
**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

iTech Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/IEC 27034-7:2018](https://standards.iteh.ai/catalog/standards/iso/021c8488-40df-46d6-9bbd-461e56ea20fe/iso-iec-27034-7-2018)

<https://standards.iteh.ai/catalog/standards/iso/021c8488-40df-46d6-9bbd-461e56ea20fe/iso-iec-27034-7-2018>



iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[ISO/IEC 27034-7:2018](https://standards.itih.ai/catalog/standards/iso/021c8488-40df-46d6-9bbd-461e56ea20fe/iso-iec-27034-7-2018)

<https://standards.itih.ai/catalog/standards/iso/021c8488-40df-46d6-9bbd-461e56ea20fe/iso-iec-27034-7-2018>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

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	v
0 Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	3
5 Prediction concepts	3
5.1 Goal of prediction	3
5.2 Prediction framework	4
5.3 Expected Level of Trust	4
5.3.1 Concept	4
5.3.2 Expected level of trust in the ONF	5
5.3.3 Expected level of trust in the ANF	6
5.3.4 ASC data in the ANF	7
5.3.5 Expected level of trust over sequence of application versions	8
5.4 Principles	10
5.4.1 ISO/IEC 27034-1 principles	10
5.4.2 Appropriate investment for application security principle	10
5.4.3 Application security should be demonstrated principle	10
5.5 Prediction authorization	10
5.5.1 Prediction accountability	10
5.5.2 Forced authorization	11
5.6 Claims relative to the actual level of trust	11
6 Predictions	11
6.1 Prediction initiator	11
6.2 Prediction circumstances	12
6.2.1 Typical circumstance	12
6.2.2 Relationship to level of trust	12
6.3 Prediction consumer	12
7 Substantial changes	13
7.1 Definition discussion	13
7.2 Guidance for substantial changes risk analysis	13
7.2.1 General	13
7.2.2 Code change and static analysis	13
7.2.3 Architectural review	14
7.2.4 Deprecation of tests over time	14
8 Confidence	14
8.1 Confidence building blocks	14
8.2 Establishing confidence	14
9 Prediction application security rationale	15
9.1 Linkage to ASC	15
9.2 Components	15
9.3 Format	16
9.3.1 Identifiers, actors, ASCs outcomes	16
9.3.2 Rationale	16
9.3.3 Duplication of information	16
9.3.4 Assurance cases	16
9.4 Approval by ONF Committee	16
9.5 Use of RACI charts in description of activities, roles, and responsibilities	17
10 PASR audit	17

10.1	Auditing linkage.....	17
10.2	Auditing actual level of trust.....	17
10.3	Auditing expected level of trust.....	17
10.4	PASR quality.....	18
11	PASR Verification.....	18
11.1	Validation.....	18
11.2	Verification.....	18
11.3	Expected results.....	18
11.4	Missing state.....	18
	11.4.1 Inability to generate verification measurements.....	18
	11.4.2 Example.....	18
12	PASR implementation.....	19
12.1	Prediction framework.....	19
12.2	Steps to implement a PASR.....	19
	12.2.1 General.....	19
	12.2.2 Actor responsibilities.....	20
12.3	ONF feedback.....	20
13	Expected level of trust report.....	20
13.1	Purpose.....	20
13.2	Components.....	20
13.3	Format.....	21
13.4	History, assumptions and social history.....	21
Annex A (informative) Expected level of trust assurance case.....		23
Annex B (informative) Comparison of ASC to PASR.....		25
Bibliography.....		29

Document Preview

ISO/IEC 27034-7:2018

<https://standards.iteh.ai/catalog/standards/iso/021c8488-40df-46d6-9bbd-461e56ea20fe/iso-iec-27034-7-2018>

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.

<https://standards.iteh.ai/catalog/standards/iso/021c8488-40df-46d6-9bbd-461e56ea20fe/iso-iec-27034-7-2018>