INTERNATIONAL STANDARD

ISO/IEC 27034-3

First edition
2018-05

Information technology — Application security —

Part 3:
Application security management process

Technologie de l'information — Sécurité des applications —

Partie 3: Processus de gestion de la sécurité d'une application

Reference number
ISO/IEC 27034-3:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

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

A list of all parts in the ISO/IEC 27034 series can be found on the ISO website.

Introduction

0.1 General

A systematic approach to integrate security controls throughout the engineering lifecycle provides an organization with evidence that information being used or stored by its applications is being adequately protected.

The ISO/IEC 27034 series assists organizations in integrating security throughout the life cycle of their applications by providing frameworks and processes scoped at organization and application levels.

This document defines the processes required for managing the security of an application identified as processing critical information by the organization.

Table 1 — ISO/IEC 27034 Framework overview

Scope	ISO/IEC 27034 framework	What it represents
Organization	Organization Normative Framework (ONF)	One centralized repository of application security information
	ONF Management process	Process is in place to maintain and continuously improve ONF
Application	Application Normative Framework (ANF)	Repository for all ASCs of an application
	Application Security Management Process	A risk based process that uses the ANF to build and validate applications

As shown in Table 1, organization-level framework and process are provided by the Organization Normative Framework (ONF). The ONF, its elements and supporting processes are defined in ISO/IEC 27034-2.

Application-level framework and processes are provided by this document in Clauses 5, 6 and 7. The Application Security Management Process (ASMP) helps a project team apply relevant portions of the ONF to a specific application project and formally record evidence of the outcomes in an Application Normative Framework (ANF).

Processes for determining the application requirements and environment are included in 6.1 to 6.5. Subclause 6.1 addresses the identification of the application requirements and its environment, assessing the application security risks. Evaluating the application's Targeted Level of Trust is addressed in 6.2, creating and maintaining the ANF and Application Security Controls (ASCs) is covered in 6.3, and processes pertaining to realizing and operating the application are included in 6.4. Finally, 6.5 presents a process to verify that the ANF and the ASCs are properly implemented.

0.2 Purpose

The purpose of this document is to provide requirements and guidance for the Application Security Management Process and the Application Normative Framework.

0.3 Targeted audience

0.3.1 General

Although this document provides best practices for a general audience, it is especially useful for the following actors:

a) managers;

b) provisioning and operation team;

c) acquirers;

d) suppliers;

e) auditors;

f) users.

0.3.2 Managers

Managers are persons involved in the management of an application. Examples of managers are:

a) information security managers including the Chief Information Security Officer (CISO);

b) project managers;

c) product line managers;

d) development managers;

e) application owners;

f) line managers including the Chief Information Officer (CIO), who supervise employees.

Typically, managers need to:

a) ensure that any application projects, initiatives or processes are based on the results of risk management;

b) make sure that certain proper information security clearances are in place as required by applicable information security policies and procedures;

c) manage the implementation of a secure application;

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

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

f) ensure compliance with standards, laws and regulations according to an application's regulatory context;

g) ensure the documentation of security policies and procedures for the application;

h) stay abreast of all application-related security plans throughout the organization's network;

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

j) authorize the targeted level of trust according to the context specific to the organization;

k) periodically review the applications for security weaknesses and threats and take corrective and preventive actions;

l) review auditor reports recommending application acceptance or rejection based on proper implementation of required application security controls;

m) ensure that security flaws are prevented through secure coding practices;

n) base their decisions on lessons learned derived from knowledge base records.

0.3.3 Provisioning and operation team

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

a) architects;

b) analysts;

c) programmers;

d) testers;

e) IT administrators, such as system administrators, database administrators, network administrators, and application administrators.

Typically, members need to:

a) understand which application security 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;

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

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

c) select suppliers that comply with such requirements;

d) verify evidence of security controls applied by outsourcing services;

e) 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;

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;

d) apply standardized audit processes based on the use of verifiable evidence, according to ISO/IEC 27034 (all parts).

0.3.7 Users

Users are persons who need to trust that:

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

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

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

Information technology — Application security —

Part 3: Application security management process

1 Scope

This document provides a detailed description and implementation guidance for the Application Security Management Process.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27034-1, *Information technology — Security techniques — Application security — Part 1: Overview and concepts*

ISO/IEC 27034-2, *Information technology — Security techniques — Application security — Part 2: Organization normative framework*

ISO/IEC 27034-5, *Information technology — Security techniques — Application security — Part 5: Protocols and application security controls data structure*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27034-1, ISO/IEC 27034-2, and ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
application security audit
AS audit
systematic, independent and documented process for obtaining audit evidence from the verification of application security activities, and evaluating it objectively to determine the extent to which the audit criteria required by an application security authority are fulfilled

3.2
application security verification
process of reviewing and verifying security activity outcomes by performing the associated verification-measurement activity

Note 1 to entry: For an organization, required ONF elements and security activities meet ONF specifications and are compliant with ONF management process.

Note 2 to entry: For an application, a security activity and its associated verification-measurement activity may be part of an ASC.

3.3
critical information
information which, if compromised, can result in an unacceptable risk

3.4
domain expert
person who is an expert in a particular domain, area or topic

3.5
risk management
coordinated activities to direct and control an organization with regard to risk

Note 1 to entry: This document uses the term "process" to describe risk management overall. The elements within the risk management process are termed "activities".

[SOURCE: ISO Guide 73:2009, 2.1]

4 Abbreviated terms

AS	Application Security
ASC	Application Security Control
ASMP	Application Security Management Process
ANF	Application Normative Framework
ASLCRM	Application Life Cycle Security Reference Model
ONF	Organization Normative Framework

5 Application Security Management Process

5.1 General

The Application Security Management Process (ASMP) is the overall process for managing security on each specific application used or developed by an organization.

The ONF Committee is responsible for implementing and maintaining the ASMP by use of the ONF management process (see ISO/IEC 27034-2:2015, 5.4.3). This committee is also responsible for ensuring that the ASMP is applied to all application projects in the organization.

The Application owner is accountable for ensuring an ASMP is in place for the application project (see Table 3).

For each application project, the project manager is responsible for implementing and using the ASMP in the course of the project (see Table 3).

The Application Security Management Process is performed in five steps:

a) identifying the application requirements and environment;

b) assessing application security risks;

c) creating and maintaining the Application Normative Framework;

d) provisioning and operating the application;

e) auditing the security of the application.

The first 3 steps of the ASMP are focused on identifying and recording appropriate application security controls (ASCs) for an application. Considering that security up front is a fundamental aspect of application security, the optimal point to define security requirements for a software project is during the initial planning stages. This early definition of requirements allows project teams to identify key milestones and deliverables, and permits the integration of security in a way that minimizes any disruption to plans and schedules.

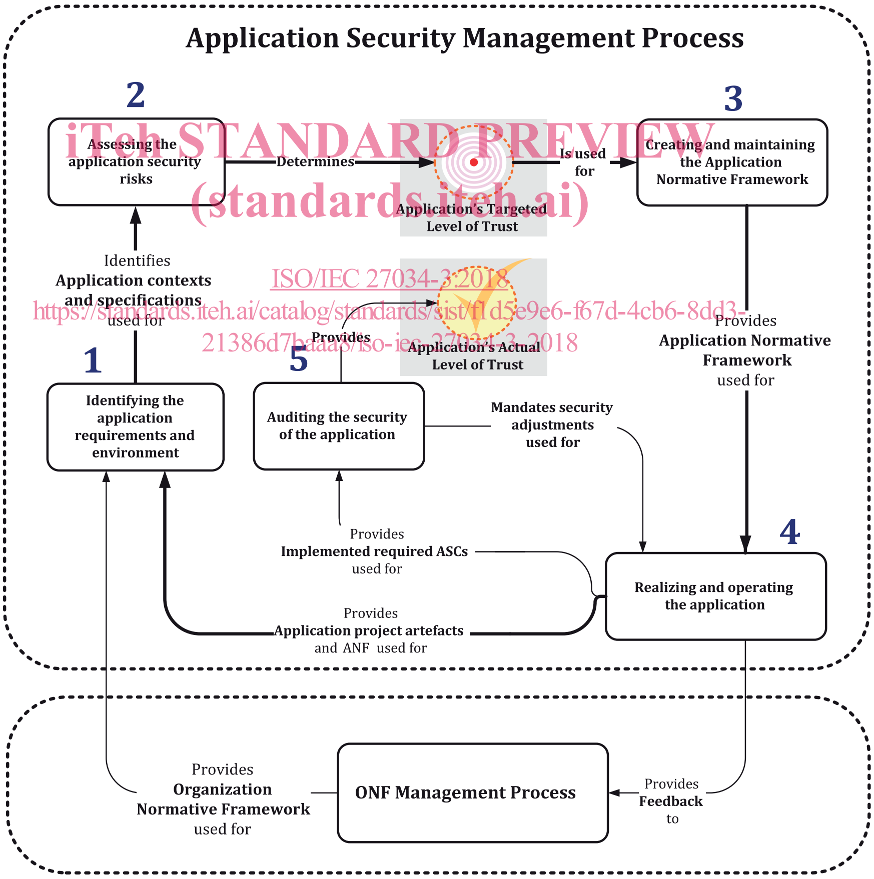
The last 2 steps of the ASMP are focused on implementation and verification of ASCs.

ISO/IEC 27034 (all parts) provides components, processes and frameworks that help an organization to acquire, implement and use applications it can trust, at an acceptable security cost determined by the organization. Moreover specifically, these components, processes and frameworks provide demonstrable evidence that applications reach and maintain a targeted level of trust.

As shown in Figure 1, these components, processes and frameworks are part of two overall processes:

a) the ONF Management Process;

b) the Application Security Management Process (ASMP).


Application Security Management Process
2
Assessing the application security risks
Determines
Application's Targeted Level of Trust
Is used for
3
Creating and maintaining the Application Normative Framework
Identifies Application contexts and specifications used for
Provides Application Normative Framework used for
Provides
Application's Actual Level of Trust
1
Identifying the application requirements and environment
5
Auditing the security of the application
Mandates security adjustments used for
4
Provides Implemented required ASCs used for
Realizing and operating the application
Provides Application project artefacts and ANF used for
Provides Organization Normative Framework used for
ONF Management Process
Provides Feedback to

Key

⬚	group	▢	process
▨	element	→	action

Figure 1 — Application Security Management Process

These two processes are used at different levels and time frames in the organization and have different scopes. The ONF Management Process (see ISO/IEC 27034-2) is a continuous organizational-level process and the ASMP is used for managing security on each specific application project.

5.2 Purpose

The Application Security Management Process allows an organization to manage security for each application it uses.

5.3 Principles and concepts

5.3.1 General

In addition to principles introduced in ISO/IEC 27034-1, organizations creating, operating or maintaining applications should be guided by the following principles:

a) every application should be assigned a Targeted Level of Trust;

b) any security component or process used in an application project should be selected from the ONF;

c) all ASCs selected with the Targeted Level of Trust should be implemented, verified and audited.

5.3.2 Clearly communicate roles and responsibilities

This document uses RACI charts for assigning roles and responsibilities for carrying out activities in processes. Such charts identify actors responsible, accountable, consulted or informed for the realization of an activity. Abbreviations are used for describing responsibilities of actors. Those are enumerated in Table 2.

Table 2 — Abbreviations for responsibilities used in RACI charts

Code	Responsibility
R	Responsible for the realization of an activity
A	Accountable for the realization of an activity
C	Consulted during the realization of an activity
I	Informed of the realization of an activity

Use of RACI charts within an organization implementing this document is not required. Organizations should align guidance provided in this document with their own method of clarifying roles and responsibilities.

When conducting realization and verification activities, it is critical for organizations to determine the resources that are responsible, accountable, consulted, and are informed. Table 2 provides a starting point for discussion during the realization of an ANF.

5.3.3 Relationship of the ASMP with the Organizational Normative Framework (ONF)

The ONF, which is covered in detail in ISO/IEC 27034-2, provides an organization-level context for the ASMP. This context includes all processes involved in application security, as well as regulations, laws, best practices, roles, and responsibilities accepted by the organization. The ASMP uses this context to create and maintain the Application Normative Framework (ANF) for each application project. In return, the ASMP supports continual improvement of the ONF through feedback of new knowledge, application security control improvement suggestions and practices gained in the course of an application's development and deployment.

5.3.4 Use approved tools

Project teams should take advantage of new security analysis functionality and protections by leveraging approved tools and their associated security checks, such as compiler/linker options and warnings. A list of approved tools should be provided as part of the Organization Normative Framework. If the project team is aware of a tool that exceeds what is currently outlined in the ONF's approved list, it should use the ONF's feedback process to inform the ONF Committee about the tool.

NOTE The description, purpose and role of the ONF committee is described in ISO/IEC 27034-2:2015, 5.4.3.

5.3.5 Level of Trust

A "Level of Trust" is a label that identifies a set of applicable ASCs from the Application Security Control Library in the ONF. The ISO/IEC 27034 framework proposes two types of Levels of Trust that can be associated with an application:

a) Targeted Level of Trust;

b) Actual Level of Trust

The Targeted Level of Trust should be derived using an organizationally relevant implementation of the risk management process outlined in ISO/IEC 27005.

5.3.6 Application's Targeted Level of Trust

Applicable security controls for a Targeted Level of Trust can either be pre-defined in the ONF or be derived from a workflow that identifies the applicable controls based on the selected Level of Trust and more refined application security specifications. The workflow may leverage automation and tools, such as Secure Application Lifecycle Management systems, to make the process consistent across multiple applications.

The risk assessment process produces the security requirements from which the application's Targeted Level of Trust is derived. This in turn becomes the goal for the application's project team.

The application Targeted Level of Trust can aid in conveying a level of confidence needed by the organization so that it would be willing to use or deploy the application after accepting the residual risks determined by the risk assessment.

The application Targeted Level of Trust is vital to the security of the application because it directly determines the appropriate Application Security Controls to be selected from the ASC library and implemented in the application life cycle.

The application Targeted Level of Trust should be one of (or within the range of) the levels of trust defined in the Organization ASC Library (see ISO/IEC 27034-1:2011, 8.1.2.6), which is part of the ONF.

The ASC library (ISO/IEC 27034-1:2011, Figure 4) can be represented as a table and the application Targeted Level of Trust as a column in that table. Thus selecting a level of trust means selecting all ASCs in that column.

The following is a sample breakdown of Levels of Trust that an organization may define:

EXAMPLE 1 Business critical applications, internal applications, public applications.

EXAMPLE 2 Generic Web Public Application: Targeted Level of Trust is public applications, technology context is a web based application with a database, and business context is that the application stores and processes end user passwords.

5.3.7 Application's Actual Level of Trust

The application's Actual Level of Trust is the maximum confidence level demonstrated by the verification team according to the verification measurements of all the application's ASCs.