Technical Specification

ISO/IEC TS 24462

First edition
2024-03

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

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

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.

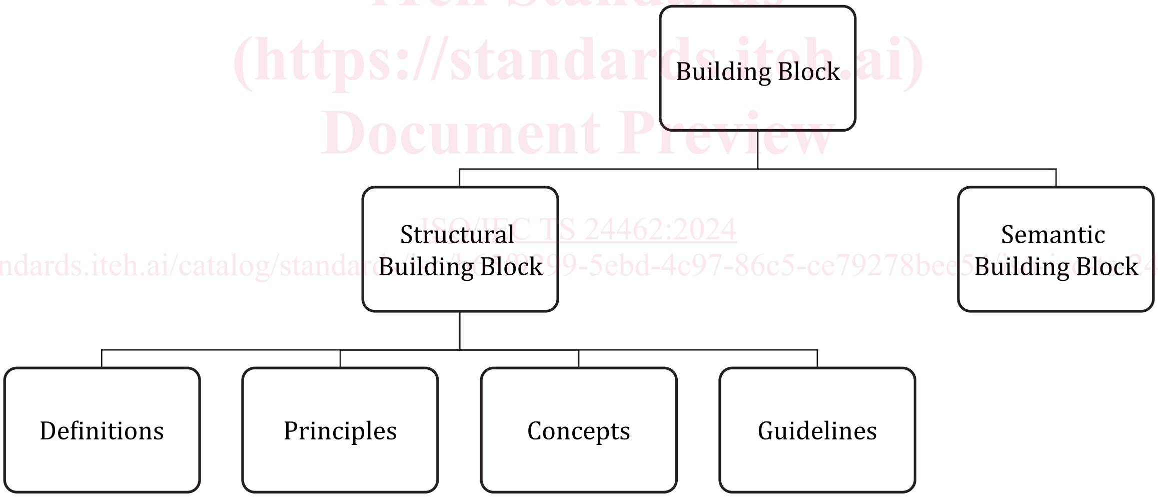

Figure 1 — Top levels of the ontology

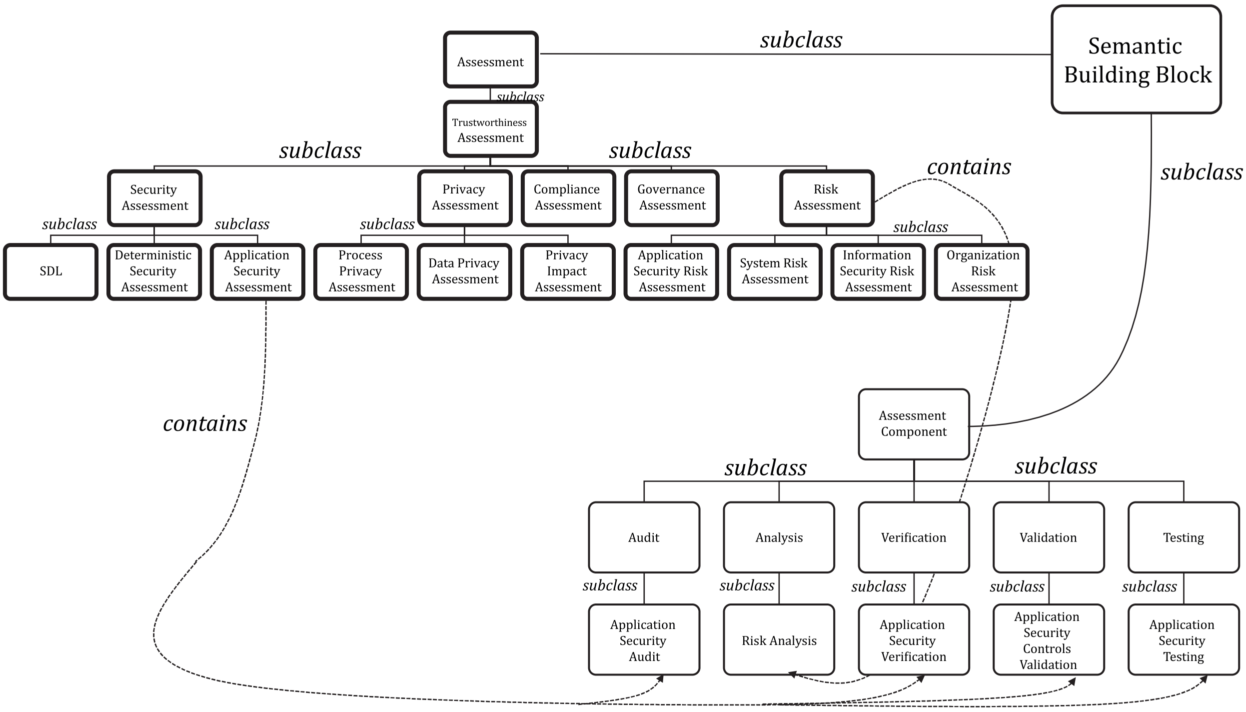

Figure 2 — Semantic Building Block branch of the ontology

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.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
structural building block
structural units that are independent of the particular assessment type, such as definitions and principles

Note 1 to entry: Structural building blocks are found in many assessment-related standards, e.g. ISO/IEC 27034-7, ISO/IEC 27007 and ISO/IEC 27036-1.

3.2
semantic building block
conceptual units that are specific to assessment types

Note 1 to entry: Examples of semantic building blocks can be found in ISO/TR 11633-2:2021, ISO/IEC 29134:2023: 3.7, ISO/IEC/IEEE 26514:2022, 4.4 and ISO/IEC 27034-3:2018, 3.1.

3.3
assessment building block
semantic building block (3.2) describing a type of information and communication technology assessment

Note 1 to entry: Information and communication technology assessment is the action of applying specific documented criteria to a specific software or hardware module, package or product for the purpose of determining acceptance or release of the software module, package or product.

3.4
assessment component building block
semantic building block (3.2) constituting an element of an *assessment building block* (3.3) that cannot be further fragmented

3.5
data property
properties that connect individuals with data values such as particular strings or integers

Note 1 to entry: In some knowledge representation systems, functional data properties are called attributes.

[SOURCE: OWL 2 Web Ontology Language Quick Reference Guide (Second Edition), 2012]

3.6
datatype
entities that refer to sets of data values such as particular strings or integers

Note 1 to entry: In this sense, datatypes are analogous to classes, the main difference being that the former contain data values such as strings and integers, rather than individuals.

[SOURCE: OWL 2 Web Ontology Language Quick Reference Guide (Second Edition), 2012]

3.7
extensible markup language
XML
subset of the Standard Generalized Markup Language (SGML)

Note 1 to entry: The goal of XML is to enable generic SGML to be served, received, and processed on the Web in the way that is now possible with HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML.

[SOURCE: OWL 2 Web Ontology Language Quick Reference Guide (Second Edition), 2012]

3.8
individual
syntactic element of *owl 2 web ontology language (OWL)* (3.11) representing actual objects from the domain

[SOURCE: OWL 2 Web Ontology Language Quick Reference Guide (Second Edition), 2012]

3.9
object property
properties that connect sets of *individuals* (3.8)

[SOURCE: OWL 2 Web Ontology Language Quick Reference Guide (Second Edition), 2012]

3.10
ontology
formal description of a domain of interest, consisting of the following three different syntactic categories: (a) entities, such as classes, *properties* (3.12), and *individuals* (3.8), identified by IRIs; (b) expressions, representing complex notions in the domain being described; (c) axioms, formalizing statements that are asserted to be true in the domain being described

Note 1 to entry: Entities form the primitive terms of an ontology and constitute the basic elements of an ontology. For example, a class a:Person can be used to represent the set of all people. Similarly, the object property a:parentOf can be used to represent the parent-child relationship. Finally, the individual a:Peter can be used to represent a particular person called “Peter”.

[SOURCE: OWL 2 Web Ontology Language Quick Reference Guide (Second Edition), 2012]

3.11
owl 2 web ontology language
OWL
ontology language for the Semantic Web with formally defined meaning

Note 1 to entry: OWL 2 ontologies provide classes, *properties* (3.12), *individuals* (3.8), and data values and are stored as Semantic Web documents. OWL 2 ontologies can be used along with information written in *RDF* (3.13), and OWL 2 ontologies themselves are primarily exchanged as RDF documents.

[SOURCE: OWL 2 Web Ontology Language Quick Reference Guide (Second Edition), 2012]

3.12
property
quality common to all members of an object class

[SOURCE: ISO/IEC 11179-1:2023, 3.3.2, modified — Domain and Note 1 to entry added.]

3.13
resource description framework
RDF
framework for representing information in the Web

Note 1 to entry: The core structure of the abstract syntax is a set of triples, each consisting of a subject, a predicate and an object. A set of such triples is called an RDF graph.

[SOURCE: OWL 2 Web Ontology Language Quick Reference Guide (Second Edition), 2012]

3.14
subclass
class derived from another class by specialization

[SOURCE: ISO/IEC 10165-1:1993, 3.8.32]

3.15
application security control
data structure, which includes requirements, descriptions, graphical representations, and *XML* (3.7) schema

4 Symbols and abbreviated terms

ASC	application security control
ASMP	application security management process
BB	building block
ICT	information and communication technologies
IRI	internationalized resource identifier
OWL	owl 2 web ontology language
RDF	resource description framework
SDL	security development lifecycle
URI	uniform resource identifier
XML	extensible markup language

5 Background

There are a large number of international standards dealing with ICT assessments covering ICT areas such as governance, secure development lifecycle, deterministic testing, or risk assessment. This body of knowledge also includes reports and best practices documents[21],[26] as well as position papers[30],[32] focusing on different approaches to ICT assessments.

When a new technology or use case becomes prominent, it is necessary to define new approaches to assessments which consider existing frameworks. However, aligning new approaches to existing standards and developing new standards is a resource intensive process that requires specialized expertise (see Reference [26] for an example). Furthermore, the dynamic cycle of technological development, and the massive need for integration of multiple systems, where independent technology domains are connected, as well as the global nature of the digital infrastructure, has elevated the need for international standards.

As the body of available standards continues to grow and the diversification of the ICT space intensifies, it has become more difficult to ensure consistency of approaches used in similar standard ICT assessments. At the same time, the need to streamline, harmonize, and quickly develop assessment-relevant standards has become acute, brought on to the dynamic technology development, increasing concerns about security, privacy, and assurance, and growing diversity in the technology space and contexts where similar technologies are used.

Thus, new frameworks and standards for developing new ICT assessments and analysing the existing ones with greater efficiency would be useful. Defining these methodologies can also lead to the development of more focused and context specific requirements in the area of ICT assessment, which is the purpose of this document.

It is worth noting that significant work has been done in international standards bodies with regard to using ontologies to harmonize concepts within specific domains. For example, ISO/IEC 21838-1 defines characteristics of a top-level ontology that can be used with lower-level domain-specific ontologies. Standardization work using ontologies to improve the efficiency of building, analysing, and implementing standards has been more limited, but it has been covered in research literature. Reference [27] uses ontologies to link standardized tags related to properties of the IoT space to the descriptions of the functions they denote. In the medical field, Reference [28] uses an ontology to standardize and classify adverse drug reactions based on the Adverse Drug Reaction Classification System. Reference [29] describes how ontologies can be used to map existing security standards, and Reference [30] developed ontologies to formalize security knowledge and make it more amenable to various analyses. Reference [31] developed an ontology for ISO software engineering standards, complete with a prototype demonstrating their approach.

6 Methodology

A methodology was devised to build this document. The methodology consists of:

a) the methodology for identifying and describing BBs and their relationships with each other;

b) the approach for using the ontology and its BBs to build new assessment standards and frameworks;

c) the approach to the governance of the ontology and its elements; and

d) the methodology for the maintenance of the BBs.

The inventory of the BBs was informed by the study and analysis of standards, specifications, guidelines and best practices documents as well as research output in the area of the ICT assessments. The elements of the documents were examined, yielding the times and instances of BBs.

It should be noted that there are structural similarities in the structural organization, semantic affinities of similar elements, and similarities among relationships linking various elements in documents related to ICT assessments. This document builds upon the observation that these documents include similar components, especially in a given field of application, e.g. security assessment and privacy assessment.

A number of standards documents from different standards development organizations were examined to identify the recurrent elements (building blocks). It was observed that, while semantically these parts are not always identical, in a given field there is a shared high-level compatibility of the semantics. For example, deterministic security assessment is used in both References [19] and [24] and examples of guidelines are available in Reference [21].

These structural and semantic similarities in assessment-related standards documents are generalized in structural and semantic building blocks (BBs). Semantic BBs can be composed of one or more structural BBs.

An inventory of BBs was iteratively created from a representative sample of standards documents related to assessments and analysis of experts' contributions. The complete inventory is available in Clause 9. For each BB, the inventory includes the type, location and description of the BB. The typology of BBs was then refined through the analysis of relevant ontologies, such as in References [32] to [35].

The minimal possible number of structural and semantic BBs were identified. The following steps were followed to develop the inventory of BBs:

e) identify pertinent structural BBs, such as definitions or principles;

f) identify semantic BBs.

The inventory was then organized in a hierarchy that reflects the logical links among BBs. The links are based on the observed similarities in structural organization and the abovementioned semantic affinities, as well as the relationships between components as they were found to occur in the documents.

Drawing from the inventory, an ontology was created that included BBs, types, and relations from the inventory and made them more precise. Additional information on the types and nature of BBs is described in Clause 7. The inventory of the BBs is presented in Clause 9. The organization follows these core criteria, which are expected to be generally applicable.

The criteria include:

g) BBs are divided into structural and semantic (see Figure 3);

h) semantic BBs are partitioned in assessments and "assessment components". The difference between them is that assessment BBs can contain other semantic BBs, while assessment components are atomic objects that are not further fragmented. This is illustrated in Figure 4, where the UML annotation 0..n on a class indicates that the relationship can apply to an arbitrary set of instances of that class, as opposed to a single instance;

i) within the above categories, BBs are hierarchically organized by a class-subclass relation (see Figure 5);

j) the relationship between assessments and BBs that occur in them is captured by a containment relation (see Figure 5);

k) the containment relation is inherited at the class level, i.e. if a BB type A contains certain types of BBs, then any sub-class of A also contains those types of BBs (see Figure 5).

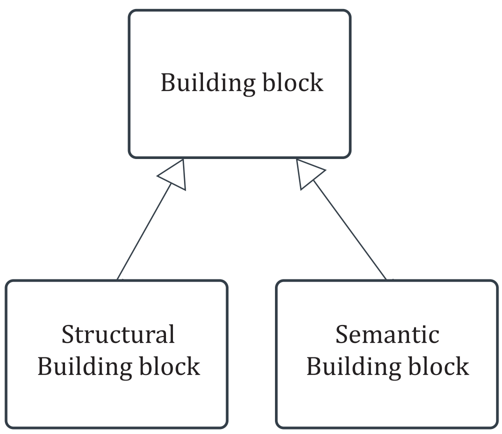

Figure 3 — BBs divided into structural and semantic BBs

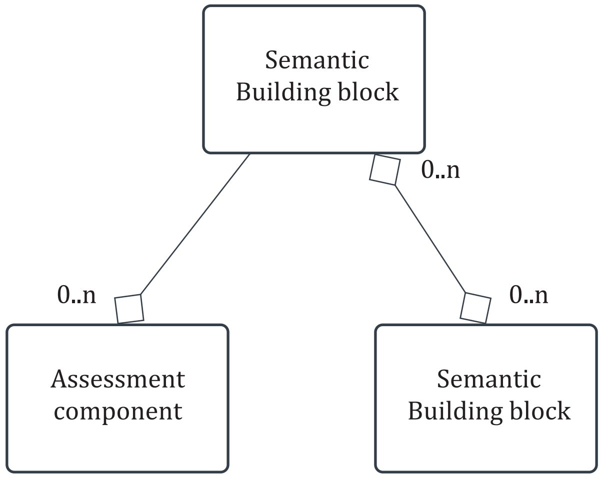

Figure 4 — Semantic building blocks

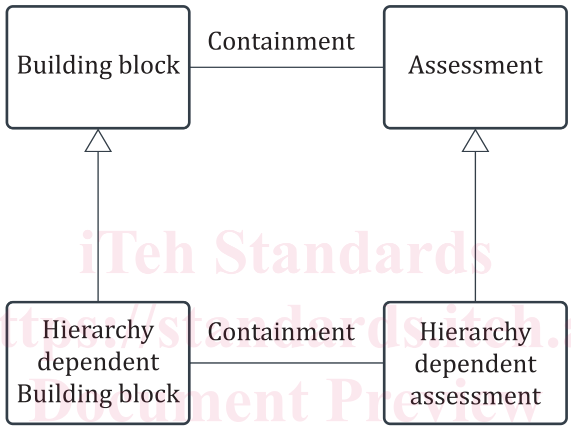

Figure 5 — Building block and assessment hierarchy

The characterization of the structure of standards documents presents certain challenges. Certain concepts are used in different documents with somewhat different informal meanings. Additionally, repeated components are present in certain assessment documents.

The ontology should be used to assist in planning new ICT assessment standards or use cases associated with existing standards. The ontology is not intended to suggest alteration to any existing assessment standards. The developer of the new assessment should follow the steps included below, which can also be automated by software tools.

— The developer should identify pertinent structural building blocks for the proposed assessment from the inventory, such as definitions or principles and observe their positioning in the ontology.

— The developer should identify semantic building blocks by considering whether the new assessment has similarities with existing assessment types.

    — If there are similarities with a single existing assessment, then the new use case should include the assessment components from the existing assessment.

    — If there are similarities with multiple existing assessments, then the new use case should include the assessment components of all of them.

As an example, an application security assessment of optical eye-level displays is considered. A standard for the application security assessment of video displays already exists (in this example). In the first step of the process, inspection of the existing standard enables definitions to be identified as a pertinent structural building block that is present in the video displays standard. Next, the similarities between the