many approaches and methodologies can be used to perform a threat assessment. An important consideration for determining which methodology to use is how it will interface and work with the methodologies used in other parts of the chosen risk assessment process.

The threat information produced by this process area is intended for use in PA03, along with the vulnerability information from PA05 and impact information from PA02. While the activities involved with gathering threat, vulnerability, and impact information have been grouped into separate process areas, they are interdependent. The goal is to find combinations of threat, vulnerability, and impact that are deemed sufficiently risky to justify action. Therefore, the search for threats should be guided to a certain extent, by the existence of corresponding vulnerabilities and impacts.

Since threats are subject to change, they must be periodically monitored to ensure that the understanding generated by this process area is maintained at all times.

#### **7.4.2 BP.04.01 - Identify Natural Threats**

Identify applicable threats arising from a natural source.

##### **7.4.2.1 Description**

Threats arising from natural sources include earthquakes, tsunamis, and tornadoes. However, not all natural based threats can occur in all locations. For example it is not possible for a tsunami to occur in the centre of a large continent. Thus it is important to identify which natural based threats can occur in a specific location.

##### **7.4.2.2 Example Work Products**

- applicable natural threat tables - tables documenting the character and likelihood of natural threats.

##### **7.4.2.3 Notes**

Much of the information required for this assessment can be obtained from actuarial lists and natural phenomena occurrence databases. While this information is valuable, it should be used with caution as it may be highly generalized and therefore may need to be interpreted to address the specific environment.

#### **7.4.3 BP.04.02 - Identify Man-made Threats**

Identify applicable threats arising from man-made sources, either accidental or deliberate.

##### **7.4.3.1 Description**

Threats arising from man-made sources require a somewhat different type of approach. There are basically two types of man-made threats: those that arise from accidental sources and those that result from a deliberate act. Some man-made threats may not be applicable in the target environment. These should be eliminated from further considerations in the analysis.

##### **7.4.3.2 Example Work Products**

- threat scenario descriptions - descriptions of how the threat works;
- threat severity estimates - measurements of likelihood associated with a threat.

##### **7.4.3.3 Notes**

In some cases, to aid in the understanding of a deliberate threat it can be helpful to develop a scenario describing how the threat might occur. Use of generic man made threat databases should be assessed for completeness and relevancy.

#### **7.4.4 BP.04.03 - Identify Threat Units of Measure**

Identify appropriate units of measure, and applicable ranges, in a specified environment.

##### **7.4.4.1 Description**

The majority of natural threats and many man-made threats have units of measure associated with them. An example is the Richter scale for earthquakes. In most cases the total range of the unit of measure will not be applicable in a particular location. It is therefore appropriate to establish the maximum, and in some cases the minimum, occurrence of an event that can occur in the particular location under consideration.

##### **7.4.4.2 Example Work Products**

- threat table with associated units of measure and location ranges.

### 7.4.4.3 Notes

In cases where a unit of measure for a particular threat does not exist an acceptable unit of measure should be created that is specific to the location. The associated range, if applicable, and the unit of measure should be described in testable terms.

### 7.4.5 BP.04.04 - Assess Threat Agent Capability

Assess capability and motivation of threat agent for threats arising from man-made sources.

#### 7.4.5.1 Description

This process area focuses on the determination of a potential human adversary's ability and capability of executing a successful attack against the system. Ability addresses the adversaries knowledge of attacks (e.g. do they have the training / knowledge). Capability is a measure of the likelihood that an able adversary can actually execute the attack (e.g. do they have the resources).

#### 7.4.5.2 Example Work Products

- threat agent descriptions - capability assessments and descriptions.

#### 7.4.5.3 Notes

Deliberate man-made threats are to a large extent dependent upon the capability of the threat agent and the resources that the threat agent has at their disposal. Thus a relatively inexperienced hacker who has access to the hacking tools of much more experienced and capable hackers, is a much more dangerous threat, but not as dangerous as the experienced hacker themselves. However, the inexperienced hacker may well cause unintended damage which the experienced hacker is less likely to do. In addition to the agent capability, an assessment of the resources that the agent has available should be considered along with their motivation for performing the act which may be affected by the agent's likely assessment of the attractiveness of the target (asset).

A threat agent may use multiple attacks in sequence or concurrently to achieve the desired goal. The effect of multiple attacks occurring in sequence or concurrently needs to be considered. The development of scenarios can assist in performing this task.

### 7.4.6 BP.04.05 - Assess Threat Likelihood

Assess the likelihood of an occurrence of a threat event.

#### 7.4.6.1 Description

Assess how likely a threat event is to occur. Many factors need to be considered in making this assessment ranging from the chance occurrence of a natural event to the deliberate or accidental act of an individual. Many of the factors to be considered do not lend themselves to calculation or measurement. A consistent metric for reporting is desirable.

#### 7.4.6.2 Example Work Products

- threat event likelihood assessment - report describing the likelihood of threats.

#### 7.4.6.3 Notes

This is a complicated probability calculation as, many of the factors involve varying probabilities. Associated with any estimate of likelihood is a factor of uncertainty as to the accuracy and validity of that assessment. The uncertainty of the assessed likelihood should be reported separately to reduce potential confusion. In all cases there will be uncertainty associated with the metrics and likelihoods. It is normally more effective to keep the factors of uncertainty, which is also a compound expression, separate so that when actions are taken to refine the working data it can be seen whether the refinement is to the data itself or to the uncertainty associated with the data.

## 7.4.7 BP.04.06 - Monitor Threats and Their Characteristics

Monitor ongoing changes in the threat spectrum and changes to their characteristics.

### 7.4.7.1 Description

The threat spectrum applicable to any location and situation is dynamic. New threats can become relevant and the characteristics of existing threats can change. It is therefore important to monitor both existing threats and their characteristics, and to check for new threats on a regular basis. This base practice is closely linked to the generalized monitoring activity in BP.07.02 Monitor changes in threats, vulnerabilities, impacts, risks and the environment.

### 7.4.7.2 Example Work Products

- threat monitoring reports - documents describing the results of the threat monitoring effort;
- threat change reports - documents describing changes in the threat spectrum.

### 7.4.7.3 Notes

Because threats can change, the threat assessment activity can be conducted multiple times in the defined environments. However, threat assessment repetition does not supplant threat monitoring.

## 7.5 PA05 - Assess Vulnerability

### 7.5.1 Process Area

#### 7.5.1.1 Summary Description

The purpose of Assess Vulnerability is to identify and characterize system security vulnerabilities. This process area includes analysing system assets, defining specific 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, "vulnerability" refers to an aspect of a system that can be exploited for purposes other than those originally intended, weaknesses, security holes, or implementation flaws within a system that are likely to be attacked by a threat. These vulnerabilities are independent of any particular threat instance or attack. 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.

#### 7.5.1.2 Goals

- An understanding of system security vulnerabilities within a defined environment is achieved.

#### 7.5.1.3 Base Practice List

- |          |   |
|----------|---|
| BP.05.01 | Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized.      |
| BP.05.02 | Identify system security vulnerabilities.   |
| BP.05.03 | Gather data related to the properties of the vulnerabilities.   |
| BP.05.04 | Assess the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations of specific vulnerabilities. |
| BP.05.05 | Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics.   |

#### 7.5.1.4 Process Area Notes

The analyses and practices associated with this process area are often "paper-studies". Discovery of system vulnerabilities by active tools and techniques is another method that supplements but does not replace other vulnerability analysis techniques. These active techniques may be viewed as a specialized form of vulnerability analysis. 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. Active vulnerability analysis is needed in some cases to validate the security posture of a system and to increase the perception and understanding

of existing security vulnerabilities. Active vulnerability analysis, 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.

The vulnerability information produced by this process area is intended for use in PA03, along with the threat information from PA04 and impact information from PA02. While the activities involved with gathering threat, vulnerability, and impact information have been grouped into separate process areas, they are interdependent. The goal is to find combinations of threat, vulnerability, and impact that are deemed sufficiently risky to justify action. Therefore, the search for vulnerabilities should be guided to a certain extent, by the existence of corresponding threats and impacts.

Since vulnerabilities are subject to change, they must be periodically monitored to ensure that the understanding generated by this process area is maintained at all times.

## 7.5.2 BP.05.01 - Select Vulnerability Analysis Method

Select the methods, techniques, and criteria by which system security vulnerabilities in a defined environment are identified and characterized.

### 7.5.2.1 Description

This base practice consists of defining the method for establishing security vulnerabilities for the system in a way that permits them to be identified and characterized. This may include a scheme for categorizing and prioritizing the vulnerabilities based on threats and their likelihood, operational functions, security requirements, or other areas of concern when provided. Identifying the depth and breadth of the analysis allows the security engineers and the customer to determine target systems to be part of the exercise and its comprehensiveness. Analysis should be performed within the framework of a known and recorded configuration during a prearranged and specified time period. The methodology for the analysis should include expected results. Specific objectives for the analysis should be clearly stated.

### 7.5.2.2 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;
- 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.

### 7.5.2.3 Notes

The vulnerability analysis method can be an existing, tailored, or one specific to the operational aspects and defined environment for the system. It often is based on or complements the risk analysis methodology selected in PA03 Assess Security Risk. Note that understandings about threats, capabilities, and value may not be provided, in which case the methodology must either narrow its scope or adopt a set of suitable assumptions.

The method used to analyse the vulnerabilities may be qualitative or quantitative. Often, analysis of vulnerabilities includes a reflection of likelihood. Attack results can be conveyed in written report but attacks may also be demonstrated in a presentation.

At least two fundamentally different approaches exist for the identification of vulnerabilities. These two approaches are characterized as analysis based approaches or testing based approaches. Testing based approaches are good for identifying vulnerabilities that are present and for which there is a known threat which is included in the test sets.

Analysis based approaches are best for identifying new vulnerabilities and those that are not immediately available for exploitation, but which can be available once another problem has been exploited. Other options that should be considered when selecting a vulnerability methodology include qualitative or quantitative based approaches. The ability to control the completeness of the analysis or testing should also be considered.

### **7.5.3 BP.05.02 - Identify Vulnerabilities**

Identify system security vulnerabilities.

#### **7.5.3.1 Description**

System vulnerabilities may be found in both security and non-security related parts of the system. In many cases, non-security mechanisms that support security functions or work in concert with security mechanisms are found to have exploitable vulnerabilities. The methodology of attack scenarios as developed in BP.05.01 should be followed to the extent that vulnerabilities are validated. All system vulnerabilities discovered should be recorded.

#### **7.5.3.2 Example Work Products**

- vulnerability list describing the vulnerability of the system to various attacks;
- penetration profile includes results of the attack testing (e.g., vulnerabilities).

#### **7.5.3.3 Notes**

In this practice, vulnerabilities are seen as inherent to the system without consideration of the likelihood of any threats. The ordering of such vulnerabilities may be prioritized in accordance with threat analysis. Attacks that are not reproducible make the task of developing countermeasures difficult.

Vulnerabilities are identified in part based on prioritized functions PA03 Assess Security Risk, and the business priorities and objectives identified in PA01 Specific Security Needs. In addition the assets considered in PA02 need to be taken into account.

### **7.5.4 BP.05.03 - Gather Vulnerability Data**

Gather data related to the properties of the vulnerabilities.

#### **7.5.4.1 Description**

Vulnerabilities have properties associated with them. The intent of this base practice is to gather data associated with those properties. In some cases a vulnerability may have a unit of measure similar to those associated with threats, see BP.04.03 Identify Threat Unit of Measure. The ease with which the vulnerability can be exploited and the likelihood that the vulnerability exists should be identified and gathered.

#### **7.5.4.2 Example Work Products**

- vulnerability property tables - tables that document the characteristics of vulnerabilities of the product or system.

#### **7.5.4.3 Notes**

Much of the data gathered during this activity will be used later to perform PA03 Assess Security Risk. It is thus important that the data is gather and stored in a format that will be usable by PA03. In all cases there will be uncertainty associated with the metrics and likelihoods. It is normally more effective to keep the uncertainty separate so that when actions are taken to refine the working data it can be seen whether the refinement is a result of the data itself or the uncertainty associated with the data.

### **7.5.5 BP.05.04 - Synthesize System Vulnerability**

Assess the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations of specific vulnerabilities.

### 7.5.5.1 Description

Analyse which vulnerabilities or combination of vulnerabilities result in problems for the system. Analysis should identify additional characteristics of the vulnerability, such as the likelihood of vulnerability exploitation and the chance for successful exploitation. Recommendations for addressing the synthesized vulnerabilities may also be included in the results.

### 7.5.5.2 Example Work Products

- vulnerability assessment report - includes a quantitative or qualitative description of the vulnerabilities that result in a problem for the system, including the likelihood of attack, likelihood of success, and the impact of the attack;
- attack reports - documents the results and analysis of the results including vulnerabilities found, their potential for exploitation, and recommendations.

### 7.5.5.3 Notes

Results of an analysis and attack exercise need to be captured. Any vulnerabilities found and their potential for exploitation need to be identified and documented in sufficient detail to allow the customer to make decisions about countermeasures.

## 7.5.6 BP.05.05 - Monitor Vulnerabilities and Their Characteristics

Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics.

### 7.5.6.1 Description

The vulnerability spectrum applicable to any location and situation is dynamic. New vulnerabilities can become relevant and the characteristics of existing vulnerabilities can change. It is therefore important to monitor both existing vulnerabilities and their characteristics, and to check for new vulnerabilities on a regular basis. This base practice is closely linked to the generalized monitoring activity in BP.07.02 Monitor changes in threats, vulnerabilities, impacts, risks and the environment.

### 7.5.6.2 Example Work Products

- vulnerability monitoring reports - documents describing the results of the vulnerability monitoring effort;
- vulnerability change reports - documents describing new or changed vulnerabilities.

### 7.5.6.3 Notes

Because vulnerabilities can change, the vulnerability assessment activity can be conducted multiple times in the defined environments. However, this should vulnerability assessment repetition should not supplant vulnerability monitoring.

## 7.6 PA06 - Build Assurance Argument

### 7.6.1 Process Area

#### 7.6.1.1 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.

### 7.6.1.2 Goals

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

### 7.6.1.3 Base Practice List

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.

### 7.6.1.4 Process Area Notes

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

## 7.6.2 BP.06.01 - Identify Assurance Objectives

Identify the security assurance objectives.

### 7.6.2.1 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 those who will approve the operation of the system, if any.

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, 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, 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.

### 7.6.2.2 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.

### 7.6.2.3 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.

## 7.6.3 BP.06.02 - Define Assurance Strategy

Define a security assurance strategy to address all assurance objectives.

### 7.6.3.1 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 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.

### 7.6.3.2 Example Work Products

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

### 7.6.3.3 Notes

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

## 7.6.4 BP.06.03 - Control Assurance Evidence

Identify and control security assurance evidence.

### 7.6.4.1 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.

### 7.6.4.2 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.

### 7.6.4.3 Notes

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

## 7.6.5 BP.06.04 - Analyse Evidence

Perform analysis of security assurance evidence.

### 7.6.5.1 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 analysed 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.

### 7.6.5.2 Example Work Products

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

### 7.6.5.3 Notes

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

from a consolidation of other assurance.

### **7.6.6 BP.06.05 - Provide Assurance Argument**

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

#### **7.6.6.1 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.

#### **7.6.6.2 Example Work Products**

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

#### **7.6.6.3 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, and users.

## **7.7 PA07 - Coordinate Security**

### **7.7.1 Process Area**

#### **7.7.1.1 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 all project personnel 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.

#### **7.7.1.2 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.

#### **7.7.1.3 Base Practice List**

BP.07.01	Define security engineering coordination objectives and relationships.
BP.07.02	Identify coordination mechanisms for security engineering.
BP.07.03	Facilitate security engineering coordination.
BP.07.04	Use the identified mechanisms to coordinate decisions and recommendations related to security.

#### **7.7.1.4 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.

## 7.7.2 BP.07.01 - Define Coordination Objectives

Define security engineering coordination objectives and relationships.

### 7.7.2.1 Description

Many 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.

### 7.7.2.2 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.

### 7.7.2.3 Notes

Coordination objectives and relationships should be defined as early as possible in the project, to ensure that communication lines are well established. All 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.

## 7.7.3 BP.07.02 - Identify Coordination Mechanisms

Identify coordination mechanisms for security engineering.

### 7.7.3.1 Description

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

It is not uncommon to have multiple security personnel working on the same project. In these situations, all security engineers 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, all engineering teams must understand the security engineering efforts and engineering activities, 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.

### 7.7.3.2 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.

### 7.7.3.3 Notes

None.

#### 7.7.4 BP.07.03 - Facilitate Coordination

Facilitate security engineering coordination.

##### 7.7.4.1 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.

##### 7.7.4.2 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.

##### 7.7.4.3 Notes

None.

#### 7.7.5 BP.07.04 - Coordinate Security Decisions and Recommendations

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

##### 7.7.5.1 Description

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

##### 7.7.5.2 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.

##### 7.7.5.3 Notes

None.

#### 7.8 PA08 - Monitor Security Posture

##### 7.8.1 Process Area

##### 7.8.1.1 Summary Description

The purpose of Monitor 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.

##### 7.8.1.2 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.

### 7.8.1.3 Base Practice List

BP.08.01	Analyse event records to determine the cause of an event, how it proceeded, and likely future events.
BP.08.02	Monitor changes in threats, vulnerabilities, impacts, risks, and the environment.
BP.08.03	Identify security relevant incidents.
BP.08.04	Monitor the performance and functional effectiveness of security safeguards.
BP.08.05	Review the security posture of the system to identify necessary changes.
BP.08.06	Manage the response to security relevant incidents.
BP.08.07	Ensure that the artifacts related to security monitoring are suitably protected.

### 7.8.1.4 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 analysed 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.

## 7.8.2 BP.08.01 - Analyse Event Records

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

### 7.8.2.1 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.

### 7.8.2.2 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.

### 7.8.2.3 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 behaviour, 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.

### 7.8.3 BP.08.02 - Monitor Changes

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

#### 7.8.3.1 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 analysed to assess their significance with regard to the effectiveness of the security.

#### 7.8.3.2 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.

#### 7.8.3.3 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.

### 7.8.4 BP.08.03 - Identify Security Incidents

Identify security relevant incidents.

#### 7.8.4.1 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.

#### 7.8.4.2 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.

#### 7.8.4.3 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).

### **7.8.5 BP.08.04 - Monitor Security Safeguards**

Monitor the performance and functional effectiveness of security safeguards.

#### **7.8.5.1 Description**

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

#### **7.8.5.2 Example Work Products**

- periodic safeguard status - describes the state of the existing safeguards in order to detect possible mis-configuration 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.

#### **7.8.5.3 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.

### **7.8.6 BP.08.05 - Review Security Posture**

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

#### **7.8.6.1 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.

#### **7.8.6.2 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.

#### **7.8.6.3 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.

### **7.8.7 BP.08.06 - Manage Security Incident Response**

Manage the response to security relevant incidents.

#### **7.8.7.1 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.).

**7.8.7.2 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 results - 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 and is typically integrated with the test schedule;
- 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;
- 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.

**7.8.7.3 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.

**7.8.8 BP.08.07 - Protect Security Monitoring Artifacts**

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

**7.8.8.1 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.

**7.8.8.2 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;
- 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 - analyses randomly selected logs and determines whether they are complete, correct, and useful to ensure adequate monitoring of system security.

**7.8.8.3 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.

## 7.9 PA09 - Provide Security Input

### 7.9.1 Process Area

#### 7.9.1.1 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, analysed, provided to and coordinated with the appropriate organization members based on the security needs identified in PA01 Specify Security Needs.

#### 7.9.1.2 Goals

- All system issues are reviewed for security implications and are resolved in accordance with security goals;
- All members of the project team have an understanding of security so they can perform their functions;
- The solution reflects the security input provided.

#### 7.9.1.3 Base Practice List

BP.09.01	Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs.
BP.09.02	Determine the security constraints and considerations needed to make informed engineering choices.
BP.09.03	Identify alternative solutions to security related engineering problems.
BP.09.04	Analyse and prioritize engineering alternatives using security constraints and considerations.
BP.09.05	Provide security related guidance to the other engineering groups.
BP.09.06	Provide security related guidance to operational system users and administrators.

#### 7.9.1.4 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.

### 7.9.2 BP.09.01 - Understand Security Input Needs

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

#### 7.9.2.1 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.

### 7.9.2.2 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.

### 7.9.2.3 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.

## 7.9.3 BP.09.02 - Determine Security Constraints and Considerations

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

### 7.9.3.1 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).

### 7.9.3.2 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).

### 7.9.3.3 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.

## 7.9.4 BP.09.03 - Identify Security Alternatives

Identify solutions to security related engineering problems.

### 7.9.4.1 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, analysing, and recomposing security related requirements until effective alternative solutions are identified.

### 7.9.4.2 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.

#### 7.9.4.3 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.

#### 7.9.5 BP.09.04 - Analyse Security of Engineering Alternatives

Analyse and prioritize engineering alternatives using security constraints and considerations.

##### 7.9.5.1 Description

The purpose of this base practice is to analyse and prioritize engineering alternatives. Using the security constraints and considerations identified when determining security constraints and considerations (BP.02.02), security engineers can evaluate each engineering alternative and come up with a recommendation for the engineering group. The security engineers 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.

##### 7.9.5.2 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, focussing on areas where security requirements may have been reduced in order to meet other objectives (e.g., cost, functionality).

##### 7.9.5.3 Notes

None.

#### 7.9.6 BP.09.05 - Provide Security Engineering Guidance

Provide security related guidance to engineering groups.

##### 7.9.6.1 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.

##### 7.9.6.2 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;

## ISO/IEC 21827:2002(E)

- 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.

### 7.9.6.3 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.

### 7.9.7 BP.09.06 - Provide Operational Security Guidance

Provide security related guidance to operational system users and administrators.

#### 7.9.7.1 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.

#### 7.9.7.2 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.

#### 7.9.7.3 Notes

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

### 7.10 PA10 - Specify Security Needs

#### 7.10.1 Process Area

##### 7.10.1.1 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 that becomes the baseline for security within the system upon approval.

##### 7.10.1.2 Goals

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

### 7.10.1.3 Base Practice List

BP.10.01	Gain an understanding of the customer's security needs.
BP.10.02	Identify the laws, policies, standards, external influences and constraints that govern the system.
BP.10.03	Identify the purpose of the system in order to determine the security context.
BP.10.04	Capture a high-level security oriented view of the system operation.
BP.10.05	Capture high-level goals that define the security of the system.
BP.10.06	Define a consistent set of statements which define the protection to be implemented in the system.
BP.10.07	Obtain agreement that the specified security requirements match the customer's needs.

### 7.10.1.4 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.

### 7.10.2 BP.10.01 - Gain Understanding of Customer's Security Needs

Gain an understanding of the customer's security needs.

#### 7.10.2.1 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.

#### 7.10.2.2 Example Work Products

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

#### 7.10.2.3 Notes

The term customer may refer to a specific recipient of a product, system, or service, or may refer to a generalized recipient based upon market research or product targeting. Different groups of users may need to be identified and distinguished. For example, ordinary users may have different needs from administrators.

### 7.10.3 BP.10.02 - Identify Applicable Laws, Policies, And Constraints

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

#### 7.10.3.1 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.

#### 7.10.3.2 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.

### 7.10.3.3 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.

### 7.10.4 BP.10.03 - Identify System Security Context

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

#### 7.10.4.1 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.

#### 7.10.4.2 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].

#### 7.10.4.3 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.

### 7.10.5 BP.10.04 - Capture Security View of System Operation

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

#### 7.10.5.1 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.

#### 7.10.5.2 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.

### 7.10.5.3 Notes

None.

## 7.10.6 BP.10.05 - Capture Security High-Level Goals

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

### 7.10.6.1 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.

### 7.10.6.2 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.

### 7.10.6.3 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.

## 7.10.7 BP.10.06 - Define Security Related Requirements

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

### 7.10.7.1 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.

### 7.10.7.2 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 security needs to requirements to solutions (e.g., architecture, design, implementation) to tests and test results.

### 7.10.7.3 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.

### **7.10.8 BP.10.07 - Obtain Agreement On Security**

Obtain agreement that the specified security requirements match the customer's needs.

#### **7.10.8.1 Description**

The purpose of this base practice is to obtain concurrence between all applicable parties on the security requirements. In cases where a generic group is identified, rather than a specific customer, the requirements should satisfy the objectives set. The specified security requirements should be a complete and consistent reflection of governing policy, laws, and customer needs. Issues should be identified and reworked until concurrence is gained.

#### **7.10.8.2 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.

#### **7.10.8.3 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.

### **7.11 PA11 - Verify and Validate Security**

#### **7.11.1 Process Area**

##### **7.11.1.1 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.

##### **7.11.1.2 Goals**

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

##### **7.11.1.3 Base Practice List**

- |          |   |
|----------|---|
| BP.11.01 | Identify the solution to be verified and validated.   |
| BP.11.02 | Define the approach and level of rigour for verifying and validating each solution.   |
| BP.11.03 | Verify that the solution implements the requirements associated with the previous level of abstraction.   |
| BP.11.04 | 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.11.05 | Capture the verification and validation results for the other engineering groups.   |

##### **7.11.1.4 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.

### 7.11.2 BP.11.01 - Identify Verification and Validation Targets

Identify the solution to be verified and validated.

#### 7.11.2.1 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.

#### 7.11.2.2 Example Work Products

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

#### 7.11.2.3 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.

### 7.11.3 BP.11.02 - Define Verification and Validation Approach

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

#### 7.11.3.1 Description

The purpose of this base practice is to define the approach and level of rigour for verifying and validating each solution. Identifying the approach involves selecting how each requirement is verified and validated. The level of rigour 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.

#### 7.11.3.2 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 rigour (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.

#### 7.11.3.3 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.

### 7.11.4 BP.11.03 - Perform Verification

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

#### 7.11.4.1 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.

#### 7.11.4.2 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.

#### 7.11.4.3 Notes

None.

#### 7.11.5 BP.11.04 - 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.

##### 7.11.5.1 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.

##### 7.11.5.2 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.

##### 7.11.5.3 Notes

This practice is related to traceability.

#### 7.11.6 BP.11.05 - Provide Verification and Validation Results

Capture the verification and validation results for engineering groups.

##### 7.11.6.1 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.

##### 7.11.6.2 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.

##### 7.11.6.3 Notes

None.

## Annex A (normative)

### Generic Practices

#### A.1 General

This annex contains the generic practices, that is, the practices that apply to all processes. The generic practices 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. The generic practices are divided into the following capability levels, each of which has several common features:

- Capability Level 1 - Performed Informally;
- Capability Level 2 - Planned and Tracked;
- Capability Level 3 - Well Defined;
- Capability Level 4 - Quantitatively Controlled;
- Capability Level 5 - Continuously Improving.

The general format of the capability levels is shown in Figure 10. The summary description contains a brief overview of the purpose of the process area. Each level is decomposed into a set of common features that consist of a set of generic practices. Each generic practice is described in detail following the common feature summary.

Capability Level 1 - Capability Level Title Summary Description - An overview of the capability level Common Features List - A list showing the number and name of each common feature Common Feature 1.1 - Common Feature Title Summary Description - An overview of the capability level Generic Practices List - A list showing the number and name of each generic practice GP 1.1.1 - Generic Practice Title Description - An overview of this generic practice Notes - Any other notes about this generic practice Relationships - Any relationships with other parts of the model GP 1.1.2...
--

**Figure 10 - Capability Level Format**

#### A.2 Capability Level 1 - Performed Informally

##### A.2.1 Capability Level Common Features

###### A.2.1.1 Common Feature Generic Practices

###### A.2.1.1.1 Summary 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.

**A.2.1.1.2 Common Features List**

This capability level comprises the following common features:

- Common Feature 1.1 - Base Practices Are Performed.

**A.2.2 Common Feature 1.1 - Base Practices Are Performed**

**A.2.2.1 Common Feature Generic Practices**

**A.2.2.1.1 Summary Description**

The Generic Practices of this Common Feature simply ensure that the Base Practices of the Process Area are being performed in some manner. However, the consistency or performance and the quality of the work products produced are likely to be highly variable due to the paucity of controls in place.

**A.2.2.1.2 Generic Practices List**

This common feature comprises the following generic practices:

- GP 1.1.1 - Perform the Process

**A.2.2.2 GP 1.1.1 - Perform the Process**

**A.2.2.2.1 Description**

Perform a process that implements the base practices of the process area to provide work products and/or services to a customer.

**A.2.2.2.2 Notes**

This process may be termed the "informal process." The customer(s) of the process area may be internal or external to the organization.

**A.3 Capability Level 2 - Planned and Tracked**

**A.3.1 Capability Level Common Features**

**A.3.1.1 Common Feature Generic Practices**

**A.3.1.1.1 Summary 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 Level 1, Performed Informally, is that the performance of the process is planned and managed.

**A.3.1.1.2 Common Features List**

This capability level comprises the following common features:

- Common Feature 2.1 - Planning Performance;
- Common Feature 2.2 - Disciplined Performance;
- Common Feature 2.3 - Verifying Performance;
- Common Feature 2.4 - Tracking Performance.

**A.3.2 Common Feature 2.1 - Planning Performance**

### A.3.2.1 Common Feature Generic Practices

#### A.3.2.1.1 Summary Description

The Generic Practices of this Common Feature focus on the aspects of planning to perform the Process Area and its associated Base Practices. Thus the documentation of the process, provision of appropriate tools to perform the process, planning of the performance of the process, training in the performance of the process, allocation of resources to the process and the assignment of responsibility for the performance of the process are all addressed. These Generic Practices form an essential foundation for disciplined performance of the process.

#### A.3.2.1.2 Generic Practices List

This common feature comprises the following generic practices:

- GP 2.1.1 - Allocate Resources;
- GP 2.1.2 - Assign Responsibilities;
- GP 2.1.3 - Document the Process;
- GP 2.1.4 - Provide Tools;
- GP 2.1.5 - Ensure Training;
- GP 2.1.6 - Plan the Process.

#### A.3.2.2 GP 2.1.1 - Allocate Resources

##### A.3.2.2.1 Description

Allocate adequate resources (including people) for performing the process area.

##### A.3.2.2.2 Notes

None.

##### A.3.2.2.3 Relationships

Identification of critical resources is done in process area PA16 Plan Technical Effort.

#### A.3.2.3 GP 2.1.2 - Assign Responsibilities

##### A.3.2.3.1 Description

Assign responsibilities for developing the work products and/or providing the services of the process area.

##### A.3.2.3.2 Notes

None.

##### A.3.2.3.3 Relationships

This practice is particularly related to process area PA16 Plan Technical Effort.

#### A.3.2.4 GP 2.1.3 - Document the Process

##### A.3.2.4.1 Description

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

**A.3.2.4.2 Notes**

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 this model. 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.

**A.3.2.4.3 Relationships**

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).

This practice is related to process areas PA17 Define Organization's Security Engineering Process and PA18 Improve Organization's Security Engineering Processes.

**A.3.2.5 GP 2.1.4 - Provide Tools**

**A.3.2.5.1 Description**

Provide appropriate tools to support performance of the process area.

**A.3.2.5.2 Notes**

The tools required will vary dependent upon the process being performed. The individual(s) performing the process likely have a good understanding of the tools required to perform the process.

**A.3.2.5.3 Relationships**

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).

Tools are managed in PA20 Manage Security Engineering Support Environment.

**A.3.2.6 GP 2.1.5 - Ensure Training**

**A.3.2.6.1 Description**

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

**A.3.2.6.2 Notes**

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

**A.3.2.6.3 Relationships**

Training and training management is described in PA21 Provide Ongoing Skills and Knowledge.

**A.3.2.7 GP 2.1.6 - Plan the Process**

**A.3.2.7.1 Description**

Plan the performance of the process area.

**A.3.2.7.2 Notes**

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.

**A.3.2.7.3 Relationships**

Project planning is described in process area PA16 Plan Technical Effort.

**A.3.3 Common Feature 2.2 - Disciplined Performance****A.3.3.1 Common Feature Generic Practices****A.3.3.1.1 Summary Description**

The Generic Practices of this Common Feature focus on the amount of control exercised over the process. Thus the use of plans for the performance of the process, performing the process according to standards and procedures, and placing the work products produced by the process under configuration management are all addressed. These Generic Practices form an important foundation for being able to verify the performance of the process.

**A.3.3.1.2 Generic Practices List**

This common feature comprises the following generic practices:

- GP 2.2.1 - Use Plans, Standards, and Procedures;
- GP 2.2.2 - Do Configuration Management.

**A.3.3.2 GP 2.2.1 - Use Plans, Standards, and Procedures****A.3.3.2.1 Description**

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

**A.3.3.2.2 Notes**

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

**A.3.3.2.3 Relationships**

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.

**A.3.3.3 GP 2.2.2 - Do Configuration Management****A.3.3.3.1 Description**

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

**A.3.3.3.2 Notes**

None.

**A.3.3.3.3 Relationships**

The typical practices needed to support systems engineering in the configuration management discipline are described in process area PA13 Manage Configurations.

Where process area PA13 Manage Configurations focuses on the general practices of configuration management, this generic practice is focussed on the deployment of these practices in relation to the work products of the individual process area under investigation.

**A.3.4 Common Feature 2.3 - Verifying Performance**

**A.3.4.1 Common Feature Generic Practices**

**A.3.4.1.1 Summary Description**

The Generic Practices of this Common Feature focus on confirming that the process has been performed as intended. Thus verification that the process was performed in compliance with the applicable standards and procedures, and the auditing of the work products are addressed. These Generic Practices form an important foundation for the ability to track the performance of the process.

**A.3.4.1.2 Generic Practices List**

This common feature comprises the following generic practices:

- GP 2.3.1 - Verify Process Compliance;
- GP 2.3.2 - Audit Work Products.

**A.3.4.2 GP 2.3.1 - Verify Process Compliance**

**A.3.4.2.1 Description**

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

**A.3.4.2.2 Notes**

None.

**A.3.4.2.3 Relationships**

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

The quality management and/or assurance process is described in PA12 Ensure Quality.

**A.3.4.3 GP 2.3.2 - Audit Work Products**

**A.3.4.3.1 Description**

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

**A.3.4.3.2 Notes**

None.

**A.3.4.3.3 Relationships**

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

Product requirements are developed and managed in process area PA10 Specify Security Needs. Verification and validation is further addressed in PA11 Verify and Validate Security.

### A.3.5 Common Feature 2.4 - Tracking Performance

#### A.3.5.1 Common Feature Generic Practices

##### A.3.5.1.1 Summary Description

The Generic Practices of this Common Feature focus on the ability to control the progress of project performance. Thus tracking the performance of the process against a measurable plan, and taking corrective action when the performance of the process deviates significantly from that plan are addressed. These Generic Practices form an essential foundation to having the ability to achieve well-defined processes.

##### A.3.5.1.2 Generic Practices List

This common feature comprises the following generic practices:

- GP 2.4.1 - Track with Measurement;
- GP 2.4.2 - Take Corrective Action.

##### A.3.5.2 GP 2.4.1 - Track with Measurement

###### A.3.5.2.1 Description

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

###### A.3.5.2.2 Notes

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

###### A.3.5.2.3 Relationships

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.

Project tracking is described in process area PA13 Monitor and Control Technical Effort.

##### A.3.5.3 GP 2.4.2 - Take Corrective Action

###### A.3.5.3.1 Description

Take corrective action as appropriate when progress varies significantly from that planned.

###### A.3.5.3.2 Notes

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.

###### A.3.5.3.3 Relationships

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.

Project control is described in process area PA15 Monitor and Control Technical Effort.

## A.4 Capability Level 3 - Well Defined

#### A.4.1 Capability Level Common Features

##### A.4.1.1 Common Feature Generic Practices

###### A.4.1.1.1 Summary Description

Base practices are performed according to a well-defined process using approved, tailored versions of standard, documented processes. The primary distinction from Level 2, Planned and Tracked, is that the process is planned and managed using an organization-wide standard process.

###### A.4.1.1.2 Common Features List

This capability level comprises the following common features:

- Common Feature 3.1 - Defining a Standard Process;
- Common Feature 3.2 - Perform the Defined Process;
- Common Feature 3.3 - Coordinate Security Practices.

#### A.4.2 Common Feature 3.1 - Defining a Standard Process

##### A.4.2.1 Common Feature Generic Practices

###### A.4.2.1.1 Summary Description

The Generic Practices of this common feature focus on the institutionalization of a standard process for the organization. The origin or basis of the institutionalized process may be one or more similar processes used successfully on specific projects. An organization standard process is likely to need tailoring to specific situational usage so the development of tailoring needs is also considered. Thus documentation of a standard process for the organization, and tailoring of the standard process to specific uses are addressed. These Generic Processes form an essential foundation to the performance of defined processes.

###### A.4.2.1.2 Generic Practices List

This common feature comprises the following generic practices:

- GP 3.1.1 - Standardize the Process;
- GP 3.1.2 - Tailor the Standard Process.

##### A.4.2.2 GP 3.1.1 - Standardize the Process

###### A.4.2.2.1 Description

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

###### A.4.2.2.2 Notes

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."

**A.4.2.2.3 Relationships**

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.

The process for developing a process description is described in process area PA17 Define Organization's Security Engineering Process.

**A.4.2.3 GP 3.1.2 - Tailor the Standard Process****A.4.2.3.1 Description**

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

**A.4.2.3.2 Notes**

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.

**A.4.2.3.3 Relationships**

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.

Tailoring guidelines are defined in process area PA17 Define Organization's Security Engineering Process.

**A.4.3 Common Feature 3.2 - Perform the Defined Process****A.4.3.1 Common Feature Generic Practices****A.4.3.1.1 Summary Description**

The generic practices of this common feature focus on the repeatable performance of a well-defined process. Thus the use of the institutionalized process, the review of the results of the process, work products, for defects, and use of data on the performance and results of the process are addressed. These Generic Practices form an important foundation to the coordination of security practices.

**A.4.3.1.2 Generic Practices List**

This common feature comprises the following generic practices:

- GP 3.2.1 - Use a Well-Defined Process;
- GP 3.2.2 - Perform Defect Reviews;
- GP 3.2.3 - Use Well-Defined Data.

**A.4.3.2 GP 3.2.1 - Use a Well-Defined Process****A.4.3.2.1 Description**

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

**A.4.3.2.2 Notes**

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.

**A.4.3.2.3 Relationships**

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.

**A.4.3.3 GP 3.2.2 - Perform Defect Reviews**

**A.4.3.3.1 Description**

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

**A.4.3.3.2 Notes**

None.

**A.4.3.3.3 Relationships**

None.

**A.4.3.4 GP 3.2.3 - Use Well-Defined Data**

**A.4.3.4.1 Description**

Use data on performing the defined process to manage it.

**A.4.3.4.2 Notes**

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.

**A.4.3.4.3 Relationships**

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).

**A.4.4 Common Feature 3.3 - Coordinate Practices**

**A.4.4.1 Common Feature Generic Practices**

**A.4.4.1.1 Summary Description**

The generic practices of this common feature focus on the coordination of activities throughout the project and the organization. Many significant activities are performed by disparate groups within and project and by organization service groups on behalf of the project. A lack of coordination can cause delays or incomparable results. Thus the coordination of intra-group, inter-group, and external activities and addressed. These generic practices form an essential foundation to having the ability to quantitatively control processes.

**A.4.4.1.2 Generic Practices List**

This common feature comprises the following generic practices:

- GP 3.3.1 - Perform Intra-Group Coordination;
- GP 3.3.2 - Perform Inter-Group Coordination;
- GP 3.3.3 - Perform External Coordination.

**A.4.4.2 GP 3.3.1 - Perform Intra-Group Coordination**

**A.4.4.2.1 Description**

Coordinate communication within an engineering discipline.

**A.4.4.2.2 Notes**

This type of coordination addresses the need for an engineering discipline ensure that decisions with regard to technical issues (e.g. Access Controls, Security Testing) are arrived at through consensus. The commitments, expectations, and responsibilities of the appropriate engineers are documented and agreed upon among the those involved. Engineering issues are tracked and resolved.

**A.4.4.2.3 Relationships**

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

Coordination objectives and approaches are addressed in PA07 Coordinate Security.

**A.4.4.3 GP 3.3.2 - Perform Inter-Group Coordination****A.4.4.3.1 Description**

Coordinate communication among the various groups within the organization.

**A.4.4.3.2 Notes**

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

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. Engineering issues are tracked and resolved among all the affected engineering groups within a project / organization.

**A.4.4.3.3 Relationships**

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

Coordination objectives and approaches are addressed in PA07 Coordinate Security. Specific security engineering practices for ensuring other engineering groups are provided with timely and accurate input are addressed in PA09 Provide Security Input.

**A.4.4.3 GP 3.3.3 - Perform External Coordination****A.4.4.3.1 Description**

Coordinate communication with external groups.

**A.4.4.3.2 Notes**

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

A relationship between external groups (e.g., customer, systems security certifier, 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.

**A.4.4.3.3 Relationships**

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

Coordination objectives and approaches are addressed in PA07 Coordinate Security. Security needs of the customer are identified in PA10 Specify Security Needs. The customer's assurance needs are addressed in PA06 Build Assurance Argument.

**A.5 Capability Level 4 - Quantitatively Controlled**

**A.5.1 Capability Level Common Features**

**A.5.1.1 Common Feature Generic Practices**

**A.5.1.1.1 Summary Description**

Detailed measures of performance are collected and analysed. 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.

**A.5.1.1.2 Common Features List**

This capability level comprises the following common features:

- Common Feature 4.1 - Establishing Measurable Quality Goals;
- Common Feature 4.2 - Objectively Managing Performance.

**A.5.2 Common Feature 4.1 - Establishing Measurable Quality Goals**

**A.5.2.1 Common Feature Generic Practices**

**A.5.2.1.1 Summary Description**

The generic practices of this common feature focus on the establishment of measurable targets for the work products developed by the organization's processes. Thus the establishment of quality goals is addressed. These generic practices form an essential foundation to objectively managing the performance of a process.

**A.5.2.1.2 Generic Practices List**

This common feature comprises the following generic practices:

- GP 4.1.1 - Establish Quality Goals.

**A.5.2.2 GP 4.1.1 - Establish Quality Goals**

**A.5.2.2.1 Description**

Establish measurable quality goals for the work products of the organization's standard process family.

**A.5.2.2.2 Notes**

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.

**A.5.2.2.3 Relationships**

Relationship to other generic practices: Data gathered via defect reviews (3.2.2) are particularly important in setting goals for work product quality.

**A.5.3 Common Feature 4.2 - Objectively Managing Performance****A.5.3.1 Common Feature Generic Practices****A.5.3.1.1 Summary Description**

The generic practices of this common feature focus on determining a quantitative measure of process capability and making use of quantitative measures to manage the process. The determining the process capability quantitatively, and using the quantitative measures as a basis for corrective action are addressed. These generic practices form an essential foundation to having the ability to achieve continuous improvement.

**A.5.3.1.2 Generic Practices List**

This common feature comprises the following generic practices:

- GP 4.2.1 - Determine Process Capability;
- GP 4.2.2 - Use Process Capability.

**A.5.3.2 GP 4.2.1 - Determine Process Capability****A.5.3.2.1 Description**

Determine the process capability of the defined process quantitatively.

**A.5.3.2.2 Notes**

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.

**A.5.3.2.3 Relationships**

Relationship to other generic practices: The defined process is established through tailoring in 3.1.2 and performed in 3.2.1.

**A.5.3.3 GP 4.2.2 - Use Process Capability****A.5.3.3.1 Description**

Take corrective action as appropriate when the process is not performing within its process capability.

**A.5.3.3.2 Notes**

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.

### A.5.3.3.3 Relationships

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.

## A.6 Capability Level 5 - Continuously Improving

### A.6.1 Capability Level Common Features

#### A.6.1.1 Common Feature Generic Practices

##### A.6.1.1.1 Summary 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.

##### A.6.1.1.2 Common Features List

This capability level comprises the following common features:

- Common Feature 5.1 - Improving Organizational Capability;
- Common Feature 5.2 - Improving Process Effectiveness.

### A.6.2 Common Feature 5.1 - Improving Organizational Capability

#### A.6.2.1 Common Feature Generic Practices

##### A.6.2.1.1 Summary Description

The Generic Practices of this common feature focus on comparing the use of the standard process throughout the organization and making comparisons between those different uses. As the process is used opportunities are sought for enhancing the standard process, and defects produced are analysed to identify other potential enhancements to the standard process. Thus goals for process effectiveness are established, improvements to the standard process are identified, and are analysed for potential changes to the standard process. These generic practices form an essential foundation to improving process effectiveness.

##### A.6.2.1.2 Generic Practices List

This common feature comprises the following generic practices:

- GP 5.1.1 - Establish Process Effectiveness Goals;
- GP 5.1.2 - Continuously Improve the Standard Process.

#### A.6.2.2 GP 5.1.1 - Establish Process Effectiveness Goals

##### A.6.2.2.1 Description

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.

**A.6.2.2.2 Notes**

None.

**A.6.2.2.3 Relationships**

None.

**A.6.2.3 GP 5.1.2 - Continuously Improve the Standard Process****A.6.2.3.1 Description**

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

**A.6.2.3.2 Notes**

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.

**A.6.2.3.3 Relationships**

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

Organizational process improvement is managed in process area PA18 Improve Organization's Security Engineering Processes.

**A.6.3 Common Feature 5.2 - Improving Process Effectiveness****A.6.3.1 Common Feature Generic Practices****A.6.3.1.1 Summary Description**

The generic practices of this common feature focus making the standard process one that is in a continual state of controlled improvement. Thus eliminating the cause of defects produced by the standard process, and continuously improving the standard process are addressed.

**A.6.3.1.2 Generic Practices List**

This common feature comprises the following generic practices:

- GP 5.2.1 - Perform Causal Analysis;
- GP 5.2.2 - Eliminate Defect Causes;
- GP 5.2.3 - Continuously Improve the Defined Process.

**A.6.3.2 GP 5.2.1 - Perform Causal Analysis****A.6.3.2.1 Description**

Perform causal analysis of defects.

**A.6.3.2.2 Notes**

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.

**A.6.3.2.3 Relationships**

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

**A.6.3.3 GP 5.2.2 - Eliminate Defect Causes**

**A.6.3.3.1 Description**

Eliminate the causes of defects in the defined process selectively.

**A.6.3.3.2 Notes**

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

**A.6.3.3.3 Relationships**

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

**A.6.3.4 GP 5.2.3 - Continuously Improve the Defined Process**

**A.6.3.4.1 Description**

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

**A.6.3.4.2 Notes**

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.

**A.6.3.4.3 Relationships**

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

Product technology insertion is managed in PA19 Manage Security Product Line Evolution.

## Annex B (normative)

### Project and Organizational Base Practices

#### B.1 General

The SSE-CMM® includes the Project and Organization process areas adapted from the SE-CMM®. These process areas are an important part of the SSE-CMM® and for interpreting the generic practices.

Each process area includes a "security considerations" section that indicates some considerations for applying the process area in the context of security engineering. This section also references related SSE-CMM® process areas.

#### B.2 General Security Considerations

In addition to the specific considerations on the interpretation sheet for each process area, the following sections include general considerations with respect to security engineering for all of the Project and Organization process areas.

##### B.2.1 Project Risk vs. Security Risk

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

##### B.2.2 Applicability to Operational Phase

Although the wording of the Project and Organization process areas seem to imply applicability to only development aspects, the process areas apply equally to the operation and maintenance phase of a life cycle. The process areas will need to be interpreted for an assessment or improvement purposes based on the view of the process areas that are applicable to an organization. The few exceptions are noted in the security considerations area.

##### B.2.3 Security Engineering vs. Systems Engineering

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

##### B.2.4 Engineering Relationships

Systems engineering and security engineering relationships are indicated for each process area. Note there are many relationships between the various process areas (in these sections only the major relationships are identified).

#### B.3 PA12 - Ensure Quality

##### B.3.1 Process Area

### B.3.1.1 Security Considerations

PA06 Build Assurance Argument is related to ensure quality. Assurance can be considered a specific type of security related quality.

### B.3.1.2 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 if a process exists to continuously measure and improve quality. In addition, this process must be adhered to throughout the system life cycle. Key aspects of the process required to develop high-quality systems are measurement, analysis, and corrective action.

### B.3.1.3 Goals

- Process quality is defined and measured;
- Expected work product quality achieved.

### B.3.1.4 Base Practice List

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

- BP.12.01 Identify quality requirements for each work product.
- BP.12.02 Ensure the defined system engineering process is adhered to during the system life cycle.
- BP.12.03 Evaluate work product measures against the requirements for work product quality.
- BP.12.04 Measure the quality of the systems engineering process used by the project.
- BP.12.05 Analyse quality measurements to develop recommendations for quality improvement or corrective action as appropriate.
- BP.12.06 Obtain employee participation in identifying and reporting quality issues.
- BP.12.07 Initiate activities that address identified quality issues or quality improvement opportunities.
- BP.12.08 Establish a mechanism or a set of mechanisms to detect the need for corrective actions to processes or products.

### B.3.1.5 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. 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. 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 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. Higher than planned costs and delays in the schedule 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.

### B.3.2 BP.12.01 - Identify the requirements for work product quality.

Identify quality requirements for each work product.

**B.3.2.1 Description**

Different types of work products and different specific work products may have different quality requirements. These quality requirements should be identified when the work product is defined.

**B.3.2.2 Example Work Products**

- Work product quality requirements;
- Generic work product quality requirements lists.

**B.3.2.3 Notes**

None.

**B.3.3 BP.12.02 - Monitor Conformance to the Defined Process**

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

**B.3.3.1 Description**

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

**B.3.3.2 Example Work Products**

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

**B.3.3.3 Notes**

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

**B.3.4 BP.12.03 - Measure Quality of the Work Product**

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

**B.3.4.1 Description**

Measuring the characteristics of the work product, related to conformance with requirements and standards, correctness and timeliness, 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.

**B.3.4.2 Example Work Products**

- assessment of the quality of the product;
- product quality certification.

**B.3.4.3 Notes**

Example approaches to measurement of work product quality include:

## ISO/IEC 21827:2002(E)

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

### B.3.5 BP.12.04 - Measure Quality of the Process

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

#### B.3.5.1 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 identified early, before the final work product is produced and found to not meet requirements. Thus, having a process that is measured may lead to less waste and higher productivity.

#### B.3.5.2 Example Work Products

- process quality certification.

#### B.3.5.3 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.

### B.3.6 BP.12.05 - Analyse Quality Measurements

Analyse quality using the measurements to develop recommendations for quality improvement or corrective action, as appropriate.

#### B.3.6.1 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.

#### B.3.6.2 Example Work Products

- analysis of deviations.;
- failure analysis;
- defect reports;
- system quality trends;
- corrective action recommendations;
- cause and effect diagrams.

#### B.3.6.3 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.

### **B.3.7 BP.12.06 - Obtain Participation**

Obtain employee participation in identifying and reporting quality issues.

#### **B.3.7.1 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. Ideas for improving quality need to be encouraged, and a forum needs to exist that allows each employee to raise process-quality issues freely.

#### **B.3.7.2 Example Work Products**

- environment that promotes quality;
- captured inputs and resolutions from workers.

#### **B.3.7.3 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.

### **B.3.8 BP.12.07 - Initiate Quality Improvement Activities**

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

#### **B.3.8.1 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 minimizing cumbersome or bureaucratic systems.

#### **B.3.8.2 Example Work Products**

- recommendations for improving the systems engineering process;
- quality improvement plan;
- process revisions.

#### **B.3.8.3 Notes**

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

### **B.3.9 BP.12.08 - Detect Need for Corrective Actions**

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

#### **B.3.9.1 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.

### B.3.9.2 Example 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.

### B.3.9.3 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 (PA11).

## B.4 PA13 - Manage Configurations

### B.4.1 Process Area

#### B.4.1.1 Security Considerations

In BP.13.02 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.

Manage Configurations provides evidence to PA06 Build Assurance Argument. Also, the configuration management system selected should itself be managed according to PA08 Administer Security Controls.

#### B.4.1.2 Summary Description

The purpose of Manage Configurations is to maintain data on and status of identified configuration units, and to analyse 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.

#### B.4.1.3 Goals

- Control over work product configurations is maintained.

#### B.4.1.4 Base Practice List

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

- |          |  |
|----------|--|
| BP.13.01 | Decide on appropriate method for configuration management..  |
| BP.13.02 | Identify the indivisible units for configuration management.   |
| BP.13.03 | Maintain a repository of work product baselines.   |
| BP.13.04 | Control changes to established configuration units.  |
| BP.13.05 | Communicate status of configuration data, proposed changes, and access information to affected groups. |

#### B.4.1.5 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.

#### B.4.2 BP.13.01 - Establish Configuration Management Method

Decide on appropriate method for configuration management.

##### B.4.2.1 Description

Three primary trade-off 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.

##### B.4.2.2 Example Work Products

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

##### B.4.2.3 Notes

Example criteria for selecting configuration units at the appropriate work product level include:

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

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;
- if system element is ready for test;
- degree of formalization selected;
- cost and schedule limitations;
- customer requirements.

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.

### B.4.3 BP.13.02 - Identify Configuration Units

Identify the indivisible units for configuration management.

#### B.4.3.1 Description

A configuration unit is one or more work products that are treated as an indivisible unit for configuration management. 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.

#### B.4.3.2 Example Work Products

- work product configuration;
- identified configuration units.

#### B.4.3.3 Notes

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

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

### B.4.4 BP.13.03 - Maintain Work Product Baselines

Maintain a repository of work product baselines.

#### B.4.4.1 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.

#### B.4.4.2 Example Work Products

- decision database;
- configuration baseline;
- traceability matrix.

#### B.4.4.3 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.

### B.4.5 BP.13.04 - Control Changes

Control changes to established configuration units.

**B.4.5.1 Description**

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

Identified problems with the work product or requests to change the work product are analysed 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, 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.

**B.4.5.2 Example Work Products**

- new work-product baselines.

**B.4.5.3 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.

**B.4.6 BP.13.05 - Communicate Configuration Status**

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

**B.4.6.1 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 that are affected by the change. Access to configuration data and status should be provided to developers, customers, and other affected groups..

**B.4.6.2 Example Work Products**

- status reports.

**B.4.6.3 Notes**

Examples of activities for communicating configuration status include:

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

**B.5 PA14 - Manage Project Risks****B.5.1 Process Area****B.5.1.1 Security Considerations**

Manage Project Risks refers to risk related to the successful completion of the project, addressing issues related to cost and schedule. The Engineering process areas address "Security Risk" activities, by determining whether operational impacts due to residual security risks are tolerable. Results of security risk activities may provide input to and influence project risk management activities.

PA07 Coordinate Security should be taken into account to ensure that security issues are addressed.

### B.5.1.2 Summary Description

The purpose of Manage Project Risks 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 (PA16) and Monitor and Control Technical Effort (PA15) 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.

### B.5.1.3 Goals

- Risks to the program are identified, understood, and mitigated.

### B.5.1.4 Base Practice List

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

- BP.14.01 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.14.02 Identify project risks by examining project objectives with respect to the alternatives and constraints, and identifying what can go wrong.
- BP.14.03 Assess risks and determine the probability of occurrence and consequence of realization.
- BP.14.04 Obtain formal recognition of the project risk assessment.
- BP.14.05 Implement the risk-mitigation activities.
- BP.14.06 Monitor risk-mitigation activities to ensure that the desired results are being obtained.

### B.5.1.5 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, analysing developer risk primarily deals with the management approach, i.e., profit and market building; whereas analysing user risk primarily is concerned with types and analysis, i.e., mission and goal satisfaction.

## B.5.2 BP.14.01 - 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.

### B.5.2.1 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.

### B.5.2.2 Example Work Products

- risk-management plan.

**B.5.2.3 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.

**B.5.3 BP.14.02 - Identify Risks**

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

**B.5.3.1 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).

**B.5.3.2 Example Work Products**

- list of identified risks.

**B.5.3.3 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-mitigation [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.

**B.5.4 BP.14.03 - Assess Risks**

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

**B.5.4.1 Description**

Estimate the chance of potential loss (or gain) and the consequence if the previously identified risks occur. Analyse 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.

**B.5.4.2 Example Work Products**

- risk assessment.

### B.5.4.3 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].

### B.5.5 BP.14.04 - Review Risk Assessment

Obtain formal recognition of the project risk assessment.

#### B.5.5.1 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.

#### B.5.5.2 Example Work Products

- risk-mitigation strategy.

#### B.5.5.3 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.

### B.5.6 BP.14.05 - Execute Risk Mitigation

Implement the risk-mitigation activities:

#### B.5.6.1 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.

#### B.5.6.2 Example Work Products

- risk-mitigation plan.

#### B.5.6.3 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].

**B.5.7 BP.14.06 - Track Risk Mitigation**

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

**B.5.7.1 Description**

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

**B.5.7.2 Example Work Products**

- risk status;
- risk taxonomy.

**B.5.7.3 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.

**B.6 PA15 - Monitor and Control Technical Effort****B.6.1 Process Area****B.6.1.1 Security Considerations**

PA07 Monitor 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.

**B.6.1.2 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.

**B.6.1.3 Goals**

- The technical effort is monitored and controlled.

**B.6.1.4 Base Practice List**

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

- |          |  |
|----------|--|
| BP.15.01 | Direct technical effort in accordance with technical management plans.   |
| BP.15.02 | Track actual use of resources against technical management plans.  |
| BP.15.03 | Track performance against the established technical parameters.  |
| BP.15.04 | Review performance against the technical management plans.   |
| BP.15.05 | Analyse issues resulting from the tracking and review of technical parameters to determine corrective actions. |
| BP.15.06 | Take corrective actions when actual results deviate from plans.  |

### B.6.1.5 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.

### B.6.2 BP.15.01 - Direct Technical Effort

Direct technical effort in accordance with technical management plans.

#### B.6.2.1 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.

#### B.6.2.2 Example Work Products

- matrix of responsibilities;
- work authorizations.

#### B.6.2.3 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.

### B.6.3 BP.15.02 - Track Project Resources

Track actual use of resources against technical management plans.

#### B.6.3.1 Description

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

#### B.6.3.2 Example Work Products

- resource usage.

#### B.6.3.3 Notes

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

### B.6.4 BP.15.03 - Track Technical Parameters

Track performance against the established technical parameters.

#### B.6.4.1 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 be communicated to management.

**B.6.4.2 Example Work Products**

- profile of technical performance management.

**B.6.4.3 Notes**

An example of a performance tracking scenario follows:

For each technical parameter, define a bench marking activity that will be used to obtain the measurement. Use persons from outside the control of the project manager to perform the bench marking activities to ensure objective measurements. Periodically perform the bench marking activity and compare the actual measurement with the planned values of the parameters.

**B.6.5 BP.15.04 - Review Project Performance**

Review performance against the technical management plans.

**B.6.5.1 Description**

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

**B.6.5.2 Example Work Products**

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

**B.6.5.3 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.

**B.6.6 BP.15.05 - Analyse Project Issues**

Analyse issues resulting from the tracking and review of technical parameters to determine corrective actions.

**B.6.6.1 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.

**B.6.6.2 Example Work Products**

- analysis of project performance issues;
- approved corrective actions.

**B.6.6.3 Notes**

New information is integrated with historical project data. 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 modelling and simulation tools as well as outside expert opinions.

## B.6.7 BP.15.06 - Take Corrective Action

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

### B.6.7.1 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.

### B.6.7.2 Example Work Products

- resource reallocation;
- changes to methods and procedures;
- change orders.

### B.6.7.3 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.

## B.7 PA16 - Plan Technical Effort

### B.7.1 Process Area

#### B.7.1.1 Security Considerations

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.

#### B.7.1.2 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.

#### B.7.1.3 Goals

- All aspects of the technical effort are planned.

#### B.7.1.4 Base Practice List

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

- |          |   |
|----------|---|
| BP.16.01 | Identify resources that are critical to the technical success of the project.                         |
| BP.16.02 | Develop estimates for the factors that affect the magnitude and technical feasibility of the project. |
| BP.16.03 | Develop cost estimates for all technical resources required by the project.                           |
| BP.16.04 | Determine the technical process to be used on the project.  |
| BP.16.05 | Identify technical activities for the entire life cycle of the project.                               |
| BP.16.06 | Define specific processes to support effective interaction with the customer(s) and supplier(s).      |
| BP.16.07 | Develop technical schedules for the entire project life cycle.  |

- BP.16.08 Establish technical parameters with thresholds for the project and the system.
- BP.16.09 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.16.10 Review the technical management plans with all affected groups and individuals, and obtain group commitment.

#### B.7.1.5 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.

#### B.7.2 BP.16.01 - Identify Critical Resources

Identify resources that are critical to the technical success of the project.

##### B.7.2.1 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 analysing project tasks and schedules, and by comparing this project with similar projects.

##### B.7.2.2 Example Work Products

- identified critical resources.

##### B.7.2.3 Notes

Example practice: Examine the project schedules 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.

#### B.7.3 BP.16.02 - Estimate Project Scope

Develop estimates for the factors that affect the magnitude and technical feasibility of the project.

##### B.7.3.1 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.

##### B.7.3.2 Example 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.

##### B.7.3.3 Notes

Example practice: Analyse 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.

**B.7.4 BP.16.03 - Estimate Project Costs**

Develop cost estimates for all technical resources required by the project.

**B.7.4.1 Description**

A detailed estimate of project costs is essential to good project management, whether or not a customer requires it. Estimates of project costs are made by determining the labour 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 labour 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.

**B.7.4.2 Example Work Products**

- total labour 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.

**B.7.4.3 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 that may otherwise be overlooked. Variance reports and "lessons-learned" documents are typically good sources of this type of information.

**B.7.5 BP.16.04 - Determine Project's Process**

Determine the technical process to be used on the project.

**B.7.5.1 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.

**B.7.5.2 Example Work Products**

- selected systems engineering process for the project.

**B.7.5.3 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.

**B.7.6 BP.16.05 - Identify Technical Activities**

Identify technical activities for the entire life cycle of the project.

**B.7.6.1 Description**

Project and systems engineering activities may be selected from applicable standards, known best practice within the industry segment, reference models such as the SSE-CMM®, or the organization's historical experience.

**B.7.6.2 Example Work Products**

- identified technical activities.

**B.7.6.3 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 non systems engineering technical activities, use this same method while working with other disciplines according to the Integrate Disciplines process area (PA04).

**B.7.7 BP.16.06 - Define Project Interface**

Define specific processes to support effective interaction with customer(s) and supplier(s).

**B.7.7.1 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.

**B.7.7.2 Example Work Products**

- defined processes for project interfaces.

**B.7.7.3 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.

**B.7.8 BP.16.07 - Develop Project Schedules**

Develop technical schedules for the entire project life cycle.

**B.7.8.1 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.

**B.7.8.2 Example Work Products**

- project schedules.

### B.7.8.3 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 non critical path activities, it may be necessary to adjust the activity duration, activity sequencing, or activity start dates to avoid unacceptable resource peaking.

### B.7.9 BP.16.08 - Establish Technical Parameters

Establish technical parameters with thresholds for the project and the system.

#### B.7.9.1 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.

#### B.7.9.2 Example 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.

#### B.7.9.3 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.

### B.7.10 BP.16.09 - 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.

#### B.7.10.1 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.

**B.7.10.2 Example Work Products**

- technical management plan.

**B.7.10.3 Notes**

Technical management plans typically include;

- plans for developing the system;
- plans for interacting with other organizations (e.g., subcontractors) performing the technical effort.

**B.7.11 BP.16.10 - Review and Approve Project Plans**

Review the technical management plans with all affected groups and individuals, and obtain group commitment.

**B.7.11.1 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. Whenever possible, these inputs are incorporated to build team ownership of the plans. 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.

**B.7.11.2 Example Work Products**

- interface issues between disciplines/groups;
- risks;
- project plan inputs;
- project plan comments;
- project plan issues and resolutions.

**B.7.11.3 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.

**B.8 PA17 - Define Organization's Systems Engineering Process****B.8.1 Process Area**

### B.8.1.1 Security Considerations

This process area uses the term "Systems Engineering" However, this process area is broadly applicable and the term "Systems Engineering" can be replaced with the term "Security Engineering" when assessing an organization's security engineering capability.

Base practices need to address the integration of security engineering with systems engineering and other engineering disciplines. Therefore, PA09 Coordinate Security should be taken into account when defining the organization's security engineering process.

### B.8.1.2 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 systems-engineering process assets. Assets include example processes, process fragments, process-related documentation, process architectures, process-tailoring rules and tools, and process measurements.

### B.8.1.3 Goals

- A standard systems engineering process is defined for the organization.

### B.8.1.4 Base Practice List

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

- BP.17.01 Establish goals for the organization's systems engineering process from the organization's business goals.
- BP.17.02 Collect and maintain systems-engineering process assets.
- BP.17.03 Develop a well-defined standard systems engineering process for the organization.
- BP.17.04 Define guidelines for tailoring the organization's standard systems engineering process for project use in developing the project's defined process.

### B.8.1.5 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).

## B.8.2 BP.17.01 - Establish Process Goals

Establish goals for the organization's systems engineering process from the organization's business goals.

### B.8.2.1 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.

### B.8.2.2 Example 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.

### B.8.2.3 Notes

Establishing goals may include determining the tradeoff criteria for process performance based on time-to-market, quality, and productivity business issues.

## B.8.3 BP.17.02 - Collect Process Assets

Collect and maintain systems-engineering process assets.

### B.8.3.1 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.

### B.8.3.2 Example Work Products

- instructions for use of a process asset library;
- design specifications for a process asset library;
- process assets.

### B.8.3.3 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.

## B.8.4 BP.17.03 - Develop Organization's Systems Engineering Process

Develop a well-defined standard systems engineering process for the organization.

### B.8.4.1 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.

### B.8.4.2 Example Work Products

- organization's standard systems engineering process;
- inputs to training;
- inputs to systems engineering process improvement.

### B.8.4.3 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].

### B.8.5 BP.17.04 - Define Tailoring Guidelines

Define guidelines for tailoring the organization's standard systems engineering process for project use in developing the project's defined process.

#### B.8.5.1 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 projects to bypass standards that must be followed or substantial and important practices prescribed by organization policy.

#### B.8.5.2 Example Work Products

- tailoring guidelines for the organization's standard systems engineering process.

#### B.8.5.3 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.

## B.9 PA18 - Improve Organization's Systems Engineering Processes

### B.9.1 Process Area

#### B.9.1.1 Security Considerations

In Improve Organization's Systems Engineering Processes, the term "Systems Engineering" is used. This process area 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, base practices need to address the integration of security engineering with systems engineering disciplines.

### B.9.1.2 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, analysing the performance of the processes, and explicitly planning and deploying improvements to those processes.

### B.9.1.3 Goals

- Improvements to the standard systems engineering process are planned and implemented.

### B.9.1.4 Base Practice List

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

- |          |  |
|----------|--|
| BP.18.01 | Appraise the existing processes being performed in the organization to understand their strengths and weaknesses.                                  |
| BP.18.02 | Plan improvements to the organization's processes based on analysing the impact of potential improvements on achieving the goals of the processes. |
| BP.18.03 | Change the organization's standard systems engineering process to reflect targeted improvements.   |
| BP.18.04 | Communicate process improvements to existing projects and to other affected groups, as appropriate.  |

### B.9.1.5 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.

## B.9.2 BP.18.01 - Appraise the Process

Appraise the existing processes being performed in the organization to understand their strengths and weaknesses.

### B.9.2.1 Description

Appraise the existing processes being performed in the organization to understand their strengths and weaknesses.

### B.9.2.2 Example Work Products

- process maturity profiles;
- process performance analyses;
- appraisal findings;
- gap analyses.

### B.9.2.3 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,