ISO/IEC DTS 24462:2023(~~X~~E)

ISO/IEC JTC 1/SC27/WG3

Secretariat: DIN

Date: 2023-~~08-28~~11-20

Information ~~Security, Cybersecurity~~security, cybersecurity and ~~Privacy Protection~~privacy protection — Ontology ~~Building Blocks~~building blocks for ~~Security~~security and ~~Risk Assessment~~risk assessment

~~WD/CD/DIS/FDIS stage~~

~~Warning for WDs and CDs~~

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.~~

~~*A model manuscript of a draft International Standard (known as "The Rice Model") is available at https://www.iso.org/iso/model_document-rice_model.pdf*~~

Style Definition ...
Formatted: Font: 11 pt, English (United Kingdom)
Formatted ...
Formatted: zzCover, Left
Formatted ...
Formatted: Font: Not Bold
Formatted: zzCover, Left, Space After: 0 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: 11 pt
Formatted: zzCover, Line spacing: single, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted ...

Formatted: Font: 11.5 pt, Bold
Formatted: Normal
Formatted: Font: 11.5 pt, Bold
Formatted: Font: 11.5 pt, Bold
Formatted
Formatted: Font: 11 pt, Font color: Blue
Formatted: Indent: Left: 0 pt, Right: 0 pt, Border: Left: (No border), Right: (No border)
Formatted: Font: 11 pt, Font color: Blue
Formatted: Font: 11 pt, Font color: Blue
Formatted: Font: 11 pt, Font color: Blue
Formatted: Font: 11 pt
Formatted: Font: 11 pt, Font color: Blue
Formatted: Font: 11 pt, Font color: Blue
Formatted: Indent: Left: 0 pt, First line: 0 pt, Right: 0 pt, Border: Left: (No border), Right: (No border)
Formatted: Font: 11 pt, Font color: Blue, English (United Kingdom)
Formatted: Font: 11 pt, Font color: Blue, English (United Kingdom)
Formatted: Font: 11 pt, Font color: Blue, English (United Kingdom)
Formatted: Font: 11 pt, Font color: Blue, English (United Kingdom)
Formatted: Indent: Left: 0 pt, First line: 0 pt, Right: 0 pt, Border: Bottom: (No border), Left: (No border), Right: (No border)
Formatted: Font: 11 pt, Font color: Blue, English (United Kingdom)
Formatted: Font: 11 pt, Font color: Blue, English (United Kingdom)
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single

Formatted: Font: 11.5 pt, Bold
Formatted: Font: 11.5 pt, Bold
Formatted: Normal
Formatted: Font: 11.5 pt, Bold

Contents

Formatted: Space Before: 48 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

This template allows you to work with default MS Word functions and styles. You can use these if you want to maintain the Table of Contents automatically and apply auto-numbering.

To update the Table of Contents please select it and press "F9".

Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single

Formatted: Font: 11.5 pt, Bold
Formatted: Font: 11.5 pt, Bold
Formatted: Normal
Formatted: Font: 11.5 pt, Bold
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documentsdocument 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 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawnISO and IEC draw attention to the possibility that some of the elementsimplementation of this document may beinvolve the subjectuse of (a) patent rights. ISO(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. 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 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) 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 JTC1/WG27JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Formatted: Font: 11.5 pt, Bold
Formatted: Font: 11.5 pt, Bold
Formatted: Normal
Formatted: Font: 11.5 pt, Bold
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single

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.htmlwww.iso.org/members.html and www.iec.ch/national-committees.

Formatted: Font: 11.5 pt, Bold
Formatted: Font: 11.5 pt, Bold
Formatted: Normal
Formatted: Font: 11.5 pt, Bold
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single

Introduction

The assessment of trustworthiness within ~~Information~~information and ~~Computer Technologies~~computer technologies (ICT) is associated with various types of best practices and evaluations, such as governance, secure development lifecycle, security evaluation~~, risk assessment. This document defines an inventory of building blocks conceptually associated with different types of assessments, an ontology that organizes the building blocks, and instructions for using the inventory of building blocks and the ontology. Relevant areas include assessments related to governance, risk management, security evaluation, Secure Development Lifecycle (SDL), supply chain integrity, privacy.~~ and risk assessment.

This document was developed to build upon international standards dealing with ICT assessment such as ISO/IEC 27034-7~~:2018(E), 0.2~~, ISO/IEC 27007~~:2020(en), 4.0,~~ and ISO/IEC 27036-1~~:2021(en), 5.0~~.

When a new technology or use case ~~become~~becomes prominent, novel approaches to assessments ~~taking into consideration~~should be defined, which take existing frameworks ~~should be defined.~~into consideration. The dynamic cycle of ~~technology~~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.

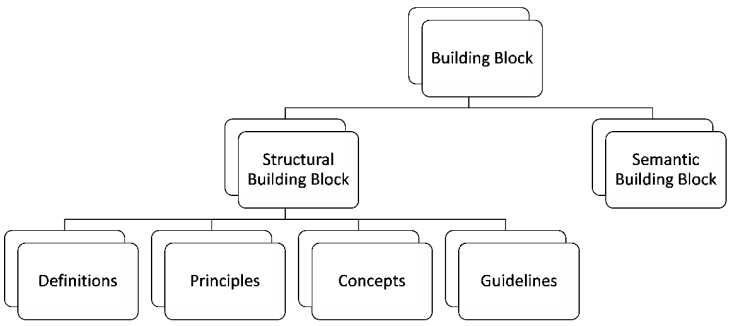
This document contains the following elements:

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

~~b)~~ b) ontology capturing relationships among BBs;

~~c)~~ 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.



Formatted: Font: 11.5 pt, Bold
Formatted: Normal
Formatted: Font: 11.5 pt, Bold
Formatted: Font: 11.5 pt, Bold
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: English (United Kingdom)
Formatted: std_publisher, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_docNumber, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_docPartNumber, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_publisher, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_docNumber, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_publisher, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_docNumber, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_docPartNumber, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted ...
Formatted ...
Formatted: cite_fig
Formatted: cite_fig
Formatted: cite_fig
Formatted: cite_fig
Formatted: cite_fig
Formatted: cite_fig
Formatted: cite_fig
Formatted: cite_fig
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single

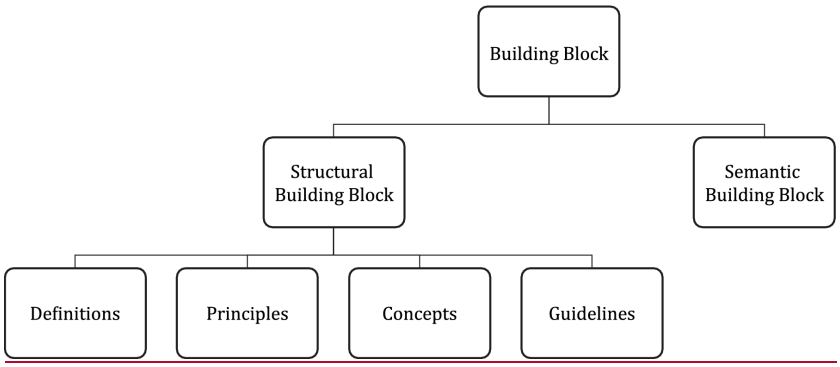
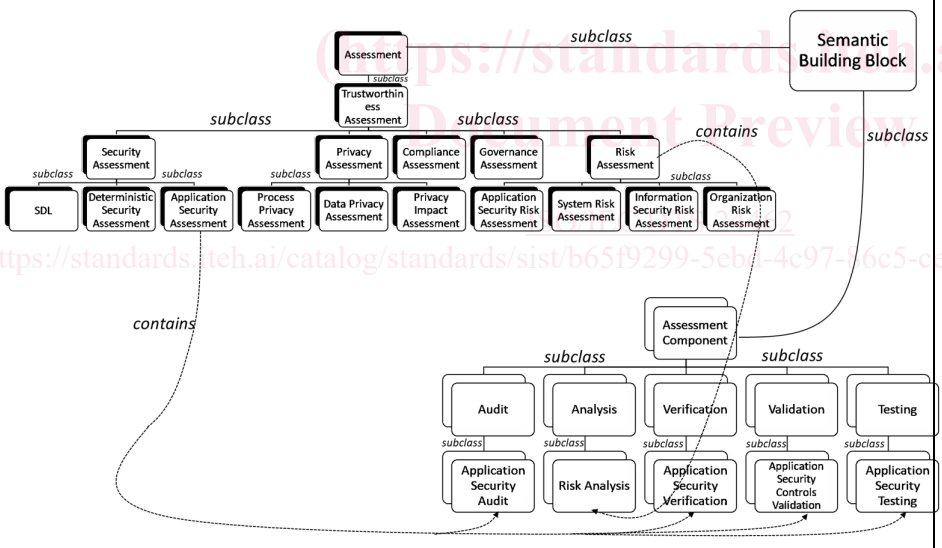


Figure 1 — Top levels of the ontology



Formatted: Font: 11.5 pt, Bold
Formatted: Font: 11.5 pt, Bold
Formatted: Normal
Formatted: Font: 11.5 pt, Bold
Formatted: Figure title, Level 1, Indent: Left: 0 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single

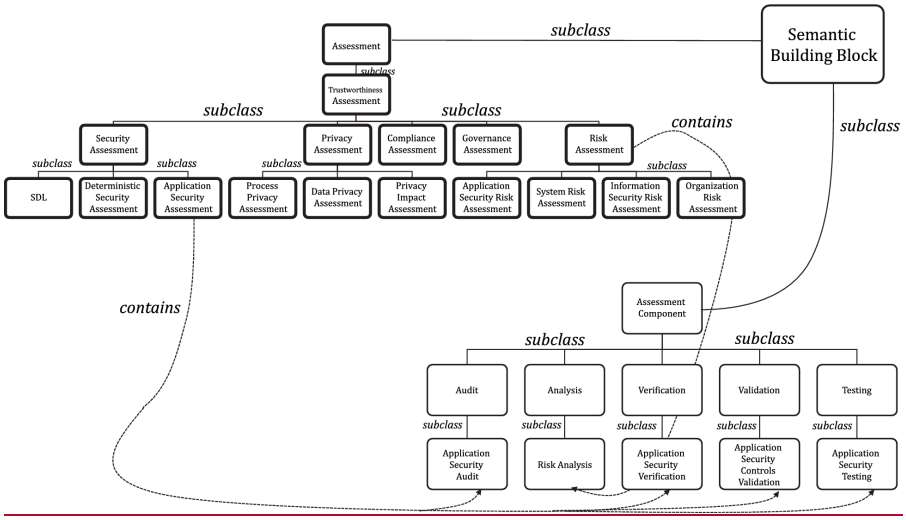


Figure 2 — Semantic Building Block branch of the ontology

Formatted: Font: 11.5 pt, Bold
Formatted: Font: 11.5 pt, Bold
Formatted: Normal
Formatted: Font: 11.5 pt, Bold
Formatted: Figure title, Level 1, Indent: Left: 0 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single

Information ~~Security, Cybersecurity~~security, cybersecurity and ~~Privacy Protection~~privacy protection — Ontology ~~Building Blocks~~building blocks for ~~Security~~security and ~~Risk Assessment~~ 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~~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~~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

Formatted: Section start: New page, Different first page header
Formatted: Font color: Blue
Formatted: Space Before: 20 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font color: Blue
Formatted: Font color: Blue
Formatted: Font color: Blue
Formatted: Font color: Blue
Formatted: Font: Bold, Font color: Blue
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: English (United Kingdom)
Formatted: Body Text, Line spacing: single, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: Not at 28 pt
Formatted: Font: English (United Kingdom)
Formatted: Font: English (United Kingdom)
Formatted: Font: English (United Kingdom)
Formatted ...
Formatted: English (United Kingdom)
Formatted ...
Formatted ...
Formatted: No underline, Font color: Auto
Formatted ...
Formatted: No underline, Font color: Auto
Formatted ...
Formatted ...
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted ...

Note 1 to entry: Examples of semantic building blocks can be found for instance in ISO/TR 11633-2:2009: 2.52021, ISO/IEC 29134:20172023: 3.7, ISO/IEC/IEEE 26514:2008:2022, 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: informationInformation 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 Structural Specification and Functional-Style SyntaxQuick Reference Guide (Second Edition)(11 December), 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 Structural Specification and Functional-Style SyntaxQuick Reference Guide (Second Edition)(11 December), 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 Structural Specification and Functional-Style SyntaxQuick Reference Guide (Second Edition)(11 December), 2012)]]

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

