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)

COPYRIGHT PROTECTED DOCUMENT

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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **2**
5 Application Security Management Process **2**
5.1 General 2
5.2 Purpose 4
5.3 Principles and concepts 4
5.3.1 General 4
5.3.2 Clearly communicate roles and responsibilities 4
5.3.3 Relationship of the ASMP with the Organizational Normative Framework (ONF) 4
5.3.4 Use approved tools 5
5.3.5 Level of Trust 5
5.3.6 Application's Targeted Level of Trust 5
5.3.7 Application's Actual Level of Trust 5
5.3.8 Impact of this document on an application project 6
6 ASMP steps **7**
6.1 Identifying the application requirements and environment 7
6.1.1 General 7
6.1.2 Purpose 8
6.1.3 Outcomes 8
6.1.4 Realization activities 8
6.1.5 Verification activities 9
6.1.6 Guidance 9
6.2 Assessing application security risks 11
6.2.1 General 11
6.2.2 Purpose 12
6.2.3 Outcomes 12
6.2.4 Realization activities 12
6.2.5 Verification activities 13
6.2.6 Guidance 13
6.3 Creating and maintaining the Application Normative Framework 21
6.3.1 General 21
6.3.2 Purpose 22
6.3.3 Outcomes 22
6.3.4 Realization activities 22
6.3.5 Verification activities 23
6.3.6 Guidance 23
6.4 Provisioning and operating the application 24
6.4.1 General 24
6.4.2 Purpose 25
6.4.3 Outcomes 26
6.4.4 Realization activities 26
6.4.5 Verification activities 26
6.4.6 Guidance 27
6.5 Auditing the security of the application 27
6.5.1 General 27
6.5.2 Purpose 28
6.5.3 Outcomes 28
6.5.4 Realization activities 29

6.5.5 Verification activities 29
6.5.6 Guidance 29

7 ANF elements 31
7.1 General 31
7.1.1 Purpose 31
7.1.2 Description 31
7.2 Component: Application business context 32
7.2.1 Purpose 32
7.2.2 Description 32
7.2.3 Contents 32
7.2.4 Guidance 33
7.3 Component: Application regulatory context 33
7.3.1 Purpose 33
7.3.2 Description 33
7.3.3 Contents 33
7.3.4 Guidance 33
7.4 Component: Application technological context 34
7.4.1 Purpose 34
7.4.2 Description 34
7.4.3 Contents 34
7.4.4 Guidance 34
7.5 Component: Application specifications 35
7.5.1 Purpose 35
7.5.2 Description 35
7.5.3 Contents 35
7.5.4 Guidance 35
7.6 Component: Application's actors: roles, responsibilities and qualifications 36
7.6.1 Purpose 36
7.6.2 Description 36
7.6.3 Contents 36
7.6.4 Guidance 38
7.7 Component: Selected ASCs for the application's life cycle stages 38
7.7.1 Purpose 38
7.7.2 Description 39
7.7.3 Contents 39
7.7.4 Guidance 39
7.8 Processes related to the security of the application 39
7.8.1 Purpose 39
7.8.2 Description 39
7.8.3 Contents 39
7.8.4 Guidance 40
7.9 Component: Application life cycle 40
7.9.1 Purpose 40
7.9.2 Description 40
7.9.3 Contents 40
7.9.4 Guidance 40
7.10 Information involved by the application 40
7.10.1 Purpose 40
7.10.2 Description 41
7.10.3 Contents 41
7.10.4 Guidance 41

Annex A (informative) **Guidance text related to the ASMP step: (6.4) Realizing and operating the application 45**

Bibliography 47

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.

国际标准

ISO/IEC 27034-3

初版 2018
年 5 月

信息技术 - 应用程序安全 - 部分3：安全管理流程

信息技术 - 应用程序安全 - 第 3 部分:应用程序安全的管理流程

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

目录

页

前言 ..... **v**

引言 ..... **六**

1 范围。1

2 规范性引用文件1

3 术语和定义 **1**

4 缩略语 **2**

5 应用程序安全管理流程 **2**

5.1 总则2

5.2 目的 4

5.3 原则与概念 4

5.3.1 一般 4

5.3.2 明确沟通角色和职责。4

5.3.3 高级战略管理流程（ASMP）与组织规范框架（ONF）的关系。4

5.3.4 使用经批准的工具。5

5.3.5 信任程度 5

5.3.6 应用程序的目标信任级别 5

5.3.7 应用程序的实际信任级别 5

5.3.8 本文件对申请项目的影响 6

6 ASMP 步骤 **7**

6.1 确定应用程序需求和环境 7

6.1.1 一般 7

6.1.2 目的 8

6.1.3 成果/结果/成效 8

6.1.4 实现活动 8

6.1.5 验证活动9

6.1.6 指导；指引；辅导；引导9

6.2 评估应用程序的安全风险 11

6.2.1 一般 11

6.2.2 目的 12

6.2.3 成果/结果/成效 12

6.2.4 实现活动 12

6.2.5 验证活动13

6.2.6 指导；指引；辅导13

6.3 创建和维护应用程序规范框架 21

6.3.1 一般 21

6.3.2 目的 22

6.3.3 成果/结果/成效 22

6.3.4 实现活动 22

6.3.5 验证活动23

6.3.6 指导；指引；辅导23

6.4 应用程序的配置与运行 24

6.4.1 一般 24

6.4.2 目的 25

6.4.3 成果/结果/成效 26

6.4.4 实现活动 26

6.4.5 验证活动26

6.4.6 指导；指引；辅导27

6.5 对应用程序的安全性进行审计 27

6.5.1 一般 27

6.5.2 目的 28

6.5.3 成果/结果/成效 28

6.5.4 实现活动 29

6.5.5 验证活动29
6.5.6 指导；指引；辅导29
7 ANF 元素 31
7.1 总则 31
7.1.1 目的 31
7.1.2 描述： 31
7.2 组件：应用业务环境 32
7.2.1 目的 32
7.2.2 描述： 32
7.2.3 目录 32
7.2.4 指导；指引；辅导33
7.3 组件：应用监管环境 33
7.3.1 目的 33
7.3.2 描述： 33
7.3.3 目录 33
7.3.4 指导；指引；辅导33
7.4 组件：应用技术背景 34
7.4.1 目的 34
7.4.2 描述： 34
7.4.3 目录 34
7.4.4 指导；指引；辅导34
7.5 组件：应用程序规格说明 35
7.5.1 目的 35
7.5.2 描述： 35
7.5.3 目录 35
7.5.4 指导；指引；辅导35
7.6 组件：应用程序的参与者：角色、职责和资质要求 36
7.6.1 目的 36
7.6.2 描述： 36
7.6.3 目录 36
7.6.4 指导；指引；辅导38
7.7 组件：为应用程序生命周期各阶段所选的 ASC（应用程序服务组件） 38
7.7.1 目的 38
7.7.2 描述： 39
7.7.3 目录 39
7.7.4 指导；指引；辅导39
7.8 与应用程序安全相关的流程 39
7.8.1 目的 39
7.8.2 描述： 39
7.8.3 目录 39
7.8.4 指导；指引；辅导40
7.9 组件：应用程序生命周期40
7.9.1 目的 40
7.9.2 描述： 40
7.9.3 目录 40
7.9.4 指导；指引；辅导40
7.10 申请所涉及的信息 40
7.10.1 目的 40
7.10.2 描述： 41
7.10.3 目录 41
7.10.4 指导；指引；辅导41
附录 A（资料性）与 ASMP 步骤相关的指导文本：（6.4）实现和操作应用程序 45
参考文献 47

前言

国际标准化组织（ISO）和国际电工委员会（IEC）构成了全球标准化的专业体系。作为 ISO 或 IEC 成员的各国机构通过各自组织为处理特定技术领域而设立的技术委员会参与国际标准的制定。ISO 和 IEC 的技术委员会在共同感兴趣的领域开展合作。其他国际组织，无论是政府的还是非政府的，通过与 ISO 和 IEC 的联络，也参与相关工作。在信息技术领域，ISO 和 IEC 共同成立了一个联合技术委员会。

国际标准化组织/国际电工委员会第 1 联合技术委员会。

ISO/IEC 指令第 2 部分的编辑规则（见 www.iso.org/directives）。

本文件的编制程序以及其后续维护所采用的程序在 ISO/IEC 指令第 1 部分中有详细说明。尤其应注意不同类型的文件所需的不同批准标准。本文件的起草遵循了 ISO/IEC 指令第 2 部分的编辑规则（见 www.iso.org/directives）。

请注意，本文件的某些内容可能受专利权约束。国际标准化组织（ISO）和国际电工委员会（IEC）不对识别任何此类专利权的责任负责。在文档开发过程中识别出的任何专利权详情将在其中列出。

本文件中提及的任何商标名称仅为方便用户而提供，并非暗示任何专利权声明或其与 ISO 标准的关系。有关收到的专利声明列表，请参阅 ISO 网站（www.iso.org/patents）。

关于 ISO 特定术语和表达的含义，以及有关 ISO 遵守的世界贸易组织（WTO）技术性贸易壁垒（TBT）原则的自愿性，请参阅以下网址：www.iso.org/iso/foreword.html。

引言

0.1 总则

在整个工程生命周期中采取系统的方法来整合安全控制措施，能够为组织提供证据，证明其应用程序所使用或存储的信息得到了充分的保护。

受保护

通过提供组织层面和应用层面的框架及流程来支持应用程序。本文件定义了管理被认定为具有特定安全要求的应用程序所需的过程。

ISO/IEC 27034 系列标准帮助组织在其产品的整个生命周期中全面整合安全措施。

该组织处理关键信息。

表 1 - ISO/IEC 27034 框架概述

范围	ISO/IEC 27034 框架	它所代表的
组织	组织规范框架（ONF）	一个集中的应用程序安全信息库
	ONF 管理流程	已建立流程以维持并持续改进 ONF。
应用程序	应用规范框架（ANF）	应用程序所有 ASC 的存储库
	应用程序安全管理流程	一种基于风险的流程，利用 ANF 进行构建并验证应用程序

如表 1 所示，组织层面的框架和流程由组织规范框架（ONF）提供。ONF 及其要素和支撑

0.3.4 收购方

这包括所有参与获取产品或服务的人员。

通常，收购方需要：

a) 建立业务关系以获取所需的商品和服务（例如，为招标、评估和授予合同）；

b) 准备包含安全控制要求的招标书；

c) 选择符合此类要求的供应商；

d) 核实外包服务所应用的安全控制措施的证据；

e) 通过验证应用安全控制措施正确实施的证据来评估产品。

0.3.5 供应商

这包括所有参与提供产品或服务的人员。

通常供应商需要：

a) 符合招标书中提出的应用程序安全要求；

b) 选择适合提案的应用程序安全控制措施，同时考虑其对成本的影响；

c) 提供证据，证明拟提供的产品或服务已正确实施了所需的安全控制措施。

0.3.6 审计员

审计员需要做到：

a) 了解相应控制措施的验证测量所涉及的范围和程序；

b) 确保审计结果具有可重复性；

c) 建立一份验证测量清单，这些测量能产生证据表明某应用程序已达到预期的信任级别；

d) 应根据 ISO/IEC 27034（所有部分）的要求，采用基于可验证证据的标准化审计流程。

0.3.7 用户

用户需要相信以下几点：

a) 认定使用或部署某个应用程序是安全的；

b) 一个应用程序能够持续稳定且及时地生成可靠的结果；

c) 控制装置及其相应的验证测量装置已正确就位并正常运行，符合预期。

信息技术 - 应用程序安全 –
第三部分：应用程序安全管理流程

1 范围

本文件提供了应用程序安全管理流程的详细说明和实施指南。

2 规范性引用文件

文中提及的下列文件，其部分或全部内容构成本文件的要求。对于有日期的引用文件，仅所引用的版本适用。对于无日期的引用文件，适用所引用文件的最新版本（包括任何修订）。

ISO/IEC 27000 信息技术 安全技术 信息安全管理体系 概述和术语

ISO/IEC 27034-1《信息技术 安全技术 应用程序安全 第 1 部分：概述和概念》

ISO/IEC 27034-2《信息技术 安全技术 应用程序安全 第 2 部分：组织规范框架》

ISO/IEC 27034-5 信息技术 - 安全技术 - 应用程序安全 - 第 5 部分：协议和应用程序安全控制数据结构

3 术语和定义

就本文件而言，ISO/IEC 27034-1、ISO/IEC 27034-2、ISO/IEC 27000 中给出的术语和定义以及以下内容适用。

国际标准化组织（ISO）和国际电工委员会（IEC）在以下网址维护用于标准化工作的术语数据库：

— 国际标准化组织在线浏览平台：访问网址为 https://www.iso.org/obp

— 国际电工委员会电工术语在线词典：访问网址 https://www.electropedia.org/

3.1
应用程序安全审计
内部审计
一种系统化、独立且有文件记录的过程，用于从应用程序安全活动的验证中获取审计证据，并客观地对其进行评估，以确定应用程序安全机构所要求的审计标准得到满足的程度。

3.2
应用程序安全验证
通过执行相关的验证测量活动来审查和核实安全活动结果的过程

注 1：对于一个组织而言，所需的 ONF 要素和安全活动应符合 ONF 规范，并遵循 ONF 管理流程。

注 2：对于一个应用，一项安全活动及其相关的验证测量活动可能是应用安全组件（ASC）的一部分。

3.3

关键信息

一旦泄露可能会造成不可接受风险的信息

3.4

领域专家

在某一特定领域、范围或主题方面有专长的人

3.5

风险管理

针对风险对组织进行指导和控制的协调活动

注 1：本文件使用“过程”一词来描述风险管理的整体情况。风险管理体系中的各个要素称为“活动”。

[来源：ISO 73:2009 指南，2.1]

4 缩略语

AS	Application Security
ASC	Application Security Control
ASMP	应用程序安全管理流程
ANF	应用规范框架
ASLCRM	Application Life Cycle Security Reference Model
ONF	组织规范框架

5 应用程序安全管理流程

5.1 总则

应用程序安全管理流程（ASMP）是组织用于管理其使用或开发的每个特定应用程序的安全性的整体流程。

ONF 委员会负责通过使用 ONF 管理流程来实施和维护 ASMP（参见 ISO/IEC 27034-2:2015，5.4.3）。该委员会还负责确保 ASMP 在组织内的所有应用项目中得到应用。

应用程序所有者有责任确保为应用程序项目制定应用安全成熟度计划（见表 3）。

对于每个应用项目，项目经理负责在项目实施过程中执行和使用 ASMP（见表 3）。

应用程序安全管理流程分为五个步骤执行：

a) 确定应用需求和环境；

b) 评估应用程序的安全风险；

c) 创建并维护应用规范框架；

d) 应用程序的配置与运行；

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2）也可通过客服电话咨询 **025-85307007**。