INTERNATIONAL STANDARD

ISO/IEC 27034-7

First edition
2018-05

Information technology — Application security —

Part 7: **Assurance prediction framework**

Technologies de l'information — Sécurité des applications —

Partie 7: Cadre de l'assurance d'une prédiction

Reference number
ISO/IEC 27034-7:2018(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 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.

0 Introduction

0.1 Basic prediction

The project team declares an application secure when the supporting evidence demonstrates the attainment of the Targeted Level of Trust (ISO/IEC 27034-1:2011, 0.4.4). A security prediction occurs when the project team uses the supporting evidence from a previous version of the application and provides a rationale as to why the supporting evidence is still valid for the subsequent application. The security prediction framework is the process whereby organizations, who use ISO/IEC 27034 (all parts), perform risk analysis and document decisions made, relative to Application Security Controls (ASCs) performed on a previous version of an application but not performed on the current version. All such predictions are fundamentally subjective, and at best can only express a degree of confidence.

Today, individuals and organizations already transfer their confidence in security claims between versions of applications without any strong rationale supporting this transfer. Making a security prediction for a subsequent application, without any rationale or justification, is inherently a bad practice. To rectify this situation, this document establishes a framework by codifying requirements for making security predictions between versions of an application.

This document focuses on predictions, or claim transfers, related to subsequent versions of the same application.

0.2 Purpose

The purpose of this document is to help organizations to develop and use Prediction Application Security Rationales (PASR) in disseminating information relative to security properties of multiple versions of the same application by:

a) providing additional guidance to Organization Normative Framework (ONF) Committees so that they can set up appropriate guidelines for when predictions are and are not appropriate for their organizations;

b) providing the results of a risk analysis that contains the rationale as to why the changes in the subsequent application are not substantial;

c) applying to application projects that are using an Application Normative Framework (ANF);

d) indicating the Actual Level of Trust for the original and subsequent applications;

e) indicating the Expected Level of Trust for the original, if used, and subsequent applications;

f) providing the rationale as to why the risk analysis, predictions for individual Application Security Control (ASC), and the Actual Level of Trust together produce the Expected Level of Trust; and

g) verifying a PASR when the auditor chooses to rerun the corresponding ASC verification activity.

This document does not provide guidelines on:

a) what is and is not an appropriate risk;

b) what is and is not substantial change;

c) when an application owner should or should not accept a specific risk; or

d) when an acquirer should or should not accept an Expected Level of Trust.

0.3 Targeted audience

0.3.1 General

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

a) managers;

b) ONF Committees;

c) project teams;

d) domain experts;

e) auditors;

f) application owners; and

g) acquirers.

0.3.2 Managers

The manager roles are the same as in ISO/IEC 27034-1:2011, 0.3.2.

0.3.3 ONF Committee

As described in ISO/IEC 27034-1:2011, 3.17, 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:

a) provides guidelines to project teams as to what is and is not a substantial change;

b) evaluates, and documents, in the ASC, the risk of choosing the PASR over performing the ASC activity;

c) reviews each ASC and determines if predictions are allowed and, if allowed, under what circumstances predictions are appropriate;

d) documents the prediction determination in each ASC in the ONF;

e) advises the application owner, when establishing the ANF, the estimated risk of using the PASR; and

f) responds to requests from project teams to modify the prediction guidelines for specific ASC.

0.3.4 Provisioning and operation team

As described in ISO/IEC 27034-1:2011, 0.3.3, members of provisioning and operation teams (known collectively as the project team) are individuals involved in an application's design, development and maintenance throughout its whole life cycle. The project manager is responsible for managing the ANF.

The project team:

a) performs a risk analysis on the proposed changes to the application to determine if the changes are substantial;

b) creates the PASR (as defined in 3.2) for each ASC for which there is a prediction; and

c) generates the Expected Level of Trust report.

0.3.5 Domain experts

An individual who is an expert in a particular domain, area, or topic that provides specific knowledge or expertise to the project team. These experts:

a) assist the project team in making an accurate risk assessment; and

b) assist the project team in making the determination if the changes to the application represent a substantial change.

0.3.6 Auditors

As described in ISO/IEC 27034-1:2011, 0.3.6, auditors are personnel performing roles in the audit process who participate in application verification.

0.3.7 Application owners

Based on the definition in ISO/IEC 27034-1:2011, 3.6, the application owner is the organization's representative who is responsible and accountable for the security and the protection of an application. Application owners make the final decisions on:

a) acceptance of the project team risk analysis that the changes to the application are not substantial;

b) approval of a set of ASCs for which the project team generates PASRs; and

c) acceptance of the Expected Level of Trust.

0.3.8 Acquirers

This includes all individuals involved in acquiring a product or service. Acquirers:

a) perform actions as per ISO/IEC 27034-1:2011, 0.3.4;

b) evaluate if the Actual Level of Trust for the original application is appropriate to mitigate the risks the acquirer anticipates for the expected contexts the acquirer will use the application in;

c) evaluate if the Expected Level of Trust for the subsequent application is appropriate to mitigate the risks the acquirer anticipates for the expected contexts the acquirer will use the application in; and

d) evaluate if the rationale that changes to the subsequent application are not substantial and, if not in agreement with the rationale, determine if additional verification is necessary.

Information technology — Application security —

Part 7: Assurance prediction framework

1 Scope

This document describes the minimum requirements when the required activities specified by an Application Security Control (ASC) are replaced with a Prediction Application Security Rationale (PASR). The ASC mapped to a PASR define the Expected Level of Trust for a subsequent application. In the context of an Expected Level of Trust, there is always an original application where the project team performed the activities of the indicated ASC to achieve an Actual Level of Trust.

The use of Prediction Application Security Rationales (PASRs), defined by this document, is applicable to project teams which have a defined Application Normative Framework (ANF) and an original application with an Actual Level of Trust.

Predictions relative to aggregation of multiple components or the history of the developer in relation to other applications is outside the scope of this document.

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*