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)

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.

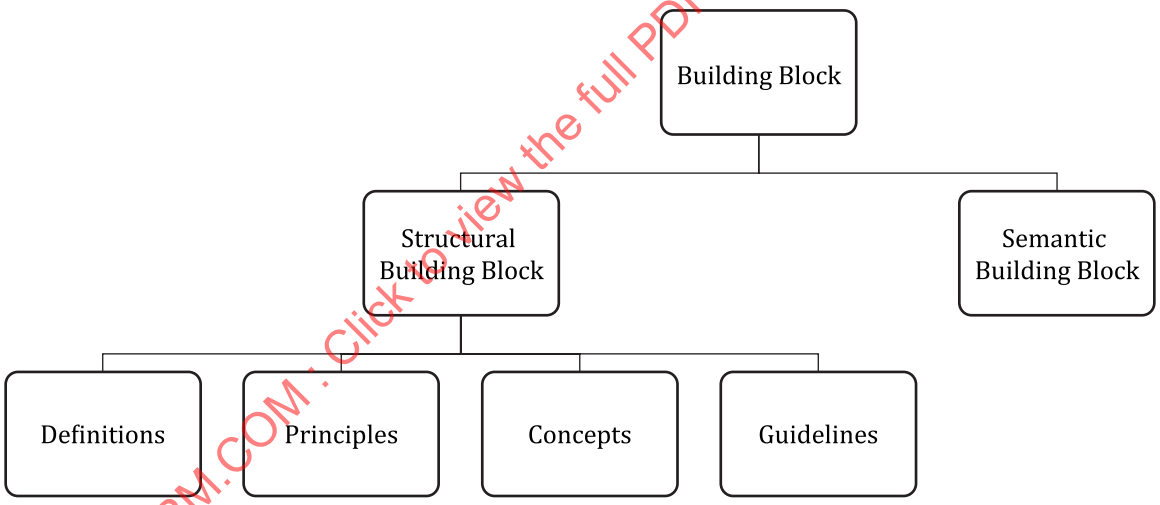

Figure 1 — Top levels of the ontology

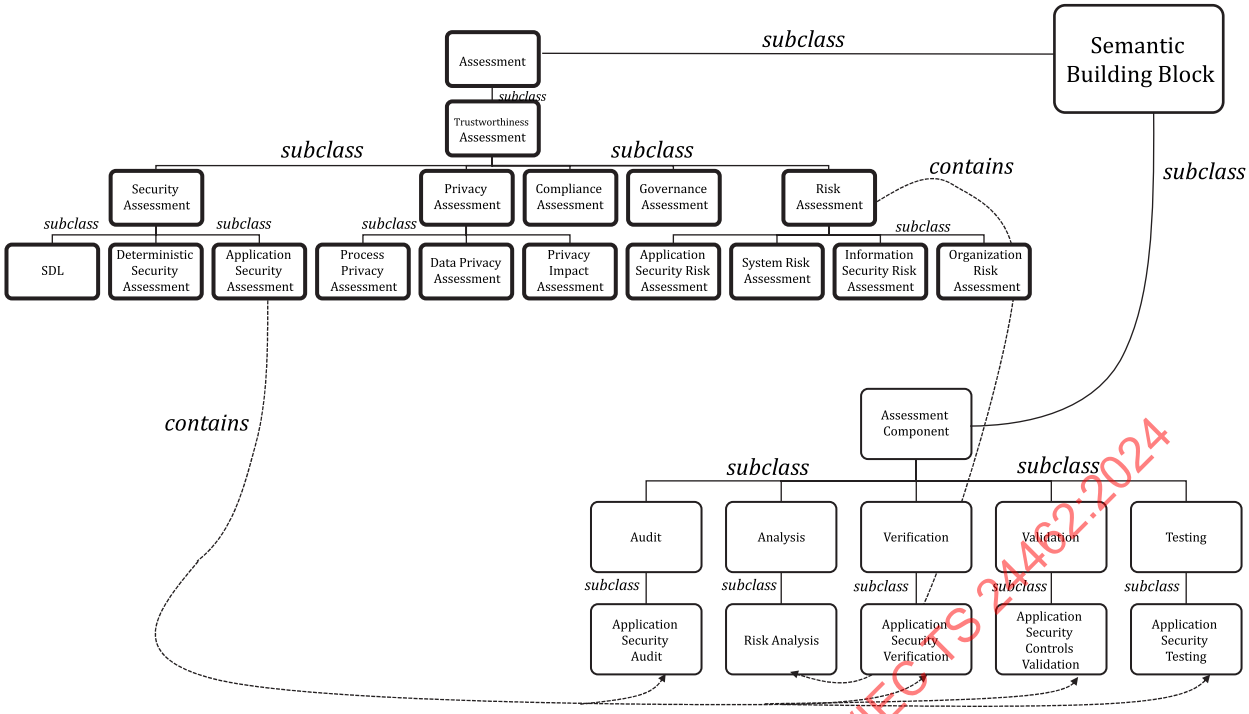

Figure 2 — Semantic Building Block branch of the ontology

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.

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).

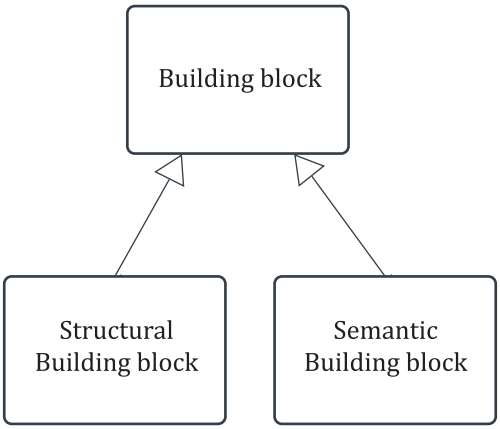

Figure 3 — BBs divided into structural and semantic BBs

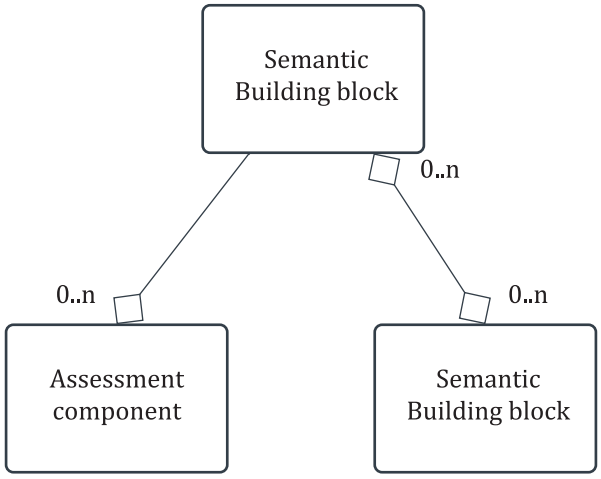

Figure 4 — Semantic building blocks

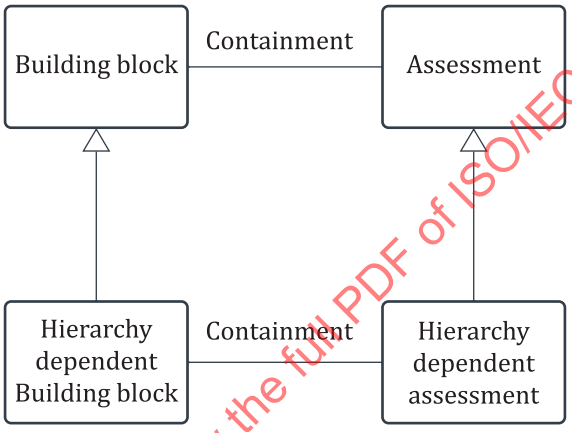

Figure 5 — Building block and assessment hierarchy

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

new assessment and the existing assessments are considered at the level of the semantic building blocks. Application security audit and application security testing are identified as relevant assessment component building blocks from the existing standard(s). These building blocks are then considered for inclusion in the standard. Additionally, the availability of machine-readable XML supports the automation of the process. The approach to automation has been demonstrated in a more general context in Reference [37].

7 Building blocks: collection and structure

7.1 General

The term building blocks (BBs) shall refer to structural components as well as semantic components. The inventory of BBs is provided later in Clauses 8, 9 and 10.

Structural BBs cover characteristics that are independent of the assessment type and are intended to capture kinds of information that is found in most standards. Examples of structural BBs include concepts, definitions and guidelines.

Semantic BBs shall be further divided into assessment and assessment component BBs. Assessment BBs can contain other semantic BBs, while assessment components should be atomic objects that are not further fragmented.

For the purpose of the ontology developed in this document, the inventory of assessment BBs (see Clause 9 for details) shall include:

a) security assessment;

b) privacy assessment;

c) compliance assessment;

d) governance assessment;

e) risk assessment.

These BBs can be further broken down. For example, security assessment can contain:

f) SDL (secure development lifecycle);

g) deterministic security assessment;

h) application security assessment.

The assessment component BBs can also be broken down. The current inventory of assessment component BBs and associated children shall include:

— audit;
  — application security audit;
— analysis;
  — risk analysis;
— verification;
  — application security verification;
— validation;
  — application security controls validation;
— testing;
  — application security testing.

Assessment BBs can contain one or more other semantic BBs. The application security assessment component can contain assessment components such as:

— application security audit;
— application security verification;
— application security controls validation;
— application security testing.

Each BB shall contain at a minimum: a name, a description, a source, and a creation date, where the creation date shall indicate the date in which the BB was introduced in the collection.

Examples of BBs, and XML encoding of BBs are presented in 7.2 to 7.6. In these examples, each BB term is represented by an ontological class with a matching individual. The properties provide the BBs with an adopted description and its source.

7.2 Application security assessment

Application security assessment is the evaluation of applications, with the intent of identifying vulnerabilities, and confirming that interactions with users, other applications and environments are secure.

The creation date is the publication date of this document.

See NIST SP 800-115:2008, Appendix C.

In this inventory, application security assessment is represented by an XML block as shown below. The properties provide the adopted description and source of the assessment.

```
<owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Assessment">
        <ts:adoptedDescription>Evaluation of applications with intent of identifying
vulnerabilities, and confirming interactions with users, other applications and environments
are secure.</ts:adoptedDescription>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
        <ts:adoptedDescriptionSource> NIST SP800-115:Appendix C </ts:adoptedDescription>
    </owl:NamedIndividual>
```

7.3 Risk assessment

Risk assessment covers risk identification, analysis and evaluation.

The creation date is the publication date of this document.

ISO 22734:2019, 3.30.

In this inventory, risk assessment is represented by an XML block as shown below. The properties provide the adopted description and source of the assessment.

```
     <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Risk_
Assessment">
        <ts:adoptedDescription> Assessment covering risk identification, analysis, and
evaluation.</ts:adoptedDescription>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
        <ts:adoptedDescriptionSource>NIST SPECIAL PUBLICATION 800-160, VOLUME 1  Appendix B</
ts:adoptedDescriptionSource>
    </owl:NamedIndividual>
```

Application security audit

Application security audit is the process through which it is determined if all application security controls (ASCs) have successfully passed their verification process.

The creation date is the publication date of this document.

See ISO/IEC 27034-3:2018, 3.1.

In this inventory, application security audit is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Audit">
        <ts:adoptedDescription>Process through which it is determined if all Application
Security Controls (ASC&amp;apos;s) have successfully passed their verification process.</
ts:adoptedDescription>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
        <ts:adoptedDescriptionSource> ISO/IEC 27034-3:2018: 3.1</ts:adoptedDescriptionSource>
    </owl:NamedIndividual>
```

7.4 Application security controls validation

Application security controls validation is the objective confirmation that all requirements for application security controls (ASC) have been fulfilled.

The creation date is the publication date of this document.

See ISO/IEC 27034-1 and ISO 9000:2015, 3.8.13.

In this inventory, application security controls validation is represented by an XML block as shown below. The properties provide the adopted description and source of the BB.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Controls_Validation">
        <ts:adoptedDescription> Objective confirmation that all requirements for Application
Security Controls (ASC) have been fulfilled. </ts:adoptedDescription>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
        <ts:adoptedDescriptionSource> ISO/IEC 27034-1:2011; ISO 9000:2015:3.8.13</
ts:adoptedDescriptionSource>
    </owl:NamedIndividual>
```

7.5 Risk analysis

Risk analysis is the process through which the level and nature of risk can be determined.

The creation date is the publication date of this document.

See ISO/Guide 73:2009, 3.6.1.

In this inventory, risk analysis is represented by an XML block as shown below. The properties provide the adopted description and source of the BB.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Risk_
Analysis">
        <ts:adoptedDescription> Process through which the level and nature of risk can be
determined.</ts:adoptedDescription>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
        <ts:adoptedDescriptionSource> ISO/Guide 73:2009: 3.6.1</ts:adoptedDescriptionSource>
    </owl:NamedIndividual>
```

8 Ontology capturing relationships among BBs

8.1 General

Ontologies are used to capture the salient aspects of a domain and to answer queries about them in a mathematically precise and explainable way. While ontologies can seem analogous to taxonomies, there are important distinctions. Similar to a taxonomy, an ontology provides uniform terminology for the domain of interest, assuring interoperability and accurate communication among researchers, operators, practitioners, regulators, and other interested parties. The ontology also captures the structural relationships from the domain at hand, e.g. an ontology individual John belongs to class software-developer and class software-developer is a subclass of class person. Differently from a taxonomy, an ontology can also include the specification of dependencies, constraints, and other rule-based relationships among entities in the model. Additionally, ontologies come with associated inference mechanisms that enable drawing conclusions over virtually arbitrary combinations of structural relationships, dependencies, constraints and rule-like relationships.

The BBs are organized according to these core criteria.

— BBs are hierarchically organized by a class-subclass relation.

— BBs are partitioned in structural and semantic categories. Structural BBs are found in many standards and cover concepts that are independent of the particular assessment type, such as definitions or principles. Semantic BBs describe specific types of assessment, such as privacy assessment or risk assessment, or parts thereof, such as risk analysis.

— Semantic BBs are further divided into assessments and “assessment components”. The distinguishing feature is that assessment components represent BBs of assessments that are not assessments themselves.

— The relationship between assessments and BBs that occur in them is captured by a containment relation.

— The containment relation is inherited. That is, if a BB class A contains a set of BBs, then any sub-class of A also contains those BBs.

— The ontology is subject to the following structural constraints:

  — Classes for structural BBs should not be subclasses of semantic BBs.

  — Classes for semantic BBs should not be subclasses of structural BBs.

  — A class should not be a subclass of multiple parent classes.

  — An individual should not belong to multiple classes.

Thus, the inventory and corresponding hierarchy are represented in the ontology as follows.

— All BBs are represented by ontology classes and by identically-named ontology individuals.

— The class-subclass relation between BBs is represented by the class-subclass relation between ontology classes that is built into ontologies.

— The containment relation is represented by an object property “contains”.

— The adopted description of a BB is represented by a data property “adoptedDescription” of type string. The source(s) of the description are represented by a data property “adoptedDescriptionSource”.

— Object property “subsumes” (with domain and range corresponding to the class of all BBs) and data properties “creationDate” and “endDate” (with the class of all BBs as domain and xsd:dateTime as the range) are introduced for managing the lifecycle of BBs. Property “subsumes” represents the fact that one BB subsumes another. Property “creationDate” specifies the creation time of a BB and “endDate” specifies its end date. More details on the lifecycle can be found in 8.7.

Figure 6 and Figure 7 provide an illustration of a representative hierarchy of BBs. Figure 6 depicts the top-level classes of the ontology. Figure 7 illustrates the semantic building block branch of the ontology, with its building blocks for assessments and assessment components.

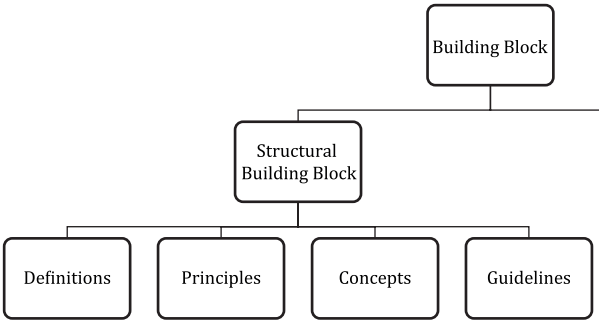

Figure 6 — Top levels of the ontology

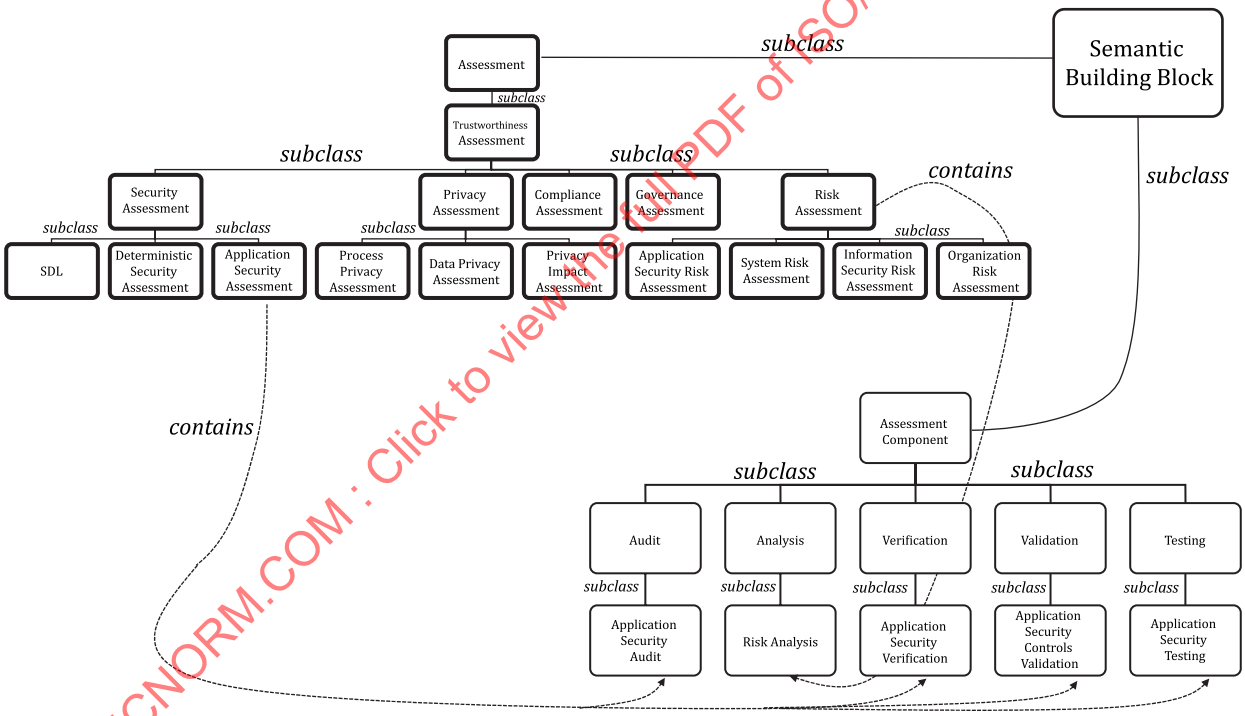

Figure 7 — Semantic building block branch of the ontology

The ontology is encoded using XML. The XML encoding uses tags indicating the type of XML object: owl:Class, owl:NamedIndividual, owl:ObjectProperty, or owl:DatatypeProperty. The rdf:about attribute defines the name of the object. The content enclosed by the beginning and ending tags provides further information, such as the parent class in a class-subclass relation (tag rdfs:subClassOf, used in conjunction with attribute rdf:resource, which indicates the name of the parent class), the parent class of an individual (tag rdf:type, also used in conjunction with rdf:resource), as well as information about the containment relation, the adopted definition and adopted definition’s source (tags ts-v04:contains, ts-v04:adoptedDescription and ts-v04:adoptedDescriptionSource, respectively). For example, Assessment is defined by the XML blocks:

```
    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#
Semantic_Building_Block"/ >
    </owl:Class>

    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Assessment">
        <rdf:type rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Assessment"/>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

where the first block states that Assessment is a class (first line), and that it is a subclass of class Semantic_ Building_Block (second line). The second block states that name Assessment is also associated with an individual (first line) of class Assessment (second line).

The relations of the ontology are defined by the following XML code:

```
    <owl:ObjectProperty rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#contains">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
        <rdfs:range rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
    </owl:ObjectProperty>

    <owl:ObjectProperty rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#subsumes">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
        <rdfs:range rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
    </owl:ObjectProperty>

    <owl:DatatypeProperty rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#adoptedDescription">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
    </owl:DatatypeProperty>

    <owl:DatatypeProperty rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#adoptedDescriptionSource">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
    </owl:DatatypeProperty>

    <owl:DatatypeProperty rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#creationDate">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
        <rdfs:range rdf:resource="http://www.w3.org/2001/XMLSchema#dateTime"/ >
    </owl:DatatypeProperty>

    <owl:DatatypeProperty rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#endDate">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
        <rdfs:range rdf:resource="http://www.w3.org/2001/XMLSchema#dateTime"/ >
    </owl:DatatypeProperty>
```

The first two blocks (ObjectProperty blocks) define the containment relation “contains” and relation “subsumes” as relations that hold between pairs of BB individuals. The remaining blocks (Datatype Property blocks) define the “adoptedDescription”, “adoptedDescriptionSource”, “creationDate”, and “endDate” relations.

In 8.2 to 8.6, examples of the XML encoding of BBs is provided. The complete encoding can be found in Clause 10.

8.2 Building block: application security assessment

A hierarchical placement of the application security assessment is a subclass of the security assessment. Application security assessment contains the BBs application security audit, application security controls validation, application security testing, and application security verification.

XML encoding:

```
    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Security_Assessment"/>
    </owl:Class>

    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Assessment">
        <rdf:type rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Assessment"/>
        <ts:adoptedDescription>Evaluation of applications with intent of identifying
vulnerabilities, and confirming interactions with users, other applications and environments
are secure.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource> NIST SP800-115:Appendix C </ts:adoptedDescription>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
        <ts:contains rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Audit"/>
        <ts:contains rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Controls_Validation"/>
        <ts:contains rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Testing"/>
        <ts:contains rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Verification"/>
    </owl:NamedIndividual>
```

The XML encoding can be explained as follows: the first three lines describe the ontology class associated with the BB and indicate of which BB it is a subclass. The next line, which contains tag “NamedIndividual”, states the name of the individual that represents the BB. The following line indicates its class. The lines with tags “adoptedDescription” and “adoptedDescriptionSource” encode the adopted description of the BB and the description’s source. The lines tagged with “contains” state that application security assessment contains BBs: application security audit, application security controls validation, application security testing, and application security validation.

8.3 Building block: risk assessment

A hierarchical placement of the risk assessment is as a subclass of the ICT assessment. Risk assessment contains the BB risk analysis.

XML encoding:

```
    <owl:Class rdf:about=”http://mbal.asklab.net/ontology-24462-current.owl#Risk_Assessment” >
        <rdfs:subClassOf rdf:resource=”http://mbal.asklab.net/ontology-24462-current.owl#ICT
Assessment”/ >
    </owl:Class>
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Risk_
Assessment">
        <rdf:type rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Risk_
Assessment"/>
        <ts:contains rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Risk_
Analysis"/>
        <ts:adoptedDescription>Overall process of risk identification, risk analysis, and risk
evaluation.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>NIST SPECIAL PUBLICATION 800-160, VOLUME 1  Appendix B</
ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

The first line states the name of the individual and the second line its class. The third line states that risk assessment contains a risk analysis BB (risk analysis is another individual). The fourth and fifth lines provide the adopted description of the BB and the source of the description.

8.4 Building block: application security audit

A hierarchical placement of the application security audit is as a subclass of audit.

XML encoding:

```
        <owl:Class rdf:about=”http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Audit”>
        <rdfs:subClassOf rdf:resource=”http://mbal.asklab.net/ontology-24462-current.
owl#Audit”/>
    </owl:Class>
    <owl:NamedIndividual rdf:about=”http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Audit”>
        <rdf:type rdf:resource=”http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Audit”/>
        <ts:adoptedDescription>Process through which it is determined if all Application
Security Controls (ASC&amp;apos;s) have successfully passed their verification process.</
ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC 27034</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

8.5 Building block: application security controls validation

A hierarchical placement of the application security controls validation is as a subclass of validation.

XML encoding:

```
    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Controls_Validation">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Validation"/>
    </owl:Class>

    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Controls_Validation">
        <rdf:type rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Controls_Validation"/>
        <ts:adoptedDescription>Objective confirmation that all requirements for Application
Security Controls (ASC) have been fulfilled.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC 27034-1:2011; ISO 9000:2015:3.8.13</
ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

8.6 Building block: risk analysis

A hierarchical placement of the risk analysis is as a subclass of analysis.

XML encoding:

```
    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Risk_Analysis">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Analysis"/>
    </owl:Class>

    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Risk_
Analysis">
        <rdf:type rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Risk_
Analysis"/>
        <ts:adoptedDescription>Process to comprehend the nature of risk and to determine the
level of risk</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/TS 13131:2014 3.5.3</ts:adoptedDescriptionSource>
```

```
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

8.7 Lifecycle of building blocks

The lifecycle of ontology building blocks is important to ensure consistency, as specified in ISO/IEC 21823-3. 8.8 describes how the ontology and its elements are used at different stages in the lifecycle.

8.8 Using BBs

8.8.1 General

8.8.2 to 8.8.4 describe the lifecycle of the ontology and building blocks. The intent of this document is to streamline the creation of assessments based on existing standards. It does not intend to amend or change the existing standards in any way. The example use cases explain the use of this document.

8.8.2 Using the ontology to structure an assessment based on an existing standard

1. Define the nature of the new assessment based on its objectives, e.g. security of eye level displays based on ISO/IEC 27034. The objectives should be defined in terms of classes in the ontology, e.g. risk assessment or governance assessment.
2. Use the ontology to assist in the creation of the description of the new form of assessment.
3. The building blocks under consideration should include semantic and structural building blocks.
4. The building blocks selected should inform a primary outline of the assessment.
5. Definitions and other information from the standard for which the assessment is created to include content (definitions, concepts, audience, etc.) should be used.
6. If desired, create tools to support the assessment or enable self-assessment under the standard, for which the assessment is created. Such tools can include automatic harvesting of building blocks or automatic comparison of building blocks.

The following is an example of the use of the ontology for this purpose:

a) The creators of the assessment define the focus of the assessment in question.

b) They pick structural and semantic building blocks from the ontology.

c) The ontology provides the initial outline, to speed up the assessment development process.

d) If automated tools have been set up, the building blocks can be harvested automatically and compared with building blocks used in other assessments.

e) An XML representation of the assessment can be created at the same time, based on the ontology, for further machine-readable applications.

The following is an example of how to create tools for automation. In order to speed up the development of the assessment and to ensure harmonization with other assessment under a certain standard, a tool can be created to fill the outline with the content of the building block from the standards in question and other standards documents, for example, definitions. The tool can also assist in the generation of the OWL2.0 machine readable version of the assessment.

8.8.3 Using the ontology to obtain components for an assessment based on a revised edition of a standard

1. Define the nature of the new standard assessment after the revision of the existing standard, e.g. assessment of eye level displays based on a revised edition of ISO/IEC 27034. The objectives should be mapped to the semantic building blocks, e.g. risk management.

2. Use the ontology to assist in the creation of the new standard assessment.
3. The building blocks under consideration should include semantic and structural building blocks.
4. The building blocks selected should form a primary outline of the assessment.
5. Definitions and other information from the standard, for which the assessment is created to include content (definitions, concepts, audience, etc,) should be used.
6. If needed, new building blocks specific to the new part of the standard should be created and added to the ontology.
7. If desired, create tools to support the assessment or enable self-assessment under the standard, for which the assessment is created.

8.8.4 Using the ontology to obtain structural components for an assessment based on the first edition of a standard

1. Define the nature of the new standard assessment based on the first edition of a standard, e.g. assessment of eye level displays based on the first edition of an ISO/IEC standard. The objectives should be mapped to the semantic building blocks, e.g. risk management.
2. Define the topical areas for the assessment, e.g. assessment for fully homomorphic encryption.
3. Use the ontology to assist in the creation of the new assessment standard.
4. The building blocks under consideration should include semantic and structural building blocks.
5. The building blocks selected should form a primary outline of the assessment.
6. If needed, new building blocks found in the new standard should be created and added to the ontology.
7. If desired, create tools to support the assessment or enable self-assessment under the standard, for which the assessment is created.

The following is an example of the use of the ontology for this purpose:

a) The creators of the assessment define the nature of the assessment.

b) They use the ontology to determine which semantic and structural building blocks (BBs) are needed.

c) The initial set of building blocks is used to create a preliminary outline.

d) Based on the outline, it is possible to harvest content, including definitions, from similar or adjacent standards and specifications.

e) Based on the outline and the ontology, additional building blocks are created if needed.

f) If automation tools are available, some of these steps can be automated.

The following is an example of how to create tools to harmonize information in the new standard assessment with existing standards and specifications:

g) Use or create a repository that contains the full text of relevant standards.

h) Build simple tools to locate information in structural and semantic building blocks present in different standards.

i) With the tools, identify differences in content that may require harmonization (e.g. definitions or processes).

9 Standard inventory of uniform components

9.1 Structural BBs

9.1.1 Description

Structural BBs are found in a majority of ICT assessment standards and cover concepts that are independent of the particular assessment type, such as definitions and principles.

9.1.2 Inventory

9.1.2.1 General

This clause provides the inventory of structural BBs.

9.1.2.2 Concepts BB

The concepts BB is a structural BB defining key concepts of an assessment.

In this inventory, concepts BB is represented by an XML block as shown below. The properties provide the adopted description and source of the BB.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Concepts_Building_Block">
        <ts:adoptedDescription> Structural BB defining key concepts of an assessment</
ts:adoptedDescription>
        <ts:adoptedDescriptionSource>WG</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.1.2.3 Definition BB

The definition BB provides a representation of a concept by an expression that describes it and differentiates it from related concepts. See ISO 1087:2019, 3.3.1.

In this inventory, definition BB is represented by an XML block as shown below. The properties provide the adopted description and source of the BB.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Definition_Building_Block">
        <ts:adoptedDescription> Structural building block defining key concepts of an
assessment</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO 1087:2019: 3.3.1</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.1.2.4 Guidelines BB

The guidelines BB captures a principle put forward to set standards or determine a course of action. This usually consists of a recommendation or advice without the requirement of law, however published guidelines can in some circumstances become a legal requirement. See ISO/TR 17427-10:2015, 2.6.

In this inventory, guidelines BB is represented by an XML block as shown below. The properties provide the adopted description and the source of the BB.

```
<owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Guidelines_
Building_Block">
        <ts:adoptedDescription>Principle put forward to set standards or determine a course
of action; usually, but not always, as a recommendation or advice without the requirement of
law but adherence to published guidelines may in some circumstances become a requirement of a
regulation.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/TR 17427-10:2015: 2.6</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.1.2.5 Principles BB

The principles BB is a structural BB that introduces fundamental, primary assumptions. See ISO/IEC 15944-5:2008, 3.80.

In this inventory, principles BB is represented by an XML block as shown below. The properties provide the adopted description and source of the BB.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Principles_Building_Block">
        <ts:adoptedDescription>Structural BB that introduces fundamental, primary
assumptions.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC 15944-5:2008: 3.80</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.2 Semantic BBs

Semantic BBs describe specific types of assessment, such as privacy assessment or risk assessment, or parts thereof, such as risk analysis. Semantic BBs are further divided in assessment BBs and assessment component BBs, where the latter are parts of assessments but are not assessments themselves.

9.3 Assessment BBs

9.3.1 Description

Assessment BBs are semantic BBs that describe an entire assessment.

9.3.2 Inventory

9.3.2.1 General

This clause provides the inventory of assessment BBs.

9.3.2.2 Application security assessment

The application security assessment BB captures the evaluation of applications with the intention of identifying vulnerabilities, and confirming that interactions with users, other applications and environments are secure.

See NIST SP 800-115, Appendix C.

In this inventory, application security assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
        <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Assessment">
        <ts:adoptedDescription>Evaluation of applications with intent of identifying
vulnerabilities, and confirming interactions with users, other applications and environments
are secure.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>NIST SP800-115:Appendix C</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.3 Application security risk assessment

The application security risk assessment BB corresponds to the second step of the Application Security Management Process (ASMP), which evaluates/assesses risks on the application level. See NIST SP 800-30, 8.2.1.

In this inventory, application security risk assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Risk_Assessment">
        <ts:adoptedDescription>Second step of the Application Security Management Process
(ASMP), which evaluates/assesses risks on the application level.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>NIST SP800-30: 8.2.1</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.4 Assessment

The assessment BB corresponds to the undertaking of an investigation in order to arrive at a judgement, based on evidence, of the suitability of a product.

In this inventory, assessment is represented by an XML block as shown below. The properties provide the adopted description and source of the BB.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Assessment">
        <ts:adoptedDescription>Undertaking of an investigation in order to arrive at a
judgement, based on evidence, of the suitability of a product.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>electropedia.org</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.5 Compliance assessment

The compliance assessment BB describes an assessment with the intent of determining whether the information security controls within a given organization remain both operational and effective. See ISO/IEC 29169:2016.

In this inventory, compliance assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Compliance_Assessment">
        <ts:adoptedDescription> Assessment with the intent of determining whether the
information security controls within a given organization remain both operational and
effective.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC 29169:2016(en)</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.6 Data privacy assessment

The data privacy assessment BB corresponds to the evaluation of the current state of an organization's data privacy, with the intent to implement a data security plan. See Reference [39].

In this inventory, data privacy assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
        <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Data_Privacy_Assessment">
        <ts:adoptedDescription>Evaluation of the current state of an organization&amp;apos;s data
privacy, with the intent to implement a data security plan.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>www.s21sec.com</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.7 Deterministic security assessment

The deterministic security assessment BB described an assessment that assumes certainty of meeting all security requirements. See ISO/TR 10400:2018, NIST SP 800-53A.

In this inventory, deterministic security assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
        <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#
Deterministic_Security_Assessment" >
        <ts:adoptedDescription>Assessment assuming certainty of meeting all security
```

```
requirements.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/TR 10400:2018;NIST SP 800-53A</
ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.8 Governance assessment

The governance assessment BB described an assessment with a focus on measuring the performance, accountability, responsiveness and capacity of formal institutions. See Reference [40].

In this inventory, governance assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Governance_Assessment">
        <ts:adoptedDescription>A focus on measuring the performance, accountability,
responsiveness and capacity of formal institutions.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>gsdrc.org</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.9 Information security risk assessment

The information security risk assessment BB describes an assessment conducted to identify potential security risks or threats with the intent of mitigating harm to sensitive data. See Reference [41].

In this inventory, information security risk assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
<owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Information_
Security_Risk_Assessment">
        <ts:adoptedDescription>Assessment to identify potential security risks or threats with
the intent of mitigating harm to sensitive data.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>TBD</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.10 Organization risk assessment

The organization risk assessment BB corresponds to the assessment of all security and privacy risks within an organization. See NIST SP800-37 r2: 3.1.

In this inventory, Organization Risk Assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Organization_Risk_Assessment">
        <ts:adoptedDescription>Assessment of all security and privacy risks within an
organization.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>adapted from NIST SP800-37 r2: 3.1</
ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.11 Privacy assessment

The privacy assessment BB describes an assessment conducted with the intent of ensuring all applicable privacy laws, policies, and processes are adhered to within a specific system. See NIST SP 800-53A: 2.1.

In this inventory, Privacy Assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Privacy_
Assessment">
        <ts:adoptedDescription>Assessment with the intent of ensuring all applicable privacy
laws, policies, and processes are adhered to within a specific system.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>NIST SP 800-53A: 2.1</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.12 Privacy impact assessment

The privacy impact assessment BB describes the evaluation of potential privacy impacts as related to the processing of personally identifiable information. See ISO/IEC 29134:2023, 3.7.

In this inventory, Privacy Impact Assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Privacy_
Impact_Assessment">
        <ts:adoptedDescription>Evaluation of potential privacy impacts as related to the
processing of personally identifiable information.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC 29134:2023: 3.7</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.13 Process privacy assessment

The process privacy assessment BB corresponds to an assessment of the current privacy state of a process, activity, or set of interrelated activities. See ISO 9000 and ISO/IEC 29134.

In this inventory, Process Privacy Assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Process_
Privacy_Assessment">
        <ts:adoptedDescription>Assessment of the current privacy state of a process, activity,
or set of interrelated activities.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO 9000:2015;ISO/IEC 29134:2023</
ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.14 Risk assessment

The risk assessment BB describes an assessment covering risk identification, analysis, and evaluation. See ISO 22734:2019, 3.30.

In this inventory, risk assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Risk_
Assessment">
        <ts:adoptedDescription>Assessment covering risk identification, analysis, and
evaluation.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>NIST SPECIAL PUBLICATION 800-160, VOLUME 1  Appendix B</
ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.15 Security development lifecycle (SDL)

The security development lifecycle BB describes a method through which the security and privacy is ensured through all phases of development. See ISO/IEC 27034.

In this inventory, SDL is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Security_Development_Lifecycle">
        <ts:adoptedDescription>A method through which the security and privacy is assured
through all phases of development.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC 27034</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.16 Security assessment

The security assessment BB captures an assessment with the intent of identifying security vulnerabilities and risks.

In this inventory, security assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
<owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Security_
Assessment">
        <ts:adoptedDescription>Assessment with the intent of identifying security
vulnerabilities and risks.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource> wikipedia.org</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.17 System risk assessment

The system risk assessment BB describes a risk assessment with the express purpose of allowing all stakeholders to make a final decision on all necessary security controls. See NIST SP 800-30, 2.4.3.

In this inventory, system risk assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#System_
Risk_Assessment">
        <ts:adoptedDescription>Risk assessment with the express purpose of allowing
all stakeholders to make a final decision on all necessary security controls.</
ts:adoptedDescription>
        <ts:adoptedDescriptionSource>NIST SP800-30:2.4.3</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.3.2.18 Trustworthiness assessment

The trustworthiness assessment BB describes techniques, mechanisms, and approaches used to evaluate trustworthiness of a system, environment, organization, technology or products. The approaches include, but are not limited to risk analysis, SDL, governance, deterministic testing, and other. See ISO/IEC 20924:2021.

In this inventory, trustworthiness assessment is represented by an XML block as shown below. The properties provide the assessment's adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Trustworthiness_Assessment">
        <ts:adoptedDescription>Techniques, mechanisms, and approaches used to evaluate
trustworthiness of a system, environment, organization, technology or products.</
ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC 20924:2021</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.4 Assessment component BBs

9.4.1 Description

For the purpose of this document, assessment component BBs are semantic BBs that are not assessments themselves.

9.4.2 Inventory

9.4.2.1 General

9.2.4 provides the inventory of assessment component BBs.

9.4.2.2 Analysis

The analysis BB describes a process focused on specifying types of users and how to best fulfil their informational needs. See ISO/IEC/IEEE 26514:2022, 3.1.5.

In this inventory, analysis is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Analysis">
        <ts:adoptedDescription>Process focused on specifying types of users and how to best
fulfil their informational needs.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC/IEEE 26514:2022,3.1.5 </
ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.4.2.3 Application security audit

The application security audit BB describes a process through which it is determined if all application security controls (ASCs) have successfully passed their verification process. See ISO/IEC 27034-3:2018, 3.1.

In this inventory, application security audit is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Audit">
        <ts:adoptedDescription>Process through which it is determined if all Application
Security Controls (ASC&amp;apos;s) have successfully passed their verification process.</
ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC 27034-3:2018: 3.1</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.4.2.4 Application security controls validation

The application security controls validation BB describes a validation aimed at providing an objective confirmation that all requirements for application security controls (ASC) have been fulfilled. See ISO/IEC 27034-1 and ISO 9000:2015, 3.8.13.

In this inventory, application security controls validation is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Controls_Validation">
        <ts:adoptedDescription>Objective confirmation that all requirements for Application
Security Controls (ASC) have been fulfilled.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC 27034-1:2011; ISO 9000:2015:3.8.13</
ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.4.2.5 Application security testing

The application security testing BB describes an evaluation of the overall efficacy of a computer system or a network's security.

In this inventory, application security testing is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <<owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Testing">
        <ts:adoptedDescription>Evaluation of the overall efficacy of a computer system or
networks&amp;apos security.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>OWASP.org</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.4.2.6 Application security verification

The application security verification BB describes the process of reviewing and verifying security activity outcomes of an application by performing the associated verification-measurement activity. See ISO/IEC 27034-3:2018, 3.2.

In this inventory, Application Security Verification is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <owl:NamedIndividual rdf:about=”http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Verification”>
        <ts:adoptedDescription>Process of reviewing and verifying security activity outcomes
of an application by performing the associated verification-measurement activity.</
ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC 27034-3:2018: 3.2</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.4.2.7 Assessment component

Assessment component BBs are semantic BBs that are not assessments themselves.

In this inventory, Assessment Component is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Assessment_Component">
        <ts:adoptedDescription>Represent BB of assessments that are not assessments
themselves.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>WG</ts:adoptedDescriptionSource>
    </owl:NamedIndividual>
```

9.4.2.8 Audit

The audit BB describes the independent process for the express purpose of obtaining all relevant information as to the fulfilment, or lack thereof, of specified requirements.

In this inventory, audit is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Audit">
        <ts:adoptedDescription>Independent process for the express purpose of obtaining all
relevant information as to the fulfilment, or lack thereof, of specified requirements.</
ts:adoptedDescription>
        <ts:adoptedDescriptionSource>electropedia.org</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.4.2.9 Risk analysis

The risk analysis BB describes the process through which the level and nature of risk can be determined. See ISO/Guide 73:2009, 3.6.1.

In this inventory, risk analysis is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Risk_
Analysis">
        <ts:adoptedDescription>Process through which the level and nature of risk can be
determined.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/Guide 73:2009: 3.6.1</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.4.2.10 Testing

The testing BB represents the determination of one or more characteristics of an object of conformity assessment, according to a relevant procedure.

In this inventory, Testing is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Testing">
        <ts:adoptedDescription>Determination of one or more characteristics of an object of
conformity assessment, according to a procedure.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>electropedia.org</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.4.2.11 Validation

The validation BB corresponds to an evidence-based confirmation that an application meets specified requirements for its intended use.

In this inventory, validation is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Validation">
        <ts:adoptedDescription>Evidence based confirmation that an application meets specified
requirements for its intended use.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>electropedia.org</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

9.4.2.12 Verification

The verification BB corresponds to an evidence-based confirmation that a requirement has been fulfilled. See ISO/IEC 12207:2017, 3.1.72.

In this inventory, verification is represented by an XML block as shown below. The properties provide the BBs adopted description and its source.

```
    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Verification">
        <ts:adoptedDescription>Evidence based confirmation that a requirement has been
fulfilled.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC 12207:2017: 3.1.72</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>
```

10 Complete XML encoding

The following is the complete XML encoding of the ICT Trustworthiness (security, privacy, risk, and governance) assessment ontology.

```
<?xml version="1.0"?>
<rdf:RDF xmlns="http://mbal.asklab.net/ontology-24462-current.owl#"
     xml:base="http://mbal.asklab.net/ontology-24462-current.owl"
     xmlns:owl="https://www.w3.org/2002/07/owl#"
     xmlns:rdf="https://www.w3.org/1999/02/22-rdf-syntax-ns#"
     xmlns:xml="https://www.w3.org/XML/1998/namespace"
     xmlns:xsd="https://www.w3.org/2001/XMLSchema#"
     xmlns:rdfs="https://www.w3.org/2000/01/rdf-schema#"
     xmlns:ts="http://mbal.asklab.net/ontology-24462-current.owl#">
    <owl:Ontology rdf:about="http://mbal.asklab.net/ontology-24462-current.owl"/>


    <!--
////////////////////////////////////////////////////////////////////////////////////
    //
    // Object Properties
    //
////////////////////////////////////////////////////////////////////////////////////
     -->
```

```
    <!-- http://mbal.asklab.net/ontology-24462-current.owl#contains -- >

    <owl:ObjectProperty rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#contains">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
        <rdfs:range rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
    </owl:ObjectProperty>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#subsumes -- >

    <owl:ObjectProperty rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#subsumes">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
        <rdfs:range rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
    </owl:ObjectProperty>


    <!--
///////////////////////////////////////////////////////////////////////////////////
    //
    // Data properties
    //
/////////////////////////////////////////////////////////////////////////////////
     -->



        <!-- http://mbal.asklab.net/ontology-24462-current.owl#adoptedDescription -- >

    <owl:DatatypeProperty rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#adoptedDescription">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
    </owl:DatatypeProperty>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#adoptedDescriptionSource -- >

    <owl:DatatypeProperty rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#adoptedDescriptionSource">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
    </owl:DatatypeProperty>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#creationDate -- >

    <owl:DatatypeProperty rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#creationDate">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
        <rdfs:range rdf:resource="http://www.w3.org/2001/XMLSchema#dateTime"/>
    </owl:DatatypeProperty>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#endDate -- >

    <owl:DatatypeProperty rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#endDate">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
        <rdfs:range rdf:resource="http://www.w3.org/2001/XMLSchema#dateTime"/>
    </owl:DatatypeProperty>


    <!-- http://www.w3.org/2002/07/owl#topDataProperty -->
```

```
    <rdf:Description rdf:about="http://www.w3.org/2002/07/owl#topDataProperty">
        <rdfs:domain rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Building_
Block"/>
    </rdf:Description>


    <!--
///////////////////////////////////////////////////////////////////////////////////////
    //
    // Classes
    //
///////////////////////////////////////////////////////////////////////////////////////
     -->



    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Analysis -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Analysis">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Assessment_Component"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Application_Security_Assessment
-- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Security_Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Application_Security_Audit -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Audit">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Audit"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Application_Security_Controls_
Validation -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Controls_Validation">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Validation"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Application_Security_Testing -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Testing">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Testing"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Application_Security_Verification
-- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Verification">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Verification"/>
    </owl:Class>
```

```
    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Semantic_Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Assessment_Component -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Assessment_
Component">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Semantic_Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Audit -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Audit">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Assessment_Component"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Building_Block -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Building_Block"/>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Compliance_Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Compliance_
Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Trustworthiness_Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Concepts -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Concepts">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Structural_Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Data_Privacy_Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Data_Privacy_
Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Privacy_Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Definitions -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Definitions">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Structural_Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Deterministic_Security_Assessment
-- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Deterministic_
Security_Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Security_Assessment"/>
```

```
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Governance_Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Governance_
Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Trustworthiness_Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Guidelines -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Guidelines">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Structural_Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Information_Security_Risk_
Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Information_
Security_Risk_Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Risk_Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Misc -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Misc">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Structural_Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Organization_Risk_Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Organization_Risk_
Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Risk_Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Principles -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Principles">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Structural_Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Privacy_Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Privacy_
Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Trustworthiness_Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Privacy_Impact_Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Privacy_Impact_
Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Privacy_Assessment"/>
    </owl:Class>
```

```
    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Process -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Process">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Structural_Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Process_Privacy_Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Process_Privacy_
Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Privacy_Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Purpose -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Purpose">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Structural_Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Risk_Analysis -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Risk_Analysis">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Analysis"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Risk_Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Risk_Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Trustworthiness_Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#SDL -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#SDL">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Security_Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Scope -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Scope">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Structural_Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Security_Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Security_
Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Trustworthiness_Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Semantic_Building_Block -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Semantic_Building_
Block">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
```

```
owl#Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Structural_Building_Block -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Structural_
Building_Block">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#System_Risk_Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#System_Risk_
Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Risk_Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Test -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Test">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Structural_Building_Block"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Testing -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Testing">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Assessment_Component"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Trustworthiness_Assessment -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Trustworthiness_
Assessment">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Assessment"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Validation -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Validation">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Assessment_Component"/>
    </owl:Class>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Verification -- >

    <owl:Class rdf:about="http://mbal.asklab.net/ontology-24462-current.owl#Verification">
        <rdfs:subClassOf rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Assessment_Component"/>
    </owl:Class>


    <!--
///////////////////////////////////////////////////////////////////////////////////
    //
    // Individuals
    //
///////////////////////////////////////////////////////////////////////////////////
     -->
```

```
    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Analysis -- >

    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Analysis">
        <rdf:type rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Analysis"/>
        <ts:adoptedDescription>Process focused on specifying types of users and how to best
fulfil their informational needs.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC/IEEE 26514:2022 3.1.5 </
ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Application_Security_Assessment
-- >

    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Assessment">
        <rdf:type rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Assessment"/>
        <ts:contains rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Audit"/>
        <ts:contains rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Controls_Validation"/>
        <ts:contains rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Testing"/>
        <ts:contains rdf:resource="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Verification"/>
        <ts:adoptedDescription rdf:datatype="http://www.w3.org/2001/
XMLSchema#string">Evaluation of applications with intent of identifying vulnerabilities, and
confirming interactions with users, other applications and environments are secure.</
ts:adoptedDescription>
        <ts:adoptedDescriptionSource rdf:datatype="http://www.w3.org/2001/
XMLSchema#string">NIST SP800-115:Appendix C</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Application_Security_Audit -- >

    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Audit">
        <rdf:type rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Audit"/>
        <ts:adoptedDescription>A systematic, independent and documented process used to
determine if all Application Security Controls (ASC&amp;apos;s) identified by the Level of Trust
of an application, have been implemented and successfully passed their verification process.</
ts:adoptedDescription>
        <ts:adoptedDescriptionSource>ISO/IEC 27034</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Application_Security_Controls_
Validation -- >

    <owl:NamedIndividual rdf:about="http://mbal.asklab.net/ontology-24462-current.
owl#Application_Security_Controls_Validation">
        <rdf:type rdf:resource="http://mbal.asklab.net/ontology-24462-current.owl#Application_
Security_Controls_Validation"/>
        <ts:adoptedDescription rdf:datatype="http://www.w3.org/2001/
XMLSchema#string">Objective confirmation that all requirements for Application Security
Controls (ASC) have been fulfilled.</ts:adoptedDescription>
        <ts:adoptedDescriptionSource rdf:datatype="http://www.w3.org/2001/
XMLSchema#string">ISO/IEC 27034-1:2011; ISO 9000:2015:3.8.13</ts:adoptedDescriptionSource>
        <ts:creationDate>[release date of this TS]</ts:creationDate>
    </owl:NamedIndividual>


    <!-- http://mbal.asklab.net/ontology-24462-current.owl#Application_Security_Testing -- >
```