
**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®)*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 21827:2008](https://standards.iteh.ai/catalog/standards/sist/a9d90a72-0b7f-4d0e-8355-9233e3dc9b53/iso-iec-21827-2008)

<https://standards.iteh.ai/catalog/standards/sist/a9d90a72-0b7f-4d0e-8355-9233e3dc9b53/iso-iec-21827-2008>

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 21827:2008](https://standards.iteh.ai/catalog/standards/sist/a9d90a72-0b7f-4d0e-8355-9233e3dc9b53/iso-iec-21827-2008)

<https://standards.iteh.ai/catalog/standards/sist/a9d90a72-0b7f-4d0e-8355-9233e3dc9b53/iso-iec-21827-2008>



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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 21827:2008](https://standards.iteh.ai/catalog/standards/sist/a9d90a72-0b7f-4d0e-8355-9233e3dc9b53/iso-iec-21827-2008)

<https://standards.iteh.ai/catalog/standards/sist/a9d90a72-0b7f-4d0e-8355-9233e3dc9b53/iso-iec-21827-2008>

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 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.

<https://standards.iteh.ai/catalog/standards/sist/a9d90a72-0b7f-4d0e-8355-0333e3de9b73/is-iso-21827-2008>

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.

ISO/IEC 21827:2008(E)

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC TR 13335-1:1996] <https://standards.iteh.ai/catalog/standards/sist/a9d90a72-0b7f-4d0e-8355-9233e3dc9b53/iso-iec-21827-2008>

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].

<https://standards.iteh.ai/catalog/standards/sist/a9d90a72-0b7f-4d0e-8355-9233e3dc9b53/iso-iec-21827-2008>

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

PREVIEW
(standards.iteh.ai)
ISO/IEC 21827:2008
<https://standards.iteh.ai/catalog/standards/gist/9d90a73-0b764d0e-8355-9233e3dc9b53/iso-iec-21827-2008>

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]

ITeH STANDARD PREVIEW
(standards.iteh.ai)

3.39
work product

artifact associated with the execution of a process

ISO/IEC 21827:2008

<https://standards.iteh.ai/catalog/standards/sist/a9d90a72-0b7f-4d0e-8355-9255e3dc9b53/iso-iec-21827-2008>

[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.