INTERNATIONAL ISO/IEC

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)

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

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.