DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27034-4

ISO/IEC JTC **1**/SC **27** Secretariat: **DIN**

Voting begins on:
2020-01-07

Voting terminates on:
2020-03-31

Information technology — Security techniques — Application security —

Part 4:
Validation and verification

Technologies de l'information — Securité des applications —

Partie 4: Validation et vérification

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.



Reference number
ISO/IEC DIS 27034-4:2020(E)

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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 **6**

0 INTRODUCTION ..... **VII**

0.1 GENERAL VII
0.2 PURPOSE VIII
0.3 TARGETED AUDIENCE VIII
0.3.1 General ..... *viii*
0.3.2 Managers ..... *viii*
0.3.3 Application security authority ..... *ix*
0.3.4 Provisioning and operation team ..... *ix*
0.3.5 Acquirers ..... *x*
0.3.6 Suppliers ..... *x*
0.3.7 Auditors ..... *x*
0.3.8 Users ..... *x*

1 SCOPE **1**

2 NORMATIVE REFERENCES **1**

3 TERMS AND DEFINITIONS **1**

4 ABBREVIATED TERMS **5**

5 VERIFICATION SCHEME FRAMEWORK **5**

5.1 GENERAL 5
5.2 PURPOSE 6
5.3 CONCEPTS 6
5.3.1 Principles *6*
5.3.2 Application security parties for AS validation, verification and audit *7*
5.3.3 Verification Scheme Framework elements *11*
5.4 CLEARLY COMMUNICATE ROLES AND RESPONSIBILITIES 13

6 VERIFICATION SCHEME MANAGEMENT PROCESS **13**

6.1 GENERAL 13
6.2 MANAGING A VERIFICATION SCHEME AND ITS AS AUDIT PROGRAMME 14
6.2.1 General *14*
6.2.2 Establish a verification scheme *14*
6.2.3 Manage a verification scheme *21*
6.2.4 Review and maintain a verification scheme *27*
6.3 ESTABLISH AN AS CERTIFICATION 28
6.3.1 Certification decision *28*
6.3.2 Maintaining certification *28*
6.3.3 Appeal *30*
6.3.4 Complaints *30*
6.3.5 Auditee records *30*
6.4 MANAGEMENT SYSTEM REQUIREMENTS FOR CERTIFICATIONS BODIES 30
6.4.1 General *30*
6.4.2 Option A: General management system requirements *30*
6.4.3 Option B: Management system requirements in accordance with ISO 9001 ..... *30*

7 AS CERTIFICATION PROCESS **30**

7.1 GENERAL 30

© ISO/IEC 2019 – All rights reserved

7.2 PRE-CERTIFICATION ACTIVITIES 30
7.2.1 Application 30
7.2.2 Application review 30
7.2.3 Analyse the Audit programme form the verification scheme 31
7.2.4 Scheduling audit 31
7.2.5 Multiple management verification scheme or systems standards (take into account the) 31
7.2.6 Conducting auditor evaluation 31
7.3 PLANNING AUDITS 31
7.3.1 Audit team assignments 31
7.3.2 Audit plan 31
7.4 INITIAL CERTIFICATION 31
7.4.1 Initial certification audit 31
7.5 MANAGING AUDIT 31
7.5.1 Cause analysis of nonconformities 32
7.5.2 Effectiveness of corrections and corrective actions 32
7.5.3 Final audit report and recommendation 32
7.6 SENDING THE AUDIT REPORT TO THE AS AUTHORITY 32

8 AS AUDIT PROCESS 32

8.1 GENERAL 32
8.2 INITIATING THE AS AUDIT 32
8.2.1 Purpose 32
8.2.2 Outcomes 33
8.2.3 Realization activities 33
8.2.4 Guidance 33
8.3 STAGE 1: PREPARING AS AUDIT ACTIVITIES 34
8.3.1 Purpose 34
8.3.2 Outcomes 34
8.3.3 Realization activities 34
8.3.4 Guidance 34
8.4 STAGE 2: CONDUCTING THE AUDIT ACTIVITIES 37
8.4.1 Purpose 37
8.4.2 Outcomes 37
8.4.3 Realization activities 37
8.4.4 Guidance 37
8.5 MAINTAINING AND IMPROVING AUDITOR COMPETENCE 44

9 CERTIFICATION SCHEMES FOR AS EXPERTS 44

9.1 GENERAL 44
9.2 CERTIFICATION SCHEMES FOR AS LEAD IMPLEMENTER 44
9.2.1 General 44
9.2.2 Purpose 44
9.2.3 Knowledge 44
9.2.4 Knowledge skills 45
9.3 CERTIFICATION SCHEMES FOR AS LEAD AUDITOR 45
9.3.1 General 45
9.3.2 Purpose 45
9.3.3 Knowledge 45
9.3.4 Knowledge skills 46
9.4 REQUIREMENTS FOR CERTIFICATION BODIES 46

10 VERIFICATION SCHEME 47

10.1 GENERAL 47
10.2 AS AUDIT PROGRAMME 48
10.2.1 General 48
10.2.2 Evaluation criteria 48
10.2.3 Verification scheme 49
10.2.4 Tailoring 49
10.3 ORGANIZATION NORMATIVE FRAMEWORK (ONF) 50
10.3.1 General 50

© ISO/IEC 2019 – All rights reserved

10.3.2 ONF Committee Management process *51*
10.3.3 ONF Management process *51*
10.3.4 Application Security Risk Management process *51*
10.3.5 Application Security Management process *51*
10.3.6 Other process or activity required *51*
10.3.7 Application Security Controls Repository (ASC) *51*
10.3.8 ASC Library *51*
10.3.9 Application Security Traceability Matrix *51*
10.3.10 Business context *51*
10.3.11 Regulatory context *51*
10.3.12 Technological context *51*
10.3.13 Application specifications and functionalities repository *51*
10.3.14 Categorized information groups repository *51*
10.3.15 Roles, responsibilities and qualifications repository *51*
10.3.16 Application Security Life Cycle Model *51*
10.3.17 Application Security Life Cycle Reference Model *51*
10.3.18 AS Verification Process *51*
10.3.19 Application Normative Framework (ANF) *51*
10.4 QUALIFICATION SCHEMES FOR APPLICATION SECURITY EXPERTS 53
10.5 EXPECTED AS AUDIT OUTCOMES 53
10.5.1 AS Audit report summary *53*
10.5.2 Detailed AS Audit report *53*

ANNEX A (INFORMATIVE) EXAMPLE OF A VERIFICATION SCHEME FOR AN ORGANIZATION 54

A.1 HOW TO USE THIS ANNEX 54
A.2 VERIFICATION SCHEME IDENTIFICATION 54
A.3 APPLICATION SECURITY AUDIT PROGRAMME DESCRIPTION 54
A.3.1 Audit programme objective *54*
A.3.2 Audit programme elements *54*
A.3.3 Audit programme implementation *54*
A.4 VERIFICATION SCHEME ELEMENTS 55
A.4.1 Organisation identification *55*
A.4.2 Required ONF committee elements *55*
A.4.3 Required ONF Management process *55*
A.4.4 Required ONF Processes *55*
A.4.5 Required ONF Components *55*
A.5 GUIDANCE 56

ANNEX B (INFORMATIVE) EXAMPLE OF A VERIFICATION SCHEME FOR AN APPLICATION 57

B.1 HOW TO USE THIS ANNEX 57
B.2 VERIFICATION SCHEME IDENTIFICATION 57
B.3 APPLICATION SECURITY AUDIT PROGRAMME DESCRIPTION 57
B.3.1 Audit programme objective *57*
B.3.2 Audit programme elements *57*
B.3.3 Audit programme implementation *57*
B.4 VERIFICATION SCHEME ELEMENTS 58
B.4.1 Application identification (auditee) *58*
B.4.2 Required application project team members *58*
B.4.3 Required processes related to the security of the application *58*
B.4.4 Required ONF Processes *58*
B.4.5 Required ANF Components *59*
B.5 GUIDANCE 59

ANNEX C (INFORMATIVE) KNOWLEDGE FOR AS LEAD IMPLEMENTER CERTIFICATION 60

ANNEX D (INFORMATIVE) KNOWLEDGE FOR AS LEAD AUDITOR CERTIFICATION 61

BIBLIOGRAPHY 62

© ISO/IEC 2019 – All rights reserved

Figures

Page

Figure 1 – Parties and components involved in application security validation and verification processes....8

Figure 2 – Verification Scheme Framework....12

Figure 3 – Managing a verification scheme and its AS audit programme....14

Figure 4 – Typical application security audit activities....32

Figure 5 – Overview of the process of collecting and verifying information....40

Figure 6 – Application Security Life Cycle Reference Model....47

Figure 7 – Organization Normative Framework – simplified graphical representation....50

Figure 8 – Application Normative Framework....52

Tables

Page

Table 1 – ISO/IEC 27034 (all parts) frameworks.... vii

Table 2 – Abbreviations for responsibilities used in RACI charts....13

Table 3 – RACI chart for process “Managing a verification scheme and its AS audit programme”....15

Table 4 – RACI chart for process “Manage a verification scheme”....21

Table 5 – RACI chart for process “Review and maintain a verification scheme”....27

Table 6 — RACI chart for process “Initiating the AS audit”....33

Table 7 — RACI chart for process “Stage 1: Preparing as audit activities”....34

Table 8 — RACI chart for process “Stage 2: Conducting the audit activities”....37

Table A.1 Table of knowledge related to AS Implementation....60

Table A.2 Table of knowledge related to AS Audit....61

© ISO/IEC 2019 – 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 must 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 World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

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

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

© ISO/IEC 2019 – All rights reserved

0 Introduction

0.1 General

ISO/IEC 27034 (all parts) Application Security proposes framework elements, including roles, processes and components that could be implemented in an organization and/or in an application to improve application security. Not all organizations or applications are the same and the ISO/IEC 27034 (all parts) frameworks may be implemented in different ways to address different specific security requirements. If no guidance is provided by the ISO/IEC 27034 (all parts) frameworks, how can application security verification and audits be performed and declared successful?

This document defines processes and elements required for managing, validating and verifying how the ISO/IEC 27034 (all parts) frameworks were implemented to enforce application security.

Table 1 – ISO/IEC 27034 (all parts) frameworks

Part	Scope	ISO/IEC 27034 Framework	What it represents
27034-2	**Organization**	Organization Normative Framework (ONF)	A centralized repository of pre-approved and reusable application security elements, used as an authoritative source of information by the organization.
		ONF management process	A process to maintain and continuously improve required ONF elements to protect the organization's sensitive information involved by the use of applications.
27034-3	**Application**	Application Normative Framework (ANF)	A repository for all processes, Application Security Controls (ASCs), reports and other outcomes related to an application.
		Application security management process	A risk-based process that uses the ANF to build, support and operate secure applications.
27034-4	**Organization & Application**	Verification Scheme Framework (VSF)	Repository for processes and components used to define and perform measurable and repeatable application security verifications and audits.
		Application Security Validation and Verification Process	Group of processes and frameworks used to build, validate, verify and maintain a verification scheme and conduct application security validations, verifications, and audits based on its requirements.
27034-7	**Application Security Control** (ASC)	Assurance Prediction Framework	A set of processes and components used to define a Prediction Application Security Rationale (PASR) that will replace an ASC for a specific application, and provide context for this prediction.
		Assurance Prediction Management Process	A risk-based process to replace an ASC with a PASR in order to reduce an application’s security cost and expect to maintain the same security level.

© ISO/IEC 2019 – All rights reserved

Organization-level frameworks and processes are provided by the Organization Normative Framework (ONF). The ONF, its elements and supporting processes are defined in ISO/IEC 27034-2.

Application-level frameworks and processes are provided by ISO/IEC 27034-3: Application Security Management Process (ASMP). The ASMP helps a project team apply relevant portions of the ONF to a specific application project and formally record evidence of the processes in an ANF.

AS validation, verification and audit-level frameworks and processes are provided by ISO/IEC 27034-4: Application security validation and verification process. This framework helps organizations and relevant authorities to measure and verify application security compliance of applications and organizations.

0.2 Purpose

The purpose of this document is to provide guidance and requirements for the Application Security validation, verification and audit processes implementation, i.e. to help the organization to perform a repeatable demonstration that a verification scheme's requirements were met.

EXAMPLE 1 Demonstrate that a specific verification scheme was validated and approved by an Application Security (AS) authority and its elements are clear, complete, measurable and verifiable.

EXAMPLE 2 Demonstrate that a specific application's Actual Level of Trust (LoT) equals or exceeds the Targeted LoT required in the verification scheme.

EXAMPLE 3 Demonstrate that an organization is addressing and managing the security of its applications as required in the verification scheme.

0.3 Targeted audience

0.3.1 General

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

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;

b) project managers;

c) administrators;

d) certification body;

e) audit client;

© ISO/IEC 2019 – All rights reserved

f) development managers;

g) application owners;

h) line managers, who supervise employees.

Typically managers need to:

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

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

c) manage the audit or the implementation of a secure application;

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

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

f) base their decisions on lessons learned derived from knowledgebase records.

0.3.3 Application security authority

Application security authority (AS authority) are individuals or organizations who wish to use a verification scheme to define and receive evidence that significant security risks have been mitigated to acceptable levels. Examples of AS authority are:

a) governments and regulators, that want to enforce laws or regulations;

b) organizations recognized as authorities in their business sector that want to enforce best practices;

c) contracting parties or potential clients;

d) internal verification groups;

e) etc.

0.3.4 Provisioning and operation team

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

a) architects;

b) analysts;

c) programmers;

d) testers;

e) system integration engineers;

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

© ISO/IEC 2019 – All rights reserved

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

d) obtain access to tools and best practices in order to streamline development, testing and documentation.

0.3.5 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.

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

0.3.7 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 LoT as required by management;

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

0.3.8 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 while protecting the confidentiality of the data;

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

© ISO/IEC 2019 – All rights reserved

Information technology — Security techniques — Application security — Part 4: Validation and verification

1 Scope

This document provides a detailed description of an application security process to develop, validate, implement, verify, and continuously improve verification schemes used to audit and verify application security in an organization.

Application security validation can be done on a verification scheme to validate and verify if it clearly defines clear AS requirements and AS controls to mitigate all risks to acceptable levels and reach application security objectives for specific contexts and environments.

Application security verification and audit can be done on an organization or an application, to verify if it complies with a verification scheme.

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 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 27034-3, Information technology — Security techniques — Application security — Part 3: Application Security Management Process

ISO/IEC 17021-1 Conformity assessment — Requirements for bodies providing audit and certification of management systems, part 1

ISO/IEC 19011:2018, Guidelines for auditing management systems

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27034-1, ISO/IEC 27034-2, ISO/IEC 27000, (ISO/IEC 27005 if needed) *ISO/IEC 19011:2018, ISO/IEC 17021:2015, ISO/IEC 17024:2012, ISO/IEC 17000, ISO/IEC 17025:2017 and* the following apply:

3.1
accreditation body

authoritative body that performs accreditation

3.2
application security
AS

protection of information and/or underlying system implied by the provisioning and the operation of an application

© ISO/IEC 2019 – All rights reserved