Technical Specification

ISO/IEC TS 24462

Information security, cybersecurity and privacy protection — Ontology building blocks for security and risk assessment

Sécurité de l'information, cybersécurité et protection de la vie privée — Blocs de construction pour l'ontologie de l'évaluation de la sécurité et des risques

First edition
2024-03

Reference number
ISO/IEC TS 24462:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The assessment of trustworthiness within information and computer technologies (ICT) is associated with various types of best practices and evaluations, such as governance, secure development lifecycle, security evaluation and risk assessment.

This document was developed to build upon international standards dealing with ICT assessment such as ISO/IEC 27034-7, ISO/IEC 27007 and ISO/IEC 27036-1.

When a new technology or use case becomes prominent, novel approaches to assessments should be defined, which take existing frameworks into consideration. The dynamic cycle of technological development and integrated environments increase the need for international standards. This document aims to simplify the approach for creating new assessments and for analysing existing assessments for their applicability in the emerging and mature technology areas.

This document contains the following elements:

a) an inventory of uniform components of assessment-related standards, called building blocks (BBs), and their structure;

b) ontology capturing relationships among BBs;

c) guidelines for using standardized BBs.

Figure 1 and Figure 2 provide an overview of a representative hierarchy of BBs from this document. Figure 1 depicts the top-level classes of the hierarchy. Figure 2 illustrates the semantic building block branch of the hierarchy, with its building blocks for assessments and assessment components.

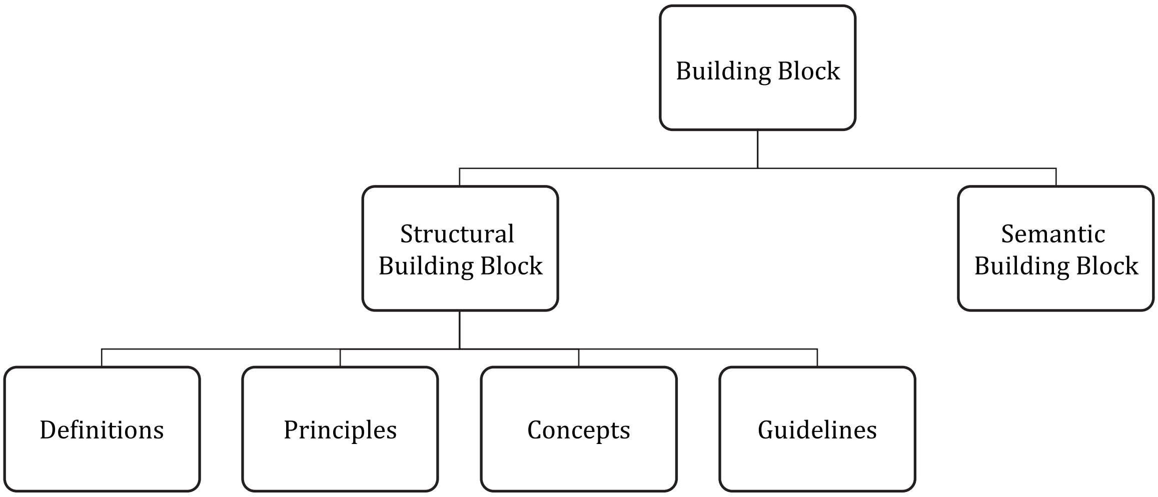

Figure 1 — Top levels of the ontology

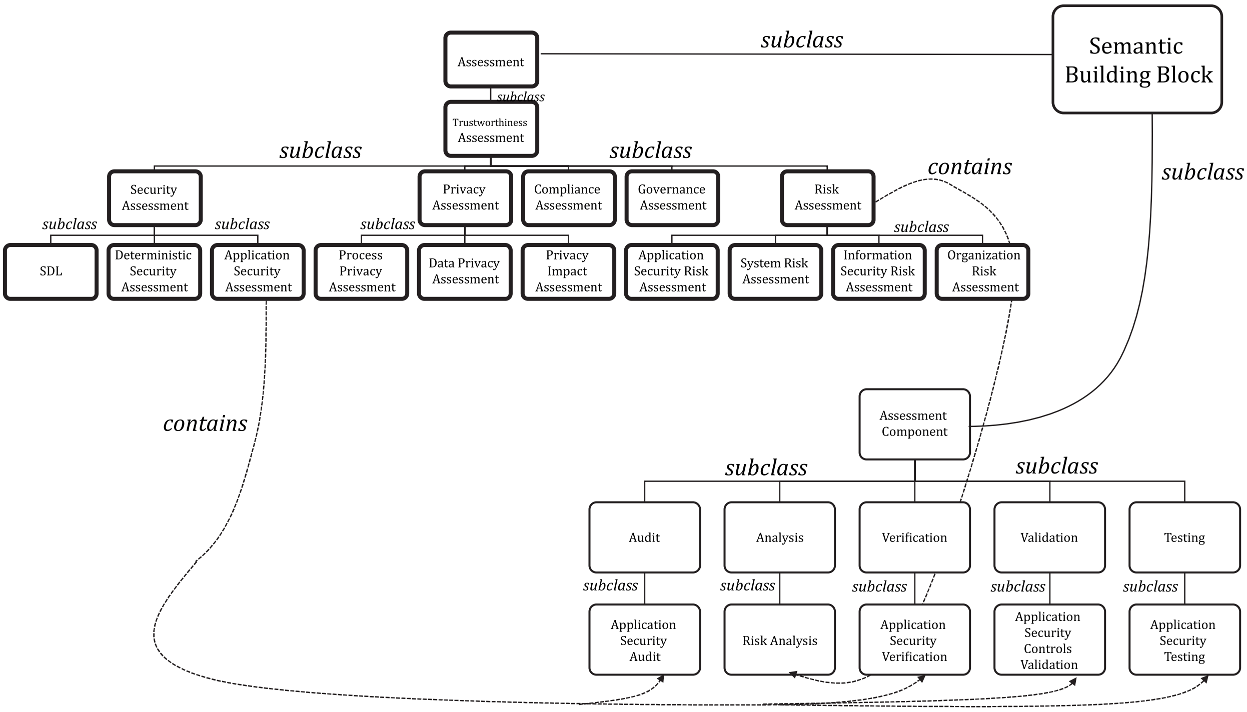

Figure 2 — Semantic Building Block branch of the ontology

Information security, cybersecurity and privacy protection — Ontology building blocks for security and risk assessment

1 Scope

This document defines an inventory of building blocks conceptually associated with different types of assessments of information and communication technology (ICT) trustworthiness. These assessments apply to areas such as governance, risk management, security evaluation, secure development lifecycle (SDL), supply chain integrity and privacy. This document also defines an ontology that organizes these building blocks and provides instructions for using the inventory of building blocks and the ontology.

Formalizing the types, categories, and structural characteristics of building blocks in the area of ICT trustworthiness assessment aims to increase efficiency and improve future harmonization in standards development and their use. Building blocks can refer to structural components as well as semantic components. These components can be connected to a variety of concepts and activities related to trustworthiness assessments, including process related, such as traceability or elements of assessment methodologies.

2 Normative references

There are no normative references in this document.