

---

---

**IT security techniques — Competence  
requirements for information security  
testers and evaluators —**

**Part 1:  
Introduction, concepts and general  
requirements**

*Techniques de sécurité IT — Exigences de compétence pour  
l'information testeurs d'assurance et les évaluateurs —*

*Partie 1: Introduction, concepts et exigences générales*





**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>iv</b>
<b>Introduction</b> .....	<b>v</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 Concepts</b> .....	<b>2</b>
<b>5 Elements of competence</b> .....	<b>3</b>
5.1 Competences .....	3
5.2 Knowledge .....	3
5.3 Skills .....	4
5.4 Experience .....	4
5.5 Education .....	5
5.6 Effectiveness .....	5
<b>6 Competency levels</b> .....	<b>5</b>
6.1 General .....	5
6.2 Level 1 (Associate) .....	5
6.3 Level 2 (Professional) .....	5
6.4 Level 3 (Manager) .....	5
6.5 Level 4 (Principal) .....	6
<b>7 Measurement of elements of competence</b> .....	<b>6</b>
7.1 Knowledge .....	6
7.2 Skills .....	6
7.3 Experience .....	6
7.4 Education .....	6
7.5 Effectiveness .....	7
7.6 Recording elements of competence .....	7
<b>Annex A (informative) Framework for describing competence requirements</b> .....	<b>8</b>
<b>Annex B (informative) Example records of experience and competence</b> .....	<b>10</b>
<b>Bibliography</b> .....	<b>11</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, *IT Security techniques*.

A list of all parts in the ISO/IEC 19896 series can be found on the ISO website.

## Introduction

The objective of the ISO/IEC 19896 series is to provide the fundamental concepts related to the topic of the competence of the individuals responsible for performing IT product security evaluations and conformance testing. The ISO/IEC 19896 series provides the framework and the specialized requirements that specify the minimum competence of individuals performing IT product security evaluations and conformance testing using established standards.

In pursuit of this objective, the ISO/IEC 19896 series comprises the following:

- a) The terms and definitions relating to the topic of competence in IT product security evaluators and testers;
- b) The fundamental concepts relating to competence in IT product security evaluations and conformance testing; and
- c) The minimum competence requirements for IT product security evaluators and testers to conduct IT product testing/evaluation.

The ISO/IEC 19896 series is of interest to:

- a) Information security evaluation and conformance-testing specialists;
- b) Information security evaluation and conformance-testing approval authorities;
- c) Information security evaluation and conformance-testing laboratories;
- d) Vendors or technology providers whose IT products can be the subject of information security assurance evaluations or conformance-testing;
- e) Organizations offering professional credentials or recognitions.

The ISO/IEC 19896 series is organized in parts to address the competence of evaluation and testing professionals as follows.

In this document, the introduction and concepts, provides an overview of the definitions, fundamental concepts and a general description of the framework used to communicate the competence requirements for certain specialized areas. This material is aimed at providing the fundamental knowledge necessary to use the framework presented in the other parts of the ISO/IEC 19896 series appropriately.

ISO/IEC 19896-2 describes the minimum set of competence requirements at each competency level for conformance testers working with ISO/IEC 19790 and associated standards.

ISO/IEC 19896-3 describes the minimum set of competence requirements at each competency level for information security evaluators working with ISO/IEC 15408 (all parts) and associated standards.



# IT security techniques — Competence requirements for information security testers and evaluators —

## Part 1:

## Introduction, concepts and general requirements

### 1 Scope

This document defines terms and establishes an organized set of concepts and relationships to understand the competency requirements for information security assurance conformance-testing and evaluation specialists, thereby establishing a basis for shared understanding of the concepts and principles central to the ISO/IEC 19896 series across its user communities. It provides fundamental information to users of the ISO/IEC 19896 series.

### 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 17000, *Conformity assessment — Vocabulary and general principles*

ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*