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)

© ISO/IEC 2011

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

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 VII

INTRODUCTION VIII

0.1 GENERAL VIII
0.2 PURPOSE VIII
0.3 TARGETED AUDIENCES IX
  0.3.1 General ix
  0.3.2 Managers ix
  0.3.3 Provisioning and operation teams x
  0.3.4 Acquirers xi
  0.3.5 Suppliers xi
  0.3.6 Auditors xi
  0.3.7 Users xi
0.4 PRINCIPLES XI
  0.4.1 Security is a requirement xi
  0.4.2 Application security is context-dependent xii
  0.4.3 Appropriate investment for application security xii
  0.4.4 Application security should be demonstrated xii
0.5 RELATIONSHIP TO OTHER INTERNATIONAL STANDARDS XIII
  0.5.1 General xiii
  0.5.2 ISO/IEC 27001, Information security management systems — Requirements xiii
  0.5.3 ISO/IEC 27002, Code of practice for information security management xiii
  0.5.4 ISO/IEC 27005, Information security risk management xiii
  0.5.5 ISO/IEC 21827, Systems Security Engineering — Capability Maturity Model® (SSE CMM®) xiii
  0.5.6 ISO/IEC 15408-3, Evaluation criteria for IT security — Part 3: Security assurance components xiii
  0.5.7 ISO/IEC TR 15443-1, A framework for IT security assurance — Part 1: Overview and framework, and ISO/IEC TR 15443-3, A framework for IT security assurance — Part 3: Analysis of assurance methods xiv
  0.5.8 ISO/IEC 15026-2, Systems and software engineering — Systems and software assurance — Part 2: Assurance case xiv
  0.5.9 ISO/IEC 15288, Systems and software engineering — System life cycle processes, and ISO/IEC 12207, Systems and software engineering — Software life cycle process xiv
  0.5.10 ISO/IEC 29193 (under development), Secure system engineering principles and techniques xiv

1 SCOPE 1

2 NORMATIVE REFERENCES 1

3 TERMS AND DEFINITIONS 1

4 ABBREVIATED TERMS 4

5 STRUCTURE OF ISO/IEC 27034 5

6 INTRODUCTION TO APPLICATION SECURITY 6

6.1 GENERAL 6
6.2 APPLICATION SECURITY VS SOFTWARE SECURITY 6
6.3 APPLICATION SECURITY SCOPE 6
  6.3.1 General 6
  6.3.2 Business context 7
  6.3.3 Regulatory context 7
  6.3.4 Application life cycle processes 7
  6.3.5 Processes involved with the application 7

6.3.6 Technological context 8
6.3.7 Application specifications 8
6.3.8 Application data 8
6.3.9 Organization and user data 8
6.3.10 Roles and permissions 8
6.4 APPLICATION SECURITY REQUIREMENTS 8
6.4.1 Application security requirements sources 8
6.4.2 Application security requirements engineering 9
6.4.3 ISMS 9
6.5 RISK 9
6.5.1 Application security risk 9
6.5.2 Application vulnerabilities 10
6.5.3 Threats to applications 10
6.5.4 Impact on applications 10
6.5.5 Risk management 10
6.6 SECURITY COSTS 10
6.7 TARGET ENVIRONMENT 10
6.8 CONTROLS AND THEIR OBJECTIVES 11

7 ISO/IEC 27034 OVERALL PROCESSES 11

7.1 COMPONENTS, PROCESSES AND FRAMEWORKS 11
7.2 ONF MANAGEMENT PROCESS 12
7.3 APPLICATION SECURITY MANAGEMENT PROCESS 13
7.3.1 General 13
7.3.2 Specifying the application requirements and environment 13
7.3.3 Assessing application security risks 13
7.3.4 Creating and maintaining the Application Normative Framework 13
7.3.5 Provisioning and operating the application 14
7.3.6 Auditing the security of the application 14

8 CONCEPTS 14

8.1 ORGANIZATION NORMATIVE FRAMEWORK 14
8.1.1 General 14
8.1.2 Components 15
8.1.3 Processes related to the Organization Normative Framework 28
8.2 APPLICATION SECURITY RISK ASSESSMENT 30
8.2.1 Risk assessment vs risk management 30
8.2.2 Application risk analysis 31
8.2.3 Risk Evaluation 31
8.2.4 Application's Targeted Level of Trust 31
8.2.5 Application owner acceptation 31
8.3 APPLICATION NORMATIVE FRAMEWORK 32
8.3.1 General 32
8.3.2 Components 33
8.3.3 Processes related to the security of the application 33
8.3.4 Application's life cycle 34
8.3.5 Processes 34
8.4 PROVISIONING AND OPERATING THE APPLICATION 34
8.4.1 General 34
8.4.2 Impact of ISO/IEC 27034 on an application project 35
8.4.3 Components 36
8.4.4 Processes 36
8.5 APPLICATION SECURITY AUDIT 37
8.5.1 General 37
8.5.2 Components 38

ANNEX A (INFORMATIVE) MAPPING AN EXISTING DEVELOPMENT PROCESS TO ISO/IEC 27034 CASE STUDY 39
A.1 GENERAL 39
A.2 ABOUT THE SECURITY DEVELOPMENT LIFECYCLE 39
A.3 SDL MAPPED TO THE ORGANIZATION NORMATIVE FRAMEWORK 40
A.4 BUSINESS CONTEXT 41
A.5 REGULATORY CONTEXT 41
A.6 APPLICATION SPECIFICATIONS REPOSITORY 42
A.7 TECHNOLOGICAL CONTEXT 42
A.8 ROLES, RESPONSIBILITIES AND QUALIFICATIONS 43
A.9 ORGANIZATION ASC LIBRARY 44
A.9.1 Training 45
A.9.2 Requirements 45
A.9.3 Design 46
A.9.4 Implementation 47
A.9.5 Verification 47
A.9.6 Release 48
A.10 APPLICATION SECURITY AUDIT 49
A.11 APPLICATION LIFE CYCLE MODEL 51
A.12 SDL MAPPED TO THE APPLICATION SECURITY LIFE CYCLE REFERENCE MODEL 53
ANNEX B (INFORMATIVE) MAPPING ASC WITH AN EXISTING STANDARD 55
B.1 ASC CANDIDATE CATEGORIES 55
B.1.1 Common security control-related considerations 55
B.1.2 Operational/environmental-related considerations 55
B.1.3 Physical Infrastructure-related considerations 55
B.1.4 Public access-related considerations 55
B.1.5 Technology-related considerations 56
B.1.6 Policy/regulatory-related considerations 56
B.1.7 Scalability-related considerations 56
B.1.8 Security objective-related considerations 56
B.2 CLASSES OF SECURITY CONTROLS 57
B.3 SUB-CLASSES IN THE ACCESS CONTROL (AC) CLASS 58
B.4 DETAILED ACCESS CONTROL CLASSES 59
B.4.1 AC-1 Access control policy and procedures 59
B.4.2 AC-2 Account management 59
B.4.3 AC-17 Remote access 60
B.5 DEFINITION OF AN ASC BUILT FROM A SAMPLE SP 800-53 CONTROL 61
B.5.1 Control AU-14 as described in SP 800-53 Rev. 3 61
B.5.2 Control AU-14 as described using ISO/IEC 27034 ASC format 62
ANNEX C (INFORMATIVE) ISO/IEC 27005 RISK MANAGEMENT PROCESS MAPPED WITH THE ASMP 65
BIBLIOGRAPHY 67

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27034-1:2011
https://standards.iteh.ai/catalog/standards/sist/ca8c290b-1318-492e-abc7-7590b5cb8cd6/iso-iec-27034-1-2011

Figures

Page
Figure 1 – Relationship to other International Standards xiii
Figure 2 – Application Security Scope 6
Figure 3 – Organization Management Processes 12
Figure 4 – Organization Normative Framework (simplified) 15
Figure 5 – Graphical representation of an example of an Organization ASC Library 18
Figure 6 – Components of an ASC 20
Figure 7 – Graph of ASCs 21
Figure 8 – Top-level view of the Application Security Life Cycle Reference Model 24
Figure 9 – ONF Management Process 28
Figure 10 – Application Normative Framework 32
Figure 11 – Impact of ISO/IEC 27034 on roles and responsibilities in a typical application project 35
Figure 12 – ASC used as a security activity 36
Figure 13 – ASC used as a measurement 37
Figure 14 – Overview of the application security verification process 38
Figure A.1 – Security Development Lifecycle 40
Figure A.2 – SDL mapped to the Organization Normative Framework 40
Figure A.3 – Example of an ASC tree 45
Figure A.4 – Example of a Line of Business Application for Application Security Audit 50
Figure A.5 – SDL Process Illustration 52
Figure A.6 – SDL mapped to the Application Security Life Cycle Reference Model 53
Figure A.7 – Detailed mapping of SDL phases with stages in the Application Security Life Cycle Reference Model 53
Figure C.1 – ISO/IEC 27005 risk management process mapped with the ASMP. 65

Tables

Page
Table 1 – Application Scope vs Application Security Scope 7
Table 2 – Mapping of ISMS and application security-related ONF management subprocesses 29
Table B.1 – Security control classes, families, and identifiers 57
Table B.2 – Security control classes and security control baselines for low-impact, moderate-impact, and high-impact information systems 58
Table B.3 – SP800-53 control AU-14 described using ISO/IEC 27034 ASC format 62

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.

ISO/IEC 27034-1:2011
https://standards.iteh.ai/catalog/standards/sist/ea8c2901-f318-4920-abe7-7390058b8dd6/iso-iec-27034-1-2011

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.

0.4.2 Application security is context-dependent

Application security is influenced by a defined target environment. The type and scope of application security requirements are determined by the risks to which the application is subjected, which in turn depend on three contexts:

a) business context: specific risks arising from the organization's business domain (phone company, transport company, government, etc.);

b) regulatory context: specific risks arising from the geographical location where the organization is doing business (intellectual property rights and licensing, restrictions on cryptography protection, copyright, laws and regulations, privacy legislation, etc.);

c) technological context: specific risks from the technologies used by the organization in the course of business [reverse engineering, security of build tools, protection of source code, use of third-party pre-compiled code, security testing, penetration testing, bounds checking, code checking, information and communication technology (ICT) environment in which the application runs, configuration files and uncompiled data, operating system privileges for installation and/or operation, maintenance, secure distribution, etc.].

   The technological context encompasses applications' technical specifications (security functionality, secure components, online payments, secure log, cryptography, permissions management, etc.).

An organization can affirm that an application is secure, but this affirmation is only valid for this particular organization in its specific business, regulatory and technological contexts. If, for example, the application's technological infrastructure changes, or the application is used for the same purposes in another country, these new contexts might impact the security requirements and the Targeted Level of Trust. The current Application Security Controls might no longer adequately address the new security requirements and the application might no longer be secure.

0.4.3 Appropriate investment for application security

The costs of applying Application Security Controls and performing audit measurements should be commensurate with the Targeted Level of Trust (see 8.1.2.6.4) required by the application owner or by management.

These costs can be considered as an investment because they reduce the costs, application owner responsibilities and legal consequences of security breaches.

0.4.4 Application security should be demonstrated

The application auditing process in ISO/IEC 27034 (see 8.5) makes use of the verifiable evidence provided by Application Security Controls (see 8.1.2.6.5).

An application cannot be declared secure unless the auditor agrees that the supporting evidence generated by the corresponding verification measurements of the applicable Application Security Controls demonstrates that it has reached management's Targeted Level of Trust.

0.5 Relationship to other International Standards

0.5.1 General

Figure 1 shows relationships between ISO/IEC 27034 and other International Standards.

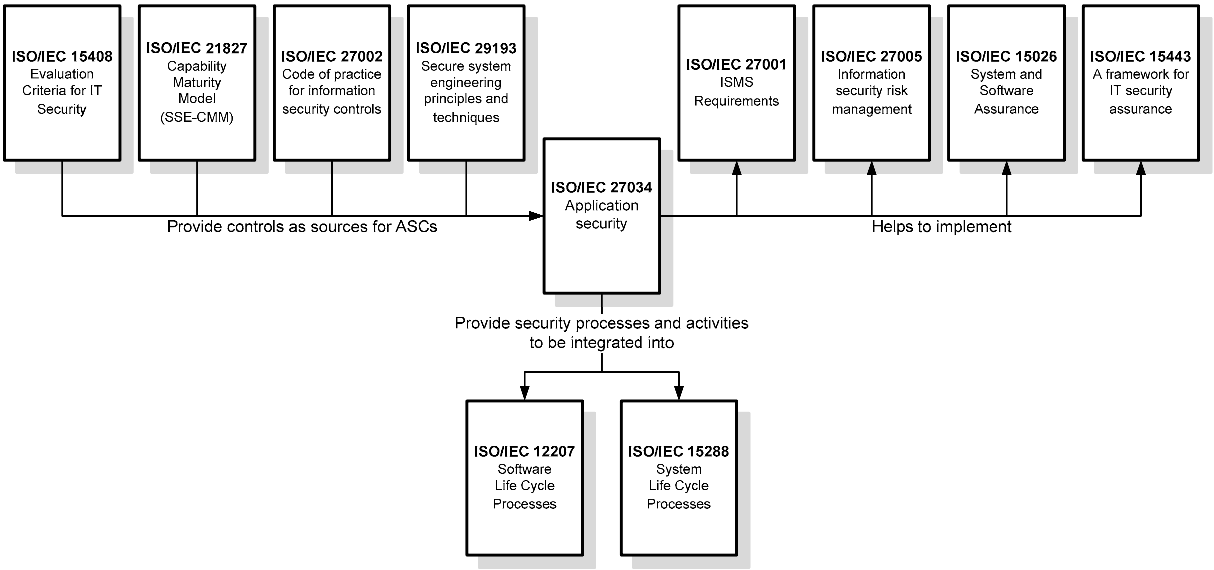
ISO/IEC 15408
Evaluation Criteria for IT Security
ISO/IEC 21827
Capability Maturity Model (SSE-CMM)
ISO/IEC 27002
Code of practice for information security controls
ISO/IEC 29193
Secure system engineering principles and techniques
ISO/IEC 27001
ISMS Requirements
ISO/IEC 27005
Information security risk management
ISO/IEC 15026
System and Software Assurance
ISO/IEC 15443
A framework for IT security assurance
ISO/IEC 27034
Application security
Provide controls as sources for ASCs
Helps to implement
Provide security processes and activities to be integrated into
ISO/IEC 12207
Software Life Cycle Processes
ISO/IEC 15288
System Life Cycle Processes

Figure 1 – Relationship to other International Standards

0.5.2 ISO/IEC 27001, Information security management systems — Requirements

ISO/IEC 27034 helps to implement, with a scope limited to application security, recommendations from ISO/IEC 27001. In particular, the following approaches are used:

a) systematic approach to security management;

b) “Plan, Do, Check, Act” process approach; and

c) implementation of information security based on risk management.

0.5.3 ISO/IEC 27002, Code of practice for information security management

ISO/IEC 27002 provides practices that an organization can implement as Application Security Controls as proposed by ISO/IEC 27034. Of utmost interest are controls from the following clauses in ISO/IEC 27002:2005:

a) clause 10: Communications and Operations Management;

b) clause 11: Access Control; and most importantly

c) clause 12: Information Systems Acquisition, Development and Maintenance.

0.5.4 ISO/IEC 27005, Information security risk management

ISO/IEC 27034 helps to implement, with a scope limited to application security, the risk management process proposed by ISO/IEC 27005. See Annex C (informative) for a more detailed discussion.

0.5.5 ISO/IEC 21827, Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)

ISO/IEC 21827 provides security engineering base practices that an organization can implement as Application Security Controls as proposed by ISO/IEC 27034. In addition, processes from ISO/IEC 27034 help to attain several of the capabilities that define the capability levels in ISO/IEC 21827.

0.5.6 ISO/IEC 15408-3, Evaluation criteria for IT security — Part 3: Security assurance components

ISO/IEC 15408-3 provides requirements and action elements that an organization can implement as Application Security Controls as proposed by ISO/IEC 27034.

0.5.7 ISO/IEC TR 15443-1, A framework for IT security assurance — Part 1: Overview and framework, and ISO/IEC TR 15443-3, A framework for IT security assurance — Part 3: Analysis of assurance methods

ISO/IEC 27034 helps to enforce and reflect the principles of security assurance from ISO/IEC TR 15443-1 and to contribute to the assurance cases of ISO/IEC TR 15443-3.

0.5.8 ISO/IEC 15026-2, Systems and software engineering — Systems and software assurance — Part 2: Assurance case

Use of processes and Application Security Controls from ISO/IEC 27034 in application projects directly provides assurance cases about the security of the application. In particular,

a) claims and their justifications are provided by the application security risk analysis process,

b) evidence is provided by Application Security Controls' built-in verification measurements, and

c) compliance to ISO/IEC 27034 can be used as argument in many such assurance cases.

See also 8.1.2.6.5.1.

0.5.9 ISO/IEC 15288, Systems and software engineering — System life cycle processes, and ISO/IEC 12207, Systems and software engineering — Software life cycle processes

ISO/IEC 27034 provides additional processes for the organization, as well as Application Security Controls that an organization can insert as additional activities into its existing systems and software engineering life cycle processes as provided by ISO/IEC 15288 and ISO/IEC 12207.

0.5.10 ISO/IEC TR 29193 (under development), Secure system engineering principles and techniques

ISO/IEC TR 29193 provides guidance for secure system engineering of ICT systems or products that an organization can implement as Application Security Controls as proposed by ISO/IEC 27034.

INTERNATIONAL STANDARD **ISO/IEC 27034-1:2011(E)**

Information technology — Security techniques — Application security —

Part 1:
Overview and concepts

1 Scope

ISO/IEC 27034 provides guidance to assist organizations in integrating security into the processes used for managing their applications.

This part of ISO/IEC 27034 presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security.

ISO/IEC 27034 is applicable to in-house developed applications, applications acquired from third parties, and where the development or the operation of the application is outsourced.

2 Normative references

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

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and the following apply.

3.1
actor
person or process that performs an activity during an application's life cycle or initiates interaction with any process provided by or impacted on by an application

3.2
Actual Level of Trust
result of an audit process that provides supporting evidence that all Application Security Controls required by the application’s Targeted Level of Trust were correctly implemented and verified, and produced the expected results