

~~ISO/IEC DTS 24462:2023(XE)~~

~~ISO/IEC JTC 1/SC27/WG3~~

~~Secretariat: DIN~~

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

~~Information Security, Cybersecurity, privacy protection — Ontology Building Blocks for Security and Risk Assessment~~

- 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

iTeh Standards

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

Document Preview

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>

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[ISO/IEC DTS 24462](#)

<https://standards.itih.ai/catalog/standards/sist/b65f9299-5ebd-4c97-86c5-cc79278bee54/iso-iec-dts-24462>

ISO/IEC TS-DTS 24462:2023 (X/E)

© ISO 2023

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 Copyright Office

CP 401 • Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

Email: copyright@iso.org

Email: copyright@iso.org

Website: www.iso.org

Published in Switzerland

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)

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC DTS 24462

<https://standards.iteh.ai/catalog/standards/sist/b65f9299-5ebd-4c97-86e5-ce792>

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

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

Foreword.....	v
Introduction.....	vi
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	1
4 Symbols and abbreviated terms.....	3
5 Background.....	3
6 Methodology.....	4
7 Building blocks: collection and structure.....	7
7.1 General.....	7
7.2 Application security assessment.....	8
7.3 Risk assessment.....	9
7.4 Application security audit.....	9
7.5 Application security controls validation.....	9
7.6 Risk analysis.....	10
8 Ontology capturing relationships among BBs.....	10
8.1 General.....	10
8.2 Building block: application security assessment.....	13
8.3 Building block: risk assessment.....	14
8.4 Building block: application security audit.....	14
8.5 Building block: application security controls validation.....	15
8.6 Building block: risk analysis.....	15
8.7 Lifecycle of building blocks.....	15
8.8 Using BBs.....	15
8.8.1 General.....	15
8.8.2 Using the ontology to structure an assessment based on an existing standard.....	16
8.8.3 Using the ontology to obtain components for an assessment based on a revised edition of a standard.....	16
8.8.4 Using the ontology to obtain structural components for an assessment based on the first edition of a standard.....	16
9 Standard inventory of uniform components.....	17

Formatted: Font: 11 pt

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

9.1	Structural BBs	17
9.1.1	Description	17
9.1.2	Inventory	17
9.2	Semantic BBs	18
9.3	Assessment BBs	18
9.3.1	Description	18
9.3.2	Inventory	18
9.4	Assessment component BBs	23
9.4.1	Description	23
9.4.2	Inventory	23
10	Complete XML encoding	26
	Bibliography	41
	Foreword	v
	Introduction	vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	4
5	Background	5
6	Methodology	5
7	Building blocks: collection and structure	10
7.1	General	10
7.2	Application security assessment	11
7.3	Risk assessment	11
7.4	Application security controls validation	12
7.5	Risk analysis	13
8	Ontology capturing relationships among BBs	13
8.1	General	13
8.2	Building block: application security assessment	19
8.3	Building block: risk assessment	20
8.4	Building block: application security audit	21
8.5	Building block: application security controls validation	21
8.6	Building block: risk analysis	22
8.7	Lifecycle of building blocks	22
8.8	Using BBs	22
8.8.1	General	22
8.8.2	Using the ontology to structure an assessment based on an existing standard	23
8.8.3	Using the ontology to obtain components for an assessment based on a revised edition of a standard	23
8.8.4	Using the ontology to obtain structural components for an assessment based on the first edition of a standard	24
9	Standard inventory of uniform components	25
9.1	Structural BBs	25
9.1.1	Description	25

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

ISO-TS /IEC DTS 24462:2023 (XE)

9.1.2 Inventory	25
9.2 Semantic BBs	27
9.3 Assessment BBs	27
9.3.1 Description	27
9.3.2 Inventory	27
9.4 Assessment component BBs	33
9.4.1 Description	33
9.4.2 Inventory	34
10 Complete XML encoding	38
Bibliography	68

Formatted: Font: 11.5 pt, Bold

Formatted: Font: 11.5 pt, Bold

Formatted: Normal

Formatted: Font: 11.5 pt, Bold

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC DTS 24462

<https://standards.iteh.ai/catalog/standards/sist/b65f9299-5ebd-4c97-86c5-cc79278bee54/iso-iec-dts-24462>

© ISO ### - All rights reserved 5

© ISO/IEC 2023 - All rights reserved

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

Foreword

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

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 documents 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).

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Attention is drawn to the possibility that some of the elements implementation of this document may be involve the subject use of (a) patent rights. 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 or 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/WG27/JTC 1, Information technology, Subcommittee SC 27, Information security, cybersecurity and privacy protection.

Formatted: Font: 11 pt

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

~~ISO-TS /IEC DTS 24462:2023 (X)~~

Formatted: Font: 11.5 pt, Bold

Formatted: Font: 11.5 pt, Bold

Formatted: Normal

Formatted: Font: 11.5 pt, Bold

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

iTeh Standards (<https://standards.iteh.ai>) Document Preview

ISO/IEC DTS 24462

<https://standards.iteh.ai/catalog/standards/sist/b65f9299-5ebd-4c97-86c5-cc79278bee54/iso-iec-dts-24462>

© ISO ### - All rights reserved 7

© ISO/IEC 2023 - All rights reserved

vii

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.~~

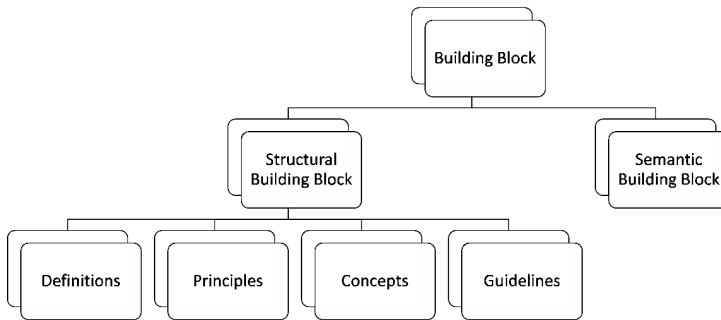
When a new technology or use case ~~become~~becomes prominent, novel approaches to assessments ~~taking into consideration should be defined, which take~~ existing frameworks ~~should be defined into consideration~~. The dynamic cycle of ~~technology~~technological development and integrated environments 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)~~ a) an inventory of uniform components of assessment-related standards, called ~~Building~~building blocks (BBs), and their structure;
- b) ~~b)~~ b) ontology capturing relationships among BBs;
- c) ~~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.~~

<https://standards.iteh.ai/catalog/standards/sist/b65f9299-5ebd-4c97-86c5-c>



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: English (United Kingdom)

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: cite_fig

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

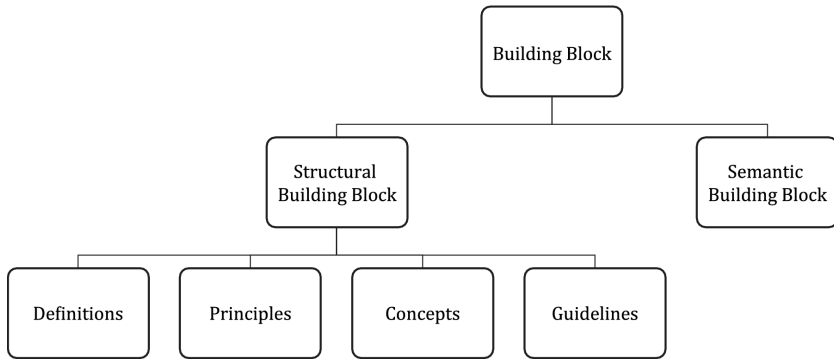
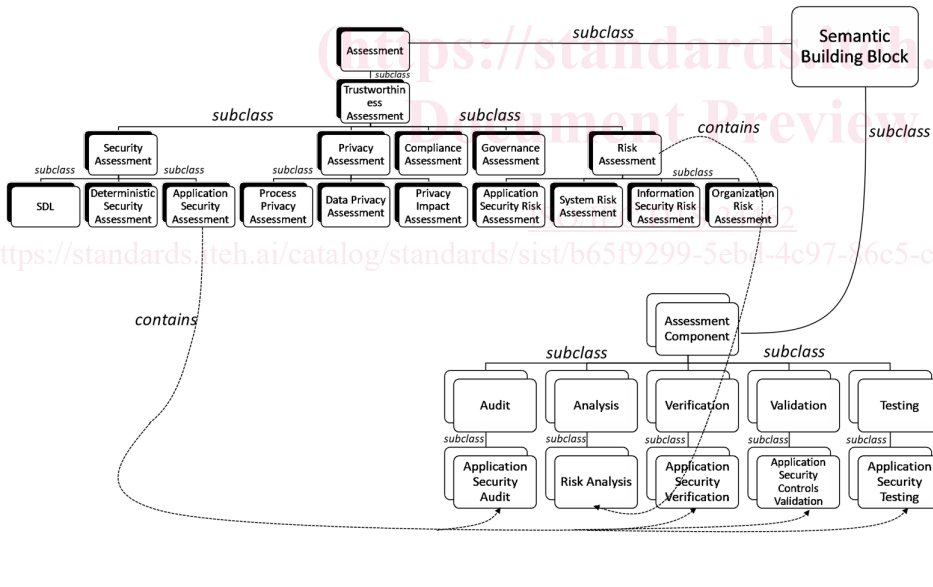
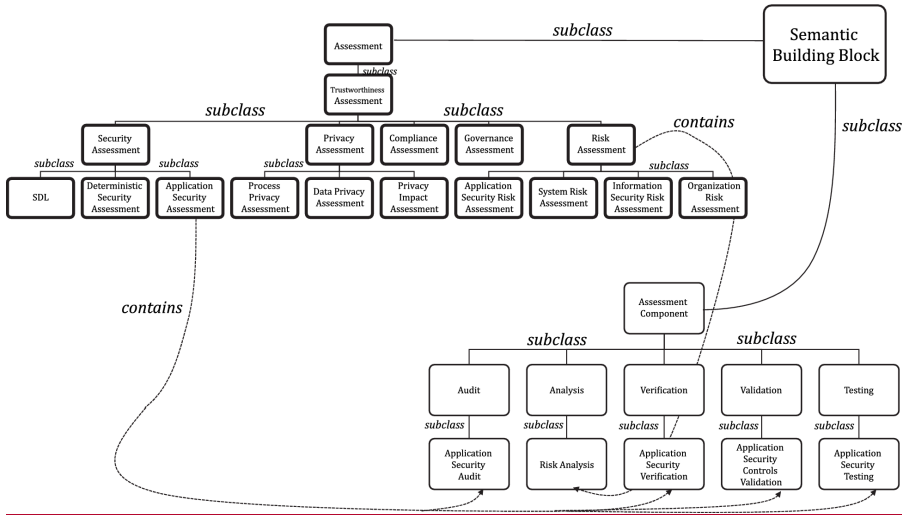


Figure 1 -- Top levels of the ontology

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



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

Figure 2 Semantic Building Block branch of the ontology

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

iteh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC DTS 24462

<https://standards.iteh.ai/catalog/standards/sist/b65f9299-5ebd-4c97-86c5-ce79278bee54/iso-iec-dts-24462>

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

Information Security, Cybersecurity, Privacy Protection and Risk Assessment — 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~~ 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~~ ISO Online browsing platform: available at <https://www.iso.org/obp>
- ~~IEC~~ 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 27034-1, ISO/IEC 27007-1, 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 ...

ISO/IEC DTS 24462:2023(E)

Formatted: Font: 12 pt

Formatted

Note 1 to entry: Examples of semantic building blocks can be found for instance in ISO/TR 11633-2:2009, 2-5:2021, ISO/IEC 29134:2017:2023, 3.7, ISO/IEC/IEEE 26514:2008:2022, 4.4, and ISO/IEC 27034-3:2018, 3.1.

Formatted

Formatted

3.3 assessment building block

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

Formatted

Formatted

Formatted

Formatted

Formatted

Note 1 to entry: ~~information~~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.

Formatted

Formatted

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

Formatted

Formatted

Formatted

Formatted

Formatted

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

Formatted

Formatted

Formatted

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

Formatted

[SOURCE: OWL-2 Web Ontology Language *Structural Specification and Functional Style Syntax Quick Reference Guide* (Second Edition) (11 December), 2012]]

Formatted

Formatted

3.6 datatype

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

Formatted

Formatted

Formatted

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.

Formatted

Formatted

[SOURCE: OWL-2 Web Ontology Language *Structural Specification and Functional Style Syntax Quick Reference Guide* (Second Edition) (11 December), 2012]]

Formatted

Formatted

3.7 extensible markup language XML

subset of the Standard Generalized Markup Language (SGML)

Formatted

Formatted

Formatted

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.

Formatted

Formatted

[SOURCE: OWL-2 Web Ontology Language *Structural Specification and Functional Style Syntax Quick Reference Guide* (Second Edition) (11 December), 2012]]

Formatted

3.8 individual

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

Formatted

Formatted

Formatted

Formatted