INTERNATIONAL STANDARD

ISO/IEC 27034-2

First edition
2015-08-15

Information technology — Security techniques — Application security —

Part 2: Organization normative framework

Technologie de l'information — Sécurité des applications —

Partie 2: Cadre normatif de l'organisation

Reference number
ISO/IEC 27034-2:2015(E)

© ISO/IEC 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Abbreviated terms ... **1**

5 Organization Normative Framework ... **2**

5.1 General ... 2
5.2 Purpose ... 2
5.3 Principles ... 2
5.4 ONF Management Process ... 2
5.4.1 General ... 2
5.4.2 Use of RACI charts in description of activities, roles and responsibilities ... 4
5.4.3 Establishing the ONF committee ... 5
5.4.4 Designing the ONF ... 6
5.4.5 Implementing the ONF ... 8
5.4.6 Monitoring and reviewing the ONF ... 10
5.4.7 Improving the ONF ... 11
5.4.8 Auditing the ONF ... 13
5.5 ONF Elements ... 15
5.5.1 General ... 15
5.5.2 Business context component ... 16
5.5.3 Regulatory context component ... 17
5.5.4 Technological context component ... 18
5.5.5 Application specifications repository ... 19
5.5.6 Roles, responsibilities and qualifications repository ... 20
5.5.7 Organization ASC Library ... 21
5.5.8 Application Security Control ... 23
5.5.9 Application Security Life Cycle Reference Model ... 26
5.5.10 Application Security Life Cycle Model ... 32
5.5.11 Application Security Management Process ... 33
5.5.12 Application Security Risk Analysis Process ... 34
5.5.13 Application Security Verification Process ... 36

Annex A (informative) **Aligning the ONF and ASMP with ISO/IEC 15288 and ISO/IEC 12207 through ISO/IEC 15026-4** ... **38**

Annex B (informative) **ONF implementation example: implementing ISO/IEC 27034 Application Security and its ONF in an existing organization** ... **42**

Bibliography ... **52**

© ISO/IEC 2015 – All rights reserved

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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *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*

— *Part 2: Organization normative framework*

The following parts are under preparation:

— *Part 3: Application security management process*

— *Part 4: Application security validation*

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

— *Part 6: Security guidance for specific applications*

— *Part 7: Application security assurance prediction*

 © ISO/IEC 2015 – All rights reserved

Introduction

General

Organizations must protect their information and technological infrastructures in order to stay in business. There is an increasing need for organizations to focus on protecting their information at the application level. A systematic approach towards improving application security provides an organization with evidence that information being used or stored by its applications is being adequately protected.

ISO/IEC 27034 provides concepts, principles, frameworks, components and processes to assist organizations in integrating security seamlessly throughout the life cycle of their applications.

The Organization Normative Framework (ONF) is the most important of those components.

The ONF is an organization-wide framework where all application security best practices recognized by the organization are stored. It comprises essential components, processes that utilize these components, and processes for managing the ONF itself. It is the foundation of application security in the organization and all the organization's future application security decisions should be made by referring to this framework. The ONF is the authoritative source for all components and processes related to application security in the organization.

This part of ISO/IEC 27034 defines the processes required to manage the security of applications in the organization. These processes are presented in 5.4. It also introduces security-related elements of applications (processes, roles and components) that should be integrated into the ONF. These elements are presented in 5.5.

Finally, this part of ISO/IEC 27034 presents the Auditing the ONF process, needed by an organization for verifying its ONF and verifying compliance of all applications with the requirements and controls in the ONF. This process is presented in 5.4.8.

Purpose

The purpose of this part of ISO/IEC 27034 is to assist organizations to create, maintain and validate their own ONF in compliance with the requirements of this International Standard.

This part of ISO/IEC 27034 is designed to enable an organization to align or integrate its ONF with the organization's enterprise architecture and/or the organization's information security management system requirements. However, implementing an information security management system as described in ISO/IEC 27001 is not a requirement for the implementation of this International Standard.

Targeted Audiences

General

The following audiences will find value and benefits when carrying their designated organizational roles:

a) managers;

b) ONF committee;

c) domain experts;

d) auditors.

Managers

Managers should read this International Standard because they are responsible for the following:

a) improving application security through the ONF and other aspects of ISO/IEC 27034;

b) ensuring the ONF stays aligned with the organization's information security management system and application security needs;

© ISO/IEC 2015 – All rights reserved

c) leading the establishment of the ONF in the organization;

d) ensuring the ONF is available, communicated and used in application projects with proper tools and procedures all across the organization;

e) determining the appropriate level(s) of management that the ONF Committee reports to.

ONF Committee

The ONF Committee is responsible for managing the implementation and maintenance of the application-security-related components and processes in the Organization Normative Framework. The ONF Committee needs to

a) manage the cost of implementing and maintaining the ONF,

b) determine what components and processes should be implemented in the ONF,

c) make sure introduced components and processes respect the organization's priorities for security requirements,

d) review auditor reports for acceptance or rejection that the ONF conforms to this International Standard and meets the organization's requirements,

e) provide processes and tools for managing compliance with standards, laws and regulations according to the regulatory context of the organization,

f) communicate security awareness, training and oversight to all actors, and

g) promote compliance with the ONF for all application projects throughout the organization.

ONF development team

Experts who have been assigned by the ONF Committee with the task of developing and implementing one or more ONF element(s), who need to

a) develop and implement a designed ONF element,

b) determine training in the use of ONF elements by its different actors, and

c) collaborate in providing adequate training to actors.

Domain experts

Provisioning, operation, acquisition and audit experts who need to

a) participate in ONF implementation and maintenance,

b) validate that the ONF is useable and useful in the course of an application project, and

c) propose new components and processes.

Auditors

Auditors are personnel performing roles in the audit processes, who need to participate in ONF validation and verification.

NOTE Auditors may be external or internal to the organization, depending on the target and circumstances of the audit, and according to the organization's audit policies and conformance requirements.

 © ISO/IEC 2015 – All rights reserved

Information technology — Security techniques — Application security —

Part 2: Organization normative framework

1 Scope

This part of ISO/IEC 27034 provides a detailed description of the Organization Normative Framework and provides guidance to organizations for its implementation.

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, *Information technology — Security Techniques — Information security management systems — Overview and vocabulary*

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

ISO/IEC 27034-1:2011, *Information technology — Security techniques — Application security — Part 1: Overview and concepts*

NOTE Additional detail about the relationship between ISO/IEC 27034 and other standards is available in ISO/IEC 27034-1:2011, 0.5.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27034-1, ISO/IEC 27000, and ISO/IEC 27005 apply.

4 Abbreviated terms

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

© ISO/IEC 2015 – All rights reserved