

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

ICS 35.040,

National foreword

This British Standard is the UK implementation of ISO/IEC 21827:2008.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 February 2009
© BSI 2009

ISBN 978 0 580 56213 6

Amendments/corrigenda issued since publication

Date	Comments

INTERNATIONAL STANDARD

BS ISO/IEC 21827:2008

ISO/IEC 21827

Second edition
2008-10-15

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

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



Reference number
ISO/IEC 21827:2008(E)

AVA Documents
Document Sharing Hub
© ISO/IEC 2008

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.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

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.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword.....	v
0 Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions.....	2
4 Background	6
4.1 Reason for Development	7
4.2 The Importance of Security Engineering.....	7
4.3 Consensus.....	7
5 Structure of the Document	8
6 Model Architecture	8
6.1 Security Engineering	8
6.2 Security Engineering Process Overview.....	11
6.3 SSE-CMM® Architecture Description	14
6.4 Summary Chart	22
7 Security Base Practices	23
7.1 PA01 Administer Security Controls	24
7.2 PA02 - Assess Impact.....	28
7.3 PA03 - Assess Security Risk	32
7.4 PA04 - Assess Threat	36
7.5 PA05 - Assess Vulnerability	39
7.6 PA06 - Build Assurance Argument	43
7.7 PA07 - Coordinate Security	46
7.8 PA08 - Monitor Security Posture.....	49
7.9 PA09 - Provide Security Input	54
7.10 PA10 - Specify Security Needs.....	59
7.11 PA11 - Verify and Validate Security	63
Annex A (normative) Generic Practices.....	67
Annex B (normative) Project and Organizational Base Practices.....	68
B.1 General.....	68
B.2 General Security Considerations	68
B.3 PA12 - Ensure Quality	69
B.4 PA13 - Manage Configurations.....	74
B.5 PA14 - Manage Project Risks	78
B.6 PA15 - Monitor and Control Technical Effort.....	82
B.7 PA16 - Plan Technical Effort.....	86
B.8 PA17 - Define Organization's Systems Engineering Process.....	92
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.....	102
B.12 PA21 - Provide Ongoing Skills and Knowledge	106
B.13 PA22 - Coordinate with Suppliers	112
Annex C (informative) Capability Maturity Model Concepts	117
C.1 General.....	117
C.2 Process Improvement	117
C.3 Expected Results	118

C.4	Common Misunderstandings.....	118
C.5	Key Concepts	120
Annex D	(informative) Generic Practices	124
D.1	General	124
D.2	Capability Level 1 - Performed Informally	125
D.3	Capability Level 2 - Planned and Tracked	126
D.4	Capability Level 3 - Well Defined	132
D.5	Capability Level 4 - Quantitatively Controlled.....	137
D.6	Capability Level 5 - Continuously Improving	139
	Bibliography	142

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 2.

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 document 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 Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*. In addition, alignment is being maintained with the publicly available System Security Engineering - Capability Maturity Model®¹⁾ (SSE-CMM®) Version 3, published by the International Systems Security Engineering Association (ISSEA) as a Publicly Available Specification.

This second edition cancels and replaces the first edition (ISO/IEC 21827:2002), which has been technically revised.

SSE-CMM includes excerpts from “A Systems Engineering Capability Maturity Model (SE-CMM), Version 1.1”, CMU/SEI—95-MM-003, Copyright 1995 by Carnegie Mellon University. SE-CMM is a collaborative effort of Hughes Space and Communications, Hughes Telecommunications and Space, Lockheed Martin, Software Engineering Institute, Software Productivity Consortium, and Texas Instruments Incorporated. Neither Carnegie Mellon University nor the Software Engineering Institute directly or indirectly endorse SSE-CMM or ISO/IEC 21827.

1) ® CMM and Capability Maturity Model are Service Marks of Carnegie Mellon University NOT-FOR-PROFIT CORPORATION PENNSYLVANIA, 5000 Forbes Avenue, Pittsburgh, PA 15213, USA.

0 Introduction

0.1 General

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 or 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 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.

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

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

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 threats, 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); and
- 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.

0.2 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; and
- standard mechanism for customers to evaluate a provider's security engineering capability.

The scope of the assessment should be defined by the assessment organization and discussed with the assessor, if applicable.

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 15504-4, *Information technology — Process assessment — Part 4: Guidance on use for process improvement and process capability determination*.

0.3 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 case, 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; and
- 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; and
- 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; and
- predictable, repeatable level of confidence in product or service.

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; and
- capability-based confidence in evidence, reducing security evaluation workload.

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

1 Scope

This International Standard specifies the Systems Security Engineering – Capability Maturity Model® (SSE-CMM®). The SSE-CMM® is a process reference model focused upon the requirements for implementing security in a system or series of related systems that are the information technology security (ITS) domain. Within the ITS domain, the SSE-CMM® is focused on the processes used to achieve ITS, most specifically on the maturity of those processes. There is no intent within the SSE-CMM® 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® 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 life cycle 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; and
- all types and sizes of security engineering organization, from commercial to government and the academe.

While the SSE-CMM® is a distinct model to improve and assess security engineering capability, this does not imply that security engineering should be practised in isolation from other engineering disciplines. On the contrary, the SSE-CMM® promotes 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 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.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15504-2, *Information technology — Process assessment — Part 2: Performing an assessment*

3 Terms and definitions

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

3.1 **accountability**

property that ensures that the actions of an entity can be traced uniquely to the entity

[ISO/IEC 7498-2:1989]

3.2 **accreditation**

formal declaration by a designated approving authority that a system is approved to operate in a particular security mode using a prescribed set of safeguards

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

NOTE Adapted from ISO/IEC TR 15443-1:2005.

3.4 **asset**

anything that has value to the organization

[ISO/IEC TR 13335-1:1996]

3.5 **assurance**

grounds for confidence that a deliverable meets its security objectives

NOTE 1 Adapted from ISO/IEC 15408-1:2005.

NOTE 2 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**

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

3.7 **assurance Claim**

assertion or supporting assertion that a system meets a security need

NOTE 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

NOTE The evidence may consist of observation, test results, analysis results and appraisals.

3.9

authenticity

property that ensures that the identity of a subject or resource is the one claimed

NOTE 1 Authenticity applies to entities such as users, processes, systems and information.

NOTE 2 Adapted from ISO/IEC TR 13335-1:1996.

3.10

availability

property of being accessible and useable upon demand by an authorized entity

[ISO/IEC 7498-2:1989]

3.11

baseline

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

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

property that information is not made available or disclosed to unauthorized individuals, entities or processes

[ISO/IEC 7498-2:1989]

3.14

consistency

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 that 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. See ISO 9000 and ISO/IEC 15504.

3.17

effectiveness

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

collection of individuals (both managers and technical staff) which is responsible for project or organizational activities related to a particular engineering discipline

NOTE Engineering disciplines include the following: 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

property of safeguarding the accuracy and completeness of information and processing methods

3.21

maintenance

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

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

3.23

penetration profile

definition of the activities required to effect a penetration

3.24

procedure

written description of a course of action to be taken to perform a given task

[IEEE-Std. 610]

3.25

process

set of interrelated activities which transform inputs into outputs

NOTE Adapted from ISO/IEC 15288:2002.

3.26

reliability

property of consistent behaviour and results

[ISO/IEC TR 13335-1:1996]

3.27

residual risk

risk that remains after safeguards have been implemented

[ISO/IEC TR 13335-1:1996]

NOTE This definition differs from that used in ISO/IEC Guide 73.

3.28

risk

potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets

[ISO/IEC TR 13335-1:1996]

NOTE This definition differs from that used in ISO/IEC Guide 73.

3.29

risk analysis

process of identifying security risks, determining their magnitude and identifying areas needing safeguards

[ISO/IEC TR 13335-1:1996]

NOTE This definition differs from that used in ISO/IEC Guide 73.

3.30

risk management

process of assessing and quantifying risk and establishing an acceptable level of risk for the organization

[ISO/IEC TR 13335-1:1996]

NOTE This definition differs from that used in ISO/IEC Guide 73.

3.31

security policy

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

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

NOTE 1 Adapted from ISO/IEC 15288.

NOTE 2 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 3 The system may need other systems during its life cycle to meet its requirements. For 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 to a program or system, or to cause these to harm others

3.35
threat agent

originator and/or 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

NOTE Adapted from ISO/IEC 15288.

3.37
verification

confirmation by examination and provision of objective evidence that specified requirements have been fulfilled

NOTE Adapted from ISO/IEC 15288.

3.38
vulnerability

includes a weakness of an asset or group of assets which can be exploited by a threat

[ISO/IEC TR 13335-1:1996]

3.39
work product

artifact associated with the execution of a process

[ISO/IEC 15504-1]

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; and
- interactions with other organizations, including acquisition, system management, certification, accreditation, and evaluation.

The SSE-CMM® Model Description provides an overall description of the principles and architecture upon which the SSE-CMM® is 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:

- focused investments in security engineering tools, training, process definition, management practices, and improvements by engineering groups;
- capability-based assurance, (i.e. trustworthiness based on confidence in the maturity of an engineering group's security practices and processes); and
- 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 organizations, many of them multinational 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.ssecmm.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 Critical Design Review 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.

6 Model Architecture

The SSE-CMM® is a compilation of the security engineering best 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 (i.e. determine acceptable risks); and
- 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;
- integrators;
- acquirers (acquisition organization or end user);
- security evaluation organizations (system certifier, product evaluator, or operation accreditor);
- system administrator;
- trusted third parties (certification authority); and
- 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; and
- 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; and
- 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, including:

- 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 (content and traffic 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; and
- computer Security deals specifically with 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.

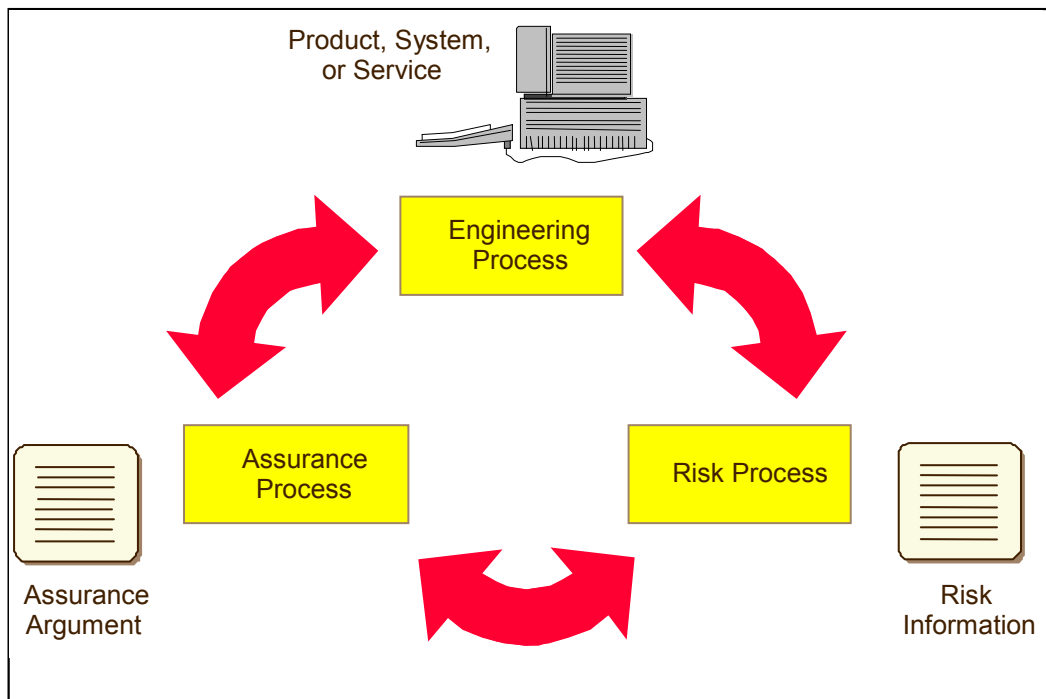


Figure 1 — The security engineering process has three main areas

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, the 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 all the activities that need to be coordinated to direct and control an organisations risk management activities. It includes establishing an acceptable level of risk for an organisation and identifying, analysing, evaluating and treating risks accordingly. Managing risk is an important part of the management of security.

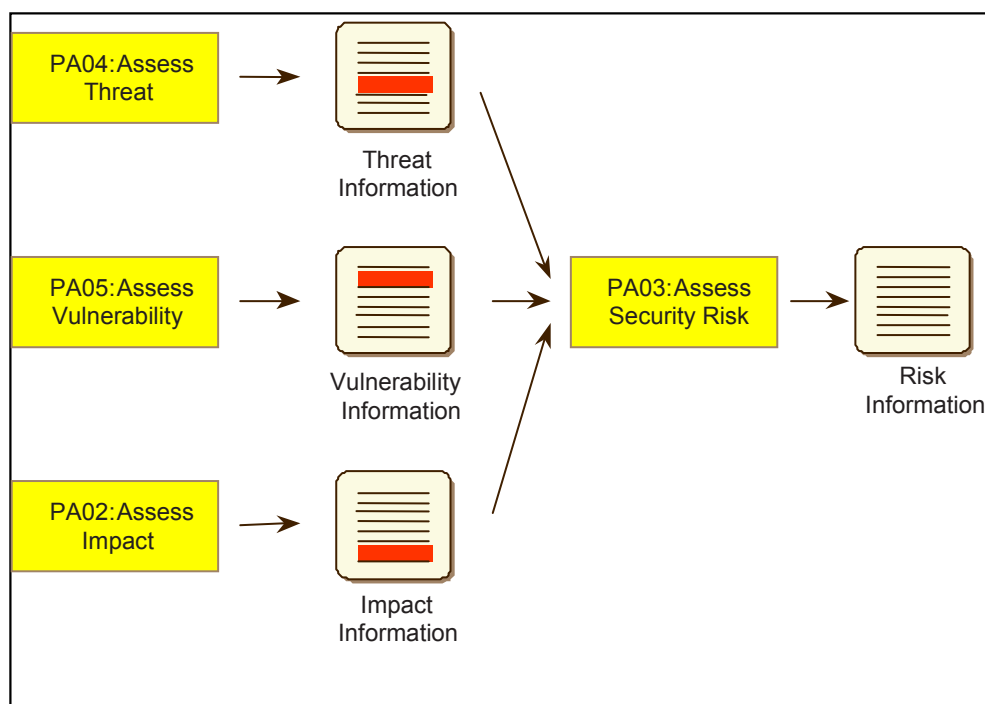


Figure 2 — The security risk process involves threats, vulnerabilities, and impact.

Risks are treated by the implementation of safeguards, which may address the threat, the vulnerability, the impact, or the risk itself. However, it is not feasible to treat all risks or completely mitigate any particular risk. This is in large part due to the cost of risk treatment, and to the associated uncertainties. Thus, some residual risk must always be accepted. In the presence of high uncertainty, risk acceptance becomes very problematic 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.

NOTE The ordering of the process areas is strictly alphabetical based on the title of the Process Area. This is done in order not to infer any sequence or precedence in the ordering of the Process Areas.

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 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.

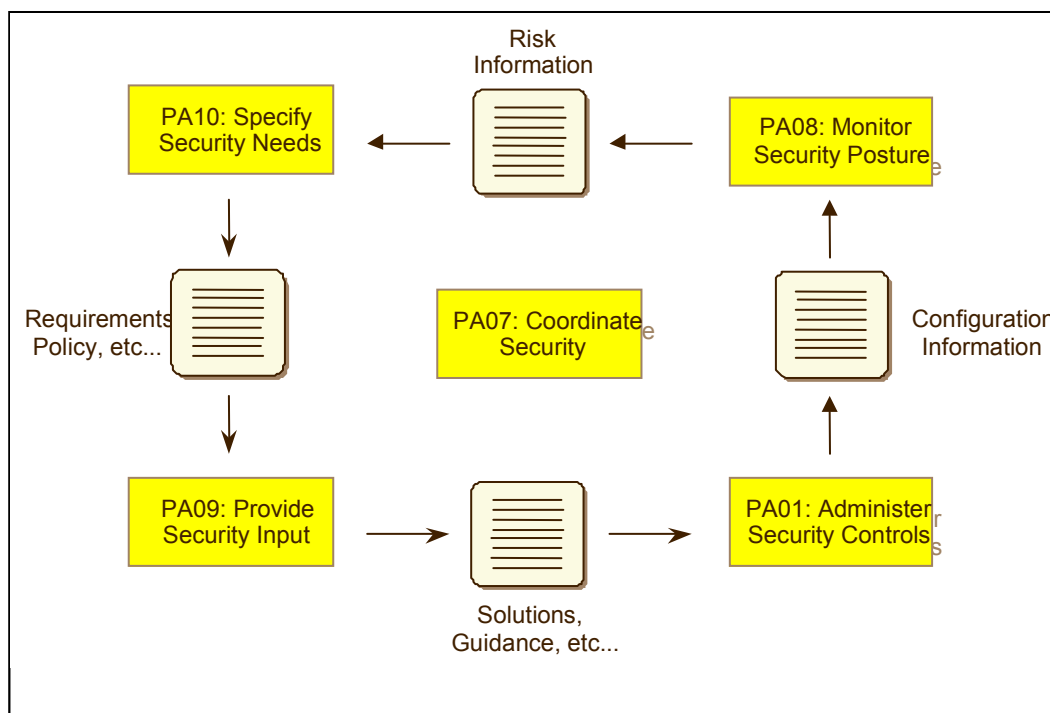


Figure 3 — Security is an integral part of the overall engineering process

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.

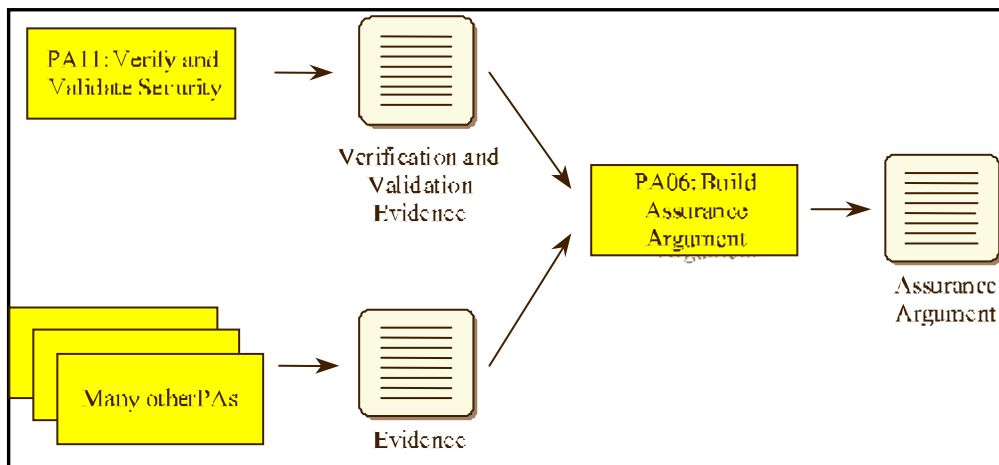


Figure 4 — The assurance process builds an argument establishing confidence

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 can be view as the property that the safeguards, as designed, implement the requirements. Effectiveness can be viewed as 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 focusing 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 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.

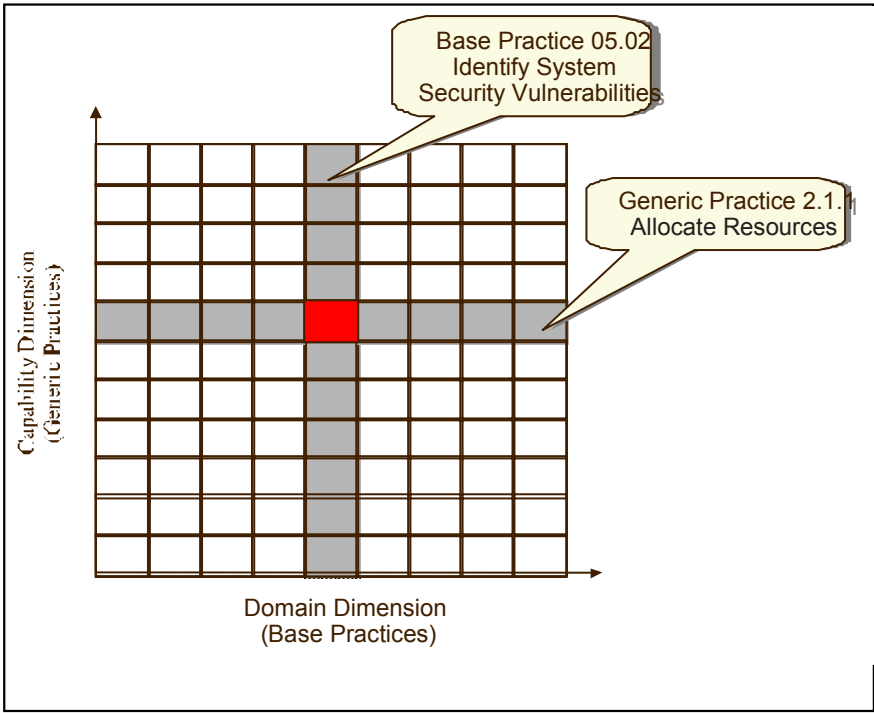


Figure 5 — The model evaluates each process area against each common feature.

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; and
- 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; and
- 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 the process areas are ordered by lifecycle phase or area. These process areas and the base practices that define them are described in Clause 7, 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; and
- 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; and
- PA22 - Coordinate with Suppliers.

NOTE These PAs have been placed in an annex to facilitate future enhanced alignment with ISO/IEC 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 the 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 feature 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 Annex A, are grouped to emphasize any major shift in an organization's characteristic manner of doing security engineering. Table 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 organizationwide processes.	The Planned and Tracked level focuses on projectlevel definition, planning and performance issues.
Use the best of what you've learned from your projects to create organizationwide processes.	The Well Defined level focuses on disciplined tailoring from defined processes at the organization level.
You can't measure it until you know what “it” is.	Although it is essential to begin collecting and using basic project measures early (i.e., at the Planned and Tracked level). Measurement and use of data is not expected organization wide until the Well Defined and particularly the Quantitatively Controlled levels have been achieved.
Managing with measurement is only meaningful when you're measuring the right things	The Quantitatively Controlled level focuses on measurements being tied to the business goals of the organization.
A culture of continuous improvement requires a foundation of sound management practice, defined processes, and measurable goals.	The Continuously Improving level gains leverage from all the management practice improvements seen in the earlier levels, then emphasizes the cultural shifts that will sustain the gains made.

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 Annex A.

Level 1:

- 1.1 Base Practices are Performed.

Level 2:

- 2.1 Planning Performance;
- 2.2 Disciplined Performance;

- 2.3 Verifying Performance; and
- 2.4 Tracking Performance.

Level 3:

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

Level 4:

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

Level 5:

- 5.1 Improving Organizational Capability; and
- 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 at any given capability level if the common features at lower capability levels have not been implemented. 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.

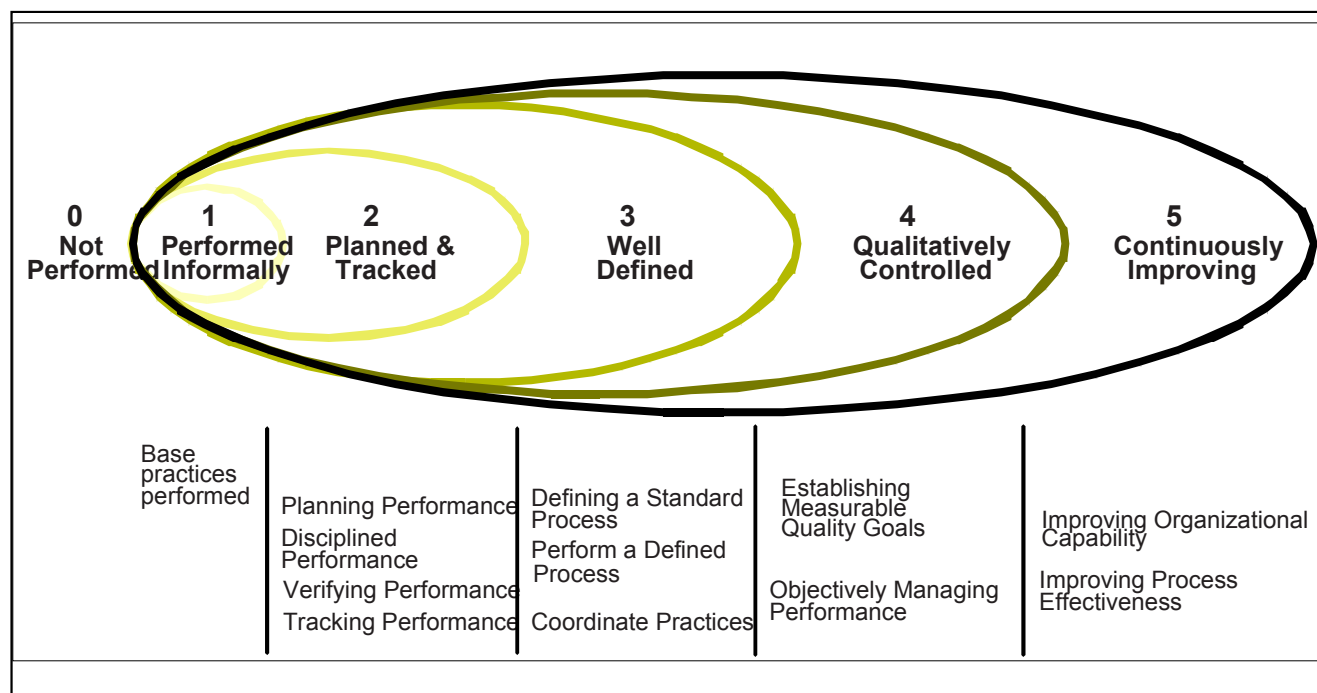


Figure 6 — Capability levels represent the maturity of security engineering organizations

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

6.3.5 Capability Dimension/Masurement 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 155042.

Table 2 — Capability Dimension to Measurement Framework Mapping

SSE-CMM® Capability Dimension	155042 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 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 5.2 Continuously improving attribute
Common Feature 5.2 Improving Process Effectiveness	PA 5.1 Process change attribute

6.3.6 Relationship to ISO/IEC 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, which are minor and are noted 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;
- ISO/IEC 21827 Work Products relate directly to ISO/IEC 15288 Outcomes; and
- ISO/IEC 21827 Process Descriptions are identical to 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 15288 is covered in more than one process area of ISO/IEC 21827.

NOTE 2 A column containing multiple "x" indicates that the particular process area of ISO/IEC 21827 is covered in more than one process of ISO/IEC 15288.

Table 3 — ISO/IEC 21827 Process Areas to ISO/IEC 15288 Processes Relationship

21827 Process Areas to 15288 Processes Relationships																							
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									X													X	
Environment Mgt	X																		X	X			
Investment Mgt																							NRE
System L-C Mgt																	X	X					
Resource Mgt																X					X	X	
Project Planning																X							
Project Assessment																X							
Project Control												X				X							
Decision Making									X														
Risk Mgt														X									
Configuration Mgt													X										
Information Mgt						X	X																
Stakeholder Requ. Def.										X													
Requirements Analysis			X						X	X	X												
Architecture Design									X														
Implementation																							NRE
Integration																							NRE
Verification										X													NRE
Transition											X												NRE
Validation																							
Operation							X												X				
Maintenance	X								X														
Disposal	X																						
Rmks					NRE	NRE	NRE																
Legend:		X																					

6.4 Summary Chart

This chart represents the model at a high level of abstraction. The practitioner is cautioned that each process area consists of a number of base practices, which are described in detail in Clause 7 and Annex B. Also, each common feature consists of a number of generic practices, which are described in detail in Annex A. It is up to each individual organization to select a combination of process areas to be applicable.

5.2 Improving Proc. Effectiveness																						
5.1 Improving Org. Capability																						
4.2 Objectively Managing Perf.																						
4.1 Establish Meas. Quality Goals																						
3.3 Coordinate Practices																						
3.2 Perform the Defined Process																						
3.1 Defining a Standard Process																						
2.4 Tracking Performance																						
2.3 Verifying Performance																						
2.2 Disciplined Performance																						
2.1 Planned Performance																						
Common Features	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	PA12 - Ensure Quality	PA13 - Manage Configurations	PA14 - Manage Project Risk	PA15 - Monitor and Control Technical Effort	PA16 - Plan Technical Effort	PA17 - Define Org. Security Eng. Process	PA18 - Improve Org. Security Eng. Process	PA19 - Manage Product Line Environment	PA20 - Manage Systems Eng. Support Env.	PA21 - Provide Ongoing Skills and Knowledge	PA22 - Coordinate with Suppliers
	Security Engineering Process Areas												Project and Organization Process Areas									

Figure 7 — Summary of Process Areas and Common Features relationships

7 Security Base Practices

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

An organization can be assessed against any one single process area or combination of process areas. The process areas together, however, are intended to cover all base practices for security engineering and there are many inter-relationships between the process areas. At present, the SSE-CMM® comprises 11 security process areas, each of which contains a number of base practices. Each process area is identified in the following subsections.

The general format of the process areas is shown in Figure 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 8 — 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.

When tracking the performance of this process area, reviewing trends among different Base Practices may indicate if an assurance argument is being satisfied. Refer to PA06.

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 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 - identifies the organization members related to security and their role;
- documents describing security roles - describe each of the organizational roles related to security and their responsibilities;
- documents describing security responsibilities - describe each of the security responsibilities in detail, including what output is expected and how it will be reviewed and used;
- documents detailing security accountabilities - describe who is accountable for security related problems, ensuring that someone is responsible for all risks; and
- documents detailing security authorizations - identify 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;
- 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 requirements 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; and
- control disposal - describes the procedure for removing or disabling security controls, including transition plans.

7.1.3.3 Notes

This BP includes the establishment of the security controls configurations, if required, however the actual task of configuring the security control is likely to be performed when the control is implemented. 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, and 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.

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; and
- catalogues 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 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; and
- 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 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. Some communities do not permit the reuse of media for less sensitive information. 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 measurements 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.

When tracking the performance of this process area, reviewing trends among different Base Practices may indicate if an assurance argument is being satisfied. Refer to PA06.

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 PA10.

7.2.2.2 Example Work Products:

- system priority lists and impact modifiers; and
- 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. An asset's value may also be defined in relation to their applicable security requirements. For example, an asset's value 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; and
- 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 defined as their significance to the value and criticality of the capabilities they support in the defined environment. In some cases, this practice is a review of the work from PA09 and PA11.

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

7.2.4.2 Example Work Products:

- selected impact measurements.

7.2.4.3 Notes

A limited set of consistent measurements minimizes the difficulty in dealing with divergent measurements. 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 measurements for this assessment and metric conversion factors if required.

7.2.5.1 Description

Some impacts may need to be assessed using different measurements. The relationship between different measurements needs to be established to ensure a consistent approach for all exposures throughout the impact assessment. "Exposure" refers to a combination of a threat, vulnerability, and impact that could cause significant harm. In some cases it will be necessary to combine measurements 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 measurements 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 measurements; and
- impact metric combination rules - describes the rules for combining impact measurements.

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 impacts of unwanted incidents with either multiple measurements or consolidated measurements 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 unauthorised disclosure, modification, loss and/or destruction. Impacts to capabilities might include interruption, delay, or reduced resilience.

Once a relatively complete list has been created, the impacts can be characterized using the measurements 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 measurements 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 measurements.

7.2.6.3 Notes

The impact assessment is performed based on the impact measurements 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 measurements 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 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 and the characteristics of existing impacts can change. 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.08.02.

7.2.7.2 Example Work Products:

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

7.2.7.3 Notes

Because impacts can change, the impact assessment activity should be iterative and should 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, analyse and evaluate 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. 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; and
- 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 identified, analysed, evaluated, 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, the 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 PA10 and the security input provided by PA09.

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.

When tracking the performance of this process area, reviewing trends among different Base Practices may indicate if an assurance argument is being satisfied. Refer to PA06.

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 identified, analysed, evaluated, 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 identified analysed, evaluated, 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 identification method describes the approach for identifying risks;
- risk assessment method - describes the approach for analysing and evaluating risks; and
- 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 threats, 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

Determine the consequences and likelihood of occurrence for each exposure, combine these values to produce a risk estimate, and evaluate the risk against pre-determined criteria.

7.3.4.2 Example Work Products:

- exposure risk list - a list of the calculated risks.

7.3.4.3 Notes

The likelihood of an exposure is a combination of the likelihood of the threat and the likelihood of the vulnerability. In many cases the likelihood of a specific magnitude or generalized magnitude, or the severity of impact, must also be factored in. In all cases there will be uncertainty associated with measurements. 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 to the data itself 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, BP.05.03 and BP.02.05 to assess impact of the realization of an exposure with either multiple measurements or consolidated measurements 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, BP.05.03 and BP.02.05. This base practice is closely associated with the activities of PA06 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 no 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 PA10, business priorities, and the overall system architecture.

7.3.6.2 Example Work Products:

- risk priority list - a list prioritizing the risks;
- safeguard requirement lists - lists of potential safeguards that can help mitigate the risks; and
- 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 PA10 and PA09.

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.08.02.

7.3.7.2 Example Work Products:

- risk monitoring reports - reports describing the current risk spectrum; and
- 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 should be conducted multiple times in the defined environments. However, risk assessment repetition should not supplant risk monitoring. Note that the term "spectrum" is used to denote new risks, and the term "characteristics" refers to the properties of existing identified risks.

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.

When tracking the performance of this process area, reviewing trends among different Base Practices may indicate if an assurance argument is being satisfied. Refer to PA06.

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; and
- 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, magnitude or frequency 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 threat events.

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 measurements 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.