INTERNATIONAL STANDARD

ISO/IEC 27034-1

First edition
2011-11-15

Information technology — Security techniques — Application security —

Part 1: Overview and concepts

Technologies de l'information — Techniques de sécurité — Sécurité des applications —

Partie 1: Aperçu général et concepts

Reference number
ISO/IEC 27034-1:2011(E)

COPYRIGHT PROTECTED DOCUMENT

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

Figures

Page

Tables

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 27034-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 27034 consists of the following parts, under the general title *Information technology — Security techniques — Application security*:

— *Part 1: Overview and concepts*

The following parts are under preparation:

— *Part 2: Organization normative framework*

— *Part 3: Application security management process*

— *Part 4: Application security validation*

— *Part 5: Protocols and application security control data structure*

Introduction

0.1 General

Organizations should protect their information and technological infrastructures in order to stay in business. Traditionally this has been addressed at the IT level by protecting the perimeter and such technological infrastructure components as computers and networks, which is generally insufficient.

In addition, organizations are increasingly protecting themselves at the governance level by operating formalized, tested and verified information security management systems (ISMS). A systematic approach contributes to an effective information security management system as described in ISO/IEC 27001.

However, organizations face an ever-growing need to protect their information at the application level.

Applications should be protected against vulnerabilities which might be inherent to the application itself (e.g. software defects), appear in the course of the application's life cycle (e.g. through changes to the application), or arise due to the use of the application in a context for which it was not intended.

A systematic approach to increased application security provides evidence that information being used or stored by an organization’s applications is adequately protected.

Applications can be acquired through internal development, outsourcing or purchasing a commercial product. Applications can also be acquired through a combination of these approaches which might introduce new security implications that should be considered and managed.

Examples of applications are human resource systems, finance systems, word-processing systems, customer management systems, firewalls, anti-virus systems and intrusion detection systems.

Throughout its life cycle, a secure application exhibits prerequisite characteristics of software quality, such as predictable execution and conformance, as well as meeting security requirements from a development, management, technological infrastructure, and audit perspective. Security-enhanced processes and practices—and the skilled people to perform them—are required to build trusted applications that do not increase risk exposure beyond an acceptable or tolerable level of residual risk and support an effective ISMS.

Additionally, a secure application takes into account the security requirements stemming from the type of data, the targeted environment (business, regulatory and technological contexts), the actors and the application specifications. It should be possible to obtain evidence that is shown to demonstrate that an acceptable (or tolerable) level of residual risk has been attained and is being maintained.

0.2 Purpose

The purpose of ISO/IEC 27034 is to assist organizations in integrating security seamlessly throughout the life cycle of their applications by:

a) providing concepts, principles, frameworks, components and processes;

b) providing process-oriented mechanisms for establishing security requirements, assessing security risks, assigning a Targeted Level of Trust and selecting corresponding security controls and verification measures;

c) providing guidelines for establishing acceptance criteria to organizations outsourcing the development or operation of applications, and for organizations purchasing from third-party applications;

d) providing process-oriented mechanisms for determining, generating and collecting the evidence needed to demonstrate that their applications can be used securely under a defined environment;

e) supporting the general concepts specified in ISO/IEC 27001 and assisting with the satisfactory implementation of information security based on a risk management approach; and

f) providing a framework that helps to implement the security controls specified in ISO/IEC 27002 and other standards.

ISO/IEC 27034:

a) applies to the underlying software of an application and to contributing factors that impact its security, such as data, technology, application development life cycle processes, supporting processes and actors; and

b) applies to all sizes and all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) exposed to risks associated with applications.

ISO/IEC 27034 does not:

a) provide guidelines for physical and network security;

b) provide controls or measurements; or

c) provide secure coding specifications for any programming language.

ISO/IEC 27034 is not:

a) a software application development standard;

b) an application project management standard; or

c) a software development life cycle standard.

The requirements and processes specified in ISO/IEC 27034 are not intended to be implemented in isolation but rather integrated into an organization's existing processes. To this effect, organizations should map their existing processes and frameworks to those proposed by ISO/IEC 27034, thus reducing the impact of implementing ISO/IEC 27034.

Annex A (informative) provides an example illustrating how an existing software development process can be mapped to some of the components and processes of ISO/IEC 27034. Generally speaking, an organization using any development life cycle should perform a mapping such as the one described in Annex A, and add whatever missing components or processes are needed for compliance with ISO/IEC 27034.

0.3 Targeted audiences

0.3.1 General

The following audiences will benefit from ISO/IEC 27034 while carrying out their designated organizational roles:

a) managers;

b) provisioning and operation teams;

c) acquisition personnel;

d) suppliers; and

e) auditors.

0.3.2 Managers

Managers are persons involved in the management of the application during its complete life cycle. The applicable stages of the application life cycle include the provisioning stages and the production stages. Examples of managers are:

a) information security managers;

b) project managers;

c) administrators;

d) software acquirers;

e) software development managers;

f) application owners;

g) line managers, who supervise employees.

Typically managers need to:

a) balance the cost of implementing and maintaining application security against the risks and value it represents for the organization;

b) review auditor's reports recommending acceptance or rejection based on whether an application has attained and maintained its Targeted Level of Trust;

c) ensure compliance with standards, laws and regulations according to an application's regulatory context (see 8.1.2.2);

d) oversee the implementation of a secure application;

e) authorize the Targeted Level of Trust according to the organization's specific context;

f) determine which security controls and corresponding verification measurements should be implemented and tested;

g) minimize application security verification costs;

h) document security policies and procedures for an application;

i) provide security awareness, training and oversight to all actors;

j) put in place proper information security clearances required by applicable information security policies and procedures; and

k) stay abreast of all system-related security plans throughout the organization's network.

0.3.3 Provisioning and operation teams

Members of provisioning and operation teams (known collectively as the project team) are persons involved in an application's design, development and maintenance throughout its whole life cycle. Members include:

a) architects,

b) analysts,

c) programmers,

d) testers,

e) system administrators,

f) database administrators,

g) network administrators, and

h) technical personnel.

Typically members need to:

a) understand which controls should be applied at each stage of an application's life cycle and why;

b) understand which controls should be implemented in the application itself;

c) minimize the impact of introducing controls into the development, test and documentation activities within the application life cycle;

d) make sure that introduced controls meet the requirements of the associated measurements;

e) obtain access to tools and best practices in order to streamline development, testing and documentation;

f) facilitate peer review;

g) participate in acquisition planning and strategy;

h) establish business relationships to obtain needed goods and services, (e.g. for the solicitation, evaluation and awarding of contracts); and

i) arrange disposal of residual items after work is completed, (e.g. property management/disposal).

0.3.4 Acquirers

This includes all persons involved in acquiring a product or service.

Typically acquirers need to:

a) prepare requests for proposals that include requirements for security controls;

b) select suppliers that comply with such requirements;

c) verify evidence of security controls applied by outsourcing services; and

d) evaluate products by verifying evidence of correctly implemented application security controls.

0.3.5 Suppliers

This includes all persons involved in supplying a product or service.

Typically suppliers need to:

a) comply to application security requirements from requests for proposals;

b) select appropriate application security controls for proposals, with respect to their impact on cost; and

c) provide evidence that required security controls are implemented correctly in proposed products or services.

0.3.6 Auditors

Auditors are persons who need to:

a) understand the scope and procedures involved in verification measurements for the corresponding controls;

b) ensure that audit results are repeatable;

c) establish a list of verification measurements which generate evidence that an application has reached the Targeted Level of Trust as required by management; and

d) apply standardized audit processes based on the use of verifiable evidence.

0.3.7 Users

Users are persons who need to:

a) trust that it is deemed secure to use or deploy an application;

b) trust that an application produces reliable results consistently and in a timely manner; and

c) trust that the controls and their corresponding verification measurements are positioned and functioning correctly as expected.

0.4 Principles

0.4.1 Security is a requirement

Security requirements should be defined and analyzed for each and every stage of an application's life cycle, adequately addressed and managed on a continuous basis.

Application security requirements (see 6.4) should be treated in the same manner as functionality, quality and usability requirements (see ISO/IEC 9126 for an example of a quality model). In addition, security-related requirements to conform to the established limitations on residual risk should be instituted.

According to ISO/IEC/IEEE 29148 (under development), requirements should be necessary, abstract, unambiguous, consistent, complete, concise, feasible, traceable and verifiable. The same characteristics apply to security requirements. Vague security requirements such as “The developer should discover all important security risks for the application” are too often encountered in application projects' documentation.