

---

---

# 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*



## **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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b>	<b>v</b>
<b>0 Introduction</b>	<b>vi</b>
<b>1 Scope</b>	<b>1</b>
<b>2 Normative references</b>	<b>1</b>
<b>3 Terms and definitions</b>	<b>1</b>
<b>4 Abbreviated terms</b>	<b>3</b>
<b>5 Prediction concepts</b>	<b>3</b>
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
<b>6 Predictions</b>	<b>11</b>
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
<b>7 Substantial changes</b>	<b>13</b>
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
<b>8 Confidence</b>	<b>14</b>
8.1 Confidence building blocks	14
8.2 Establishing confidence	14
<b>9 Prediction application security rationale</b>	<b>15</b>
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
<b>10 PASR audit</b>	<b>17</b>

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
<b>11</b>	<b>PASR Verification.....</b>	<b>18</b>
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
<b>12</b>	<b>PASR implementation.....</b>	<b>19</b>
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
<b>13</b>	<b>Expected level of trust report.....</b>	<b>20</b>
13.1	Purpose.....	20
13.2	Components.....	20
13.3	Format.....	21
13.4	History, assumptions and social history.....	21
	<b>Annex A (informative) Expected level of trust assurance case.....</b>	<b>23</b>
	<b>Annex B (informative) Comparison of ASC to PASR.....</b>	<b>25</b>
	<b>Bibliography.....</b>	<b>29</b>

## 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](http://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](http://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](http://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.