☒ Annex(es) are included with this proposal (give details)

Detailed outline of the proposed document.

ISO #####-#:####(X)

ISO/IEC JTC 1/SC 27/WG 3

Secretariat: DIN

Title Information security – Security techniques –Ontology for ICT Trustworthiness Assessment

WD/CD/DIS/FDIS stage

Warning for WDs and CDs

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

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

To help you, this guide on writing standards was produced by the ISO/TMB and is available at https://www.iso.org/iso/how-to-write-standards.pdf

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

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee *[or Project Committee]* ISO/TC *[or ISO/PC]* ###, *[name of committee]*, Subcommittee SC ##, *[name of subcommittee]*.

This second/third/… edition cancels and replaces the first/second/… edition (ISO #####:####), which has been technically revised.

The main changes compared to the previous edition are as follows:

— xxx xxxxxxx xxx xxxx

A list of all parts in the ISO ##### series can be found on the ISO website.

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.

Introduction

The proposed technical specification defines structural and semantic building blocks for ICT trustworthiness assessment, as well as an ontology that organizes them. The objective is to provide a consistent view of this space and an extensible model to understand its structure. In addition to traditional-form deliverables, the ontology will also be produced in a machine-readable form, opening the door to using this technical specification mechanically in a variety of use cases. The proposed technical specification does not intend to edit or modify any existing standards.

There are a large number of international standards with "trustworthiness" assessment components that have been created via an open standards development process by the international community of technical experts. There are also a large number of standards-based assessments focusing on various aspects of trustworthiness of a services, organization, product, or technology components, such as governance, secure development lifecycle, deterministic testing, adherence to specifically designated best practices, and other foundations. Finally, the body of knowledge includes a number of best practices documents, definitions of principles or position papers in the domain of trustworthiness assessment.

When a new technology or use case become prominent, best practices are needed to ensure the best possible environment and functionality. It is especially important for areas associated with security, privacy, and risk management as well as more general trustworthiness. However, access to the resources available, especially in emerging areas, to develop new standards and update the old ones are scarce (see, e.g., [1]). At the same time, the dynamic cycle of technology development, and the massive need for integration, where independent technology domains have to be connected, as well as the global nature of the digital infrastructure, elevated the need for international standards. The standardization community has struggled to respond to the current needs in a timely fashion due to insufficiency of resources and the relatively slow pace of international standardization associated with the formal standardization process.

Typically, such best practices are developed from scratch based on shared principles and are focused on one domain (e.g., governance or deterministic testing; software applications, or IoT systems). While it is possible for a technology provider or an organization to assess their environment in multiple domains based on several approaches, this requires significant effort, most of it preparatory, since focused assessments are created based on a broad framework, such as Protection Profiles in Common Criteria. This model has been accepted, with good reason, and works well for a number of objectives and environments, but it covers only a fraction of the assessment needs.

As the body of available standards continued to grow and the diversification of the ICT space intensified, it has become difficult to ensure consistency of approaches used in similar standards. 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 the similar technologies are used. Standards bodies, such as ISO, have consistently taken steps to improve the level of documentation harmonization, enforcing unified formats, rules for references, and consistent terminology, including ISO 704 "Terminology: Principles and Methods". Other ISO publications, e.g., ISO 860:2007 stress that "Harmonization starts at the

concept level." However, the outcomes of these efforts are difficult to expand beyond terminology and a small set of other defined components.

On the other end of the problem, it would be attractive for standards bodies to create frameworks for new assessments with greater efficiency.

Although the formal process for standardization, a process based on collaboration and consensus, will always require a significant amount of time, we believe that its efficiency and consistency can be increased by employing a broader standardization of document components. In addition to speeding up the development of consistent standards with aligned requirements, this can also lead to the development of more focused and context specific requirements, especially in the area of ICT assessment, which is the purpose of the study described in this document. (A formal report on this project was published in the proceedings of the SSR-2018 conference.)

This proposal stems from the observation that a number of structured assessment-related standards have repeated, similar, but non-identical components. The purpose of this proposal is to:

1. Define a standardized inventory of uniform components of assessment-related standards, called building blocks, and their structure.
2. Create an ontology indicating relationships among building blocks.
3. Provide guidelines for using standardized building blocks.

It is worth noticing that significant work was done in the International Standards bodies with regard to using ontologies for the harmonization of concepts within specific domains, e.g., as described in ISO/IEC SC N604, the study period report focusing on this very issue. Standardization work using ontologies to improve the efficiency of building, analyzing, and implementing standards has been more limited because it is more innovative, but it has been covered in research literature. [9] used ontologies to link standards tags relating properties of the IoT space to the descriptions of the functions they denote. In the medical field, [10] used an ontology to standardize and classify adverse drug reactions based on Adverse Drug Reaction Classification System. [11] described how ontologies could be used to map existing security standards, and [12] developed ontologies to formalize security knowledge and make it more amenable to various analyses. [13] developed an ontology for ISO software engineering standards, complete with a prototype demonstrating their approach.

Title Information Security – Security Techniques – Ontology for ICT Trustworthiness Assessment

1 Scope

We define ICT trustworthiness as a concept associated with various types of best practices and assessments, such as governance, secure development lifecycle, security evaluation, risk assessment. The proposed Technical Specification defines an inventory of building blocks of assessment-related standards, an ontology that organizes it, use cases applicable to these areas, and a methodology for creating the inventory and the ontology.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

RDF (Resource Description Framework) Specification v. 1.1 – Feb 2014, W3C

OWL (Web Ontology Language) specification v.2 – Dec 2012, W3C

Extensible Markup Language (XML) 1.0 (Fifth Edition) – Nov 2008, W3C

3 Terms and definitions

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

3.1
Trustworthiness
Demonstrable likelihood that the system performs according to designed behavior under a typical set of conditions as evidenced by its characteristics, such as safety, security, privacy, reliability and resilience (from NIST CPS Framework v1.0).

3.2
Trustworthiness assessment
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 (Secure Development Lifecycle), governance, deterministic testing, and other.

3.3
Building block
A component that fits with others to form a whole.

3.4
Ontology
A set of concepts and categories in a subject area or domain that shows their properties and the relations between them (Oxford Dictionary). In computer science, an ontology is associated with a standardized format that facilitates exchange of information.

3.5
Individual
The basic, "ground level" components of an ontology. The individuals in an ontology may include concrete objects such as people, animals, tables, automobiles, molecules, and planets, as well as abstract individuals such as numbers and words (although there are differences of opinion as to whether numbers and words are classes or individuals). (Wikipedia)

3.6
Class
A collection of individuals of an ontology.

3.7

Subclass
A subset of a class.

3.8
Property
An attribute describing how individuals of an ontology are related to other individuals or classes.

4 Building blocks: Methodology and Their Structural/Semantic Properties

This section will include methodology for defining building blocks, building blocks types, structural requirements, and properties of building blocks.

There are repeated, similar, but not identical building blocks in existing normative and non-normative documents associated with trustworthiness assessment. Each building block is a portion of text that describes a particular component of a document. A building block could also represent a diagram or a figure. It could be associated with a structural component (e.g., introduction), a concept (e.g., principle or audit), or a process.

The building blocks can be organized hierarchically over multiple layers based on their level of specificity. The top layer may correspond to the structural building block types, i.e. syntactic components of assessments that are included in assessment standards and best practices, such as "definition," "guideline," or "process." Each structural building block can be further refined into a set of semantic building blocks, e.g., related to scope or topical areas.

The following is a list of examples of structural building blocks that could be included in the inventory. They are inspired by, and/or present in, various documents we analyzed.

- Concepts – concepts used throughout the document.
- Definitions – definitions of notions.
- Guidelines – guidelines pertaining to the standard.
- Principles – guiding principles used in the document.
- Process – a process (or task) being standardized.
- Purpose – purpose of the document or of a part of the document.
- Test – one or more tests being standardized, possibly used as part of a process.
- Misc – general-purpose block

In addition to the structural building blocks, which highlight the syntactic characteristics of standards, the inventory contains semantic building blocks. These are produced by linking structural building blocks with specific concepts relevant to trustworthiness assessments. For instance, a semantic building block "risk management principle" can be derived by linking a structural building block (principle) with a concept "risk management." The table that follows provides an initial inventory of semantic building blocks, and includes examples of documents where such blocks are found (last column). The table includes examples of building block types from deeper levels of the potential hierarchy, labeled "Sub-Sub-block." While some types of building blocks are not directly present in the documents analyzed, they are listed to highlight these seemingly valuable generalizations. The information provided is limited and is intended only for illustration purposes, but we believe that it is sufficient to demonstrate the possibilities for standardization of building blocks.

Structural Building Block Type	Semantic Building Block Sub-Type	Example Source Document
Principles	Audit Principles	[2]
Principles	Testing Principles	[3]
Principles	Evaluation Principles	[4]
Principles	Application Security Principles	[2]
Principles	Risk Assessment Principles	[5]
Guidelines	Management Guidelines	[6]
Guidelines	Evaluation Guidelines	[6]
Guidelines	Vulnerability Assessment Guidelines	[3]
Concepts	Information Security Concepts	[7]
Concepts	Background Concepts	[7]
Concepts	Security Threat Concepts	[8]
Process	Initiation Process Sub-Sub-block: Audit Initiation Process	 [6]
Process	Preparation Process	

	Sub-Sub-block: Audit Preparation Process	[6]
	Sub-Sub-block: Risk Management Preparation Process	[5]
Process	Implementation Process	[5]
	Sub-Sub-block: Control Implementation Process	[7]
	Sub-Sub-block: Audit Implementation Process	[6]
Process	Monitoring Process	[7]
Process	Certification Process	[2]
Process	Risk Management Process	[2]
Process	Verification Process	[2]
Process	Assessment Process	
	Sub-Sub-block: Risk Assessment Process	[5]
	Sub-Sub-block: Scope Assessment Process	[5]
		[5]

	Sub-Sub-block: Consequence Assessment Process	

The ultimate objective of the proposed Technical Specification is the development of an ontology of building blocks, which formally captures the relationships between building blocks. Fig. 1 shows a sample ontology that was created for a subset of the building blocks identified in our preliminary study. In it, building block types are formalized as classes of the ontology. Sub-blocks are represented by means of the class-subclass relationship.

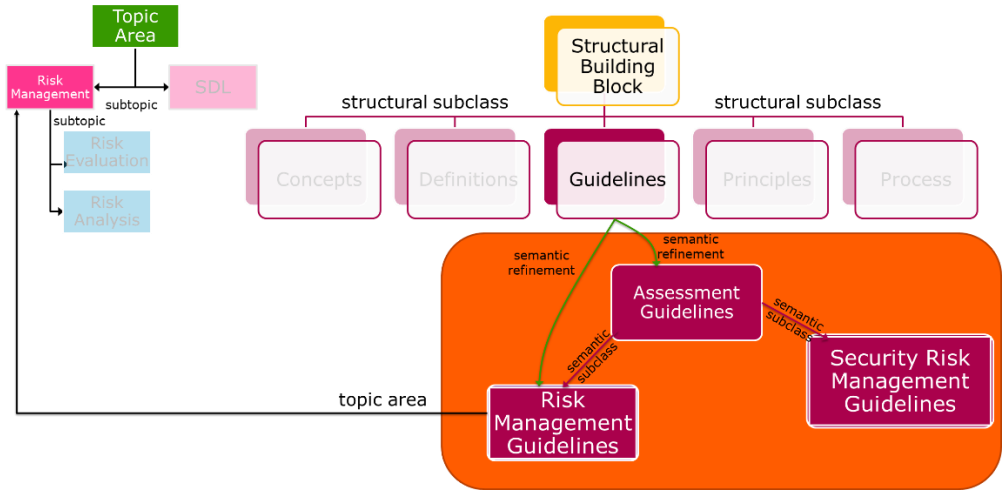

Fig. 1. Ontological representation of example building blocks

In the ontology, each class and its relationships to other classes are encoded in a standard way by a corresponding XML block. For instance, the AssessmentGuidelines sub-type can be encoded by:

```
<owl:Class rdf:about="http://webprotege.stanford.edu/AssessmentGuidelines">

     <rdfs:subClassOf
rdf:resource="http://webprotege.stanford.edu/GuidelinesBB"/>

</owl:Class>
```

Note the rdfs:subClassOf tag, which expresses the fact that AssessmentGuidelines is a sub-type of the Guidelines building block type. A more advanced example of XML can be found in Fig. 5.

While we propose RDF and OWL as the foundational formats for the ontology and building blocks at this stage, other formats can be derived from these via an automated translation.

Furthermore, properties and individuals can be used to provide a richer description of building blocks. Fig. 2 illustrates an advanced example including a number of ontology individuals and properties.

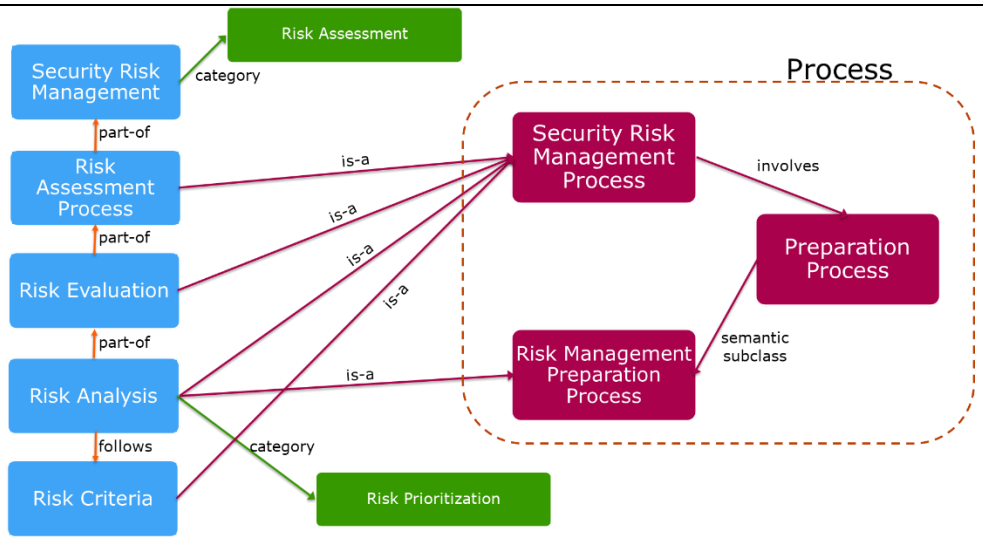

Fig. 2. Advanced example usage of the ontology

5 Inventory of building blocks

This section will include an inventory of building blocks defined according to the methodology proposed in Section 4.

6 Ontology: Methodology and Structure

The proposed Technical Specification also includes a methodology for identifying building blocks and constructing the corresponding methodology. Below is a preliminary outline of the methodology. The approach will be further refined and tested as part of the proposed work.

Structural Segmentation Phase. In the first phase of the methodology, existing documents are analyzed. The general kinds of clauses and sub-clauses, as well as other relevant portions of the narrative, are used to determine the types of structural building blocks. For instance, the standard documents cited above contain an abundance of clauses discussing guidelines, hence the guidelines building block type. Process clauses are also frequent, hence the process building block type.

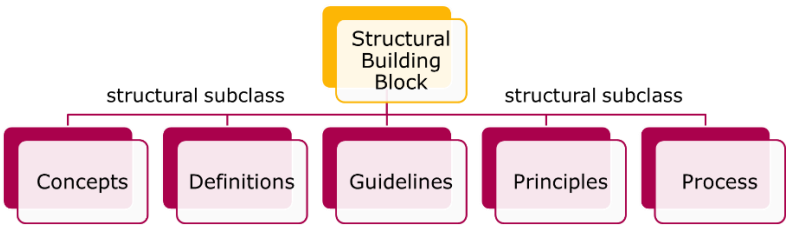

Fig. 3. Possible outcome of the Structural Segmentation Phase

Topic Area Identification Phase. In the next phase, the documents are analyzed to identify topic areas relevant to ICT trustworthiness assessment. Topic areas are defined as knowledge areas forming large domains in the area of trustworthiness assessment, e.g., risk management,

audit, or secure development lifecycle (SDL), to which semantic concepts belong. For instance, an analysis of example documents has identified, among others:

- Risk Management
- Risk Evaluation
- Risk Analysis
- SDL

Topic areas can be for instance defined using statistical methods over a representative set of documents. Using subject matter expert knowledge, the areas are then organized hierarchically; for example, Risk Evaluation and Risk Analysis can be viewed as a sub-topic of Risk Management, yielding:

- Risk Management
  - Risk Evaluation
  - Risk Analysis
- SDL

Fig. 4 visually illustrates a small sample of a potential outcome of this phase. Note that topic areas can be further grouped into categories. An example of such categories, for illustration purposes only, is visible in Fig. 2.

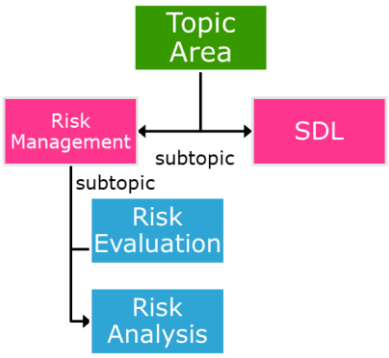

Fig. 4. Possible outcome of the Topic Area Identification Phase

Semantic Segmentation Phase. Next, the types of semantic building blocks are defined by linking structural building blocks with concepts from topic areas relevant to trustworthiness assessment. For instance, in the table below, semantic building block "Risk Management Process" is derived by linking structural building block "Process" with concept "Risk Management." Next, both structural and semantic building blocks are organized in an ontology, where building blocks are represented as classes and appropriate subclasses. A sample hierarchy may contain for instance:

- **Guidelines**
  - Assessment Guidelines
    - Risk Assessment Guidelines
  - Audit Guidelines
- **Process**
  - Assessment Process
    - Risk Assessment Process
  - Audit Process

as well as all other meaningful combinations. In the above example, the structural building blocks are highlighted in bold and serve as ancestor classes for the semantic blocks. Note how the

hierarchical organization of topic areas is reflected in the hierarchical organization of semantic building blocks. A sample outcome of the Semantic Segmentation Phase is shown in Fig. 1.

Generalization and Refinement Phase. Finally, subject matter expert knowledge is used to generalize and refine the ontology. This results in the inclusion of building blocks that are not found in documents, but are, according to expert knowledge, valuable generalizations of existing building blocks.

7 Proposed Ontology

This section will present the ontology.

8 Guidelines for the Use of the Ontology and Inventory of Building Blocks

This section will define how the inventory of building blocks and ontology can be used.

9 Use Cases and Potential Applications

This section will define use cases to demonstrate the use of the ontology and building blocks.

New technology area (for illustration only)

The use of AI in analyzing a computing environment becomes pervasive. The organizations need to select a trustworthy set of tools that fits their needs. An assessment is created that includes several categories:

- SDL processes of the providers of AI tools
- Privacy requirements
- A few tests under the security evaluation of the tools and their results
- Requirements for cryptography used by the providers
- Risk assessment requirements

Each area is built out of standard building blocks to create a template. The template is then filled with the content consistent with the assessment objectives.

New Use Case (for illustration only).

Financial organizations begin to utilize blockchain as a key tool for identity proofing. An assessment is build based on the objectives of the evaluation.

- Privacy requirements
- Compliance with the ISO 307 consensus protocol standards
- SDL processes of providers
- A few tests under the security evaluation of the implementation
- Requirements for Cloud security
- Requirements for cryptography used by the providers
- Risk assessment requirements

Each area is built out of standard building blocks to create a template. The template is then filled with the content consistent with the assessment objectives

Potential Use Case: Comparison of Existing Standards (for illustration only).

A user might want to identify the typical components of existing frameworks. Using the proposed technical specification, this is accomplished by identifying the building block types of the various parts of the available standards documents and then linking them through the ontology and its power of generalization. For an illustration, suppose that two frameworks are under consideration and that the following building block types from the proposed technical specification have been identified in them. Note that, where relevant, we also provide ancestors of the building block types as might be found in the proposed ontology.

Framework A

- Scope Assessment Process [clause 6.1]
- Risk Management Preparation Process (subclass of Preparation Process in the ontology) [clause 8.4.2]
- Risk Assessment Trigger Definition Process (subclass of Trigger Definition Process in the ontology, in turn subclass of Metrics Definition Process) [clause 6.4]
- Risk Assessment Process [clause 8.3.3]
- Stakeholder Approval Process (subclass of Approval Process) [clause 9.6.2]

Framework B

- Audit Objective Definition Process (subclass of Objective Definition Process in the ontology, in turn subclass of Metrics Definition Process) [clause 5.2]
- Manager Role Definition Process (subclass of Human Role Definition Process) [clause 5.3.1]
- Scope Assessment Process [clause 5.3.3]
- Risk Assessment Process [clause 5.3.4]
- Audit Implementation Process (subclass of Implementation Process) [clause 5.4]
- Audit Preparation Process (subclass of Preparation Process) [clause 6.3]

The following building block types occur in both lists and are thus obvious matches:

- Scope Assessment Process
- Risk Assessment Process
- Consequence Assessment Process

In addition to these matches, commonalities can also be identified through the higher-level classes of the ontology. For instance, Risk Management Preparation Process (Framework A) and Audit Preparation Process (Framework B) are both sub-types of Preparation Process. This demonstrates how the generalizing capabilities of the ontology allow one to bridge the surface-level differences between the documents. From the above lists, it is thus possible to identify the additional shared building blocks:

- Preparation Process
- Metrics Definition Process
- Implementation Process

Bibliography

[1] Boje, D. M. (Ed.). (2015). *Organizational change and global standardization: Solutions to standards and norms overwhelming organizations*. Routledge.

[2] ISO/IEC 27034, Information technology -- Security techniques -- Application security

[3] ISO/IEC 19792, Information technology -- Security techniques -- Security evaluation of biometrics

[4] ISO/IEC 15408, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

[5] ISO/IEC 27005, Information technology -- Security techniques -- Information security risk management

[6] ISO/IEC 27007, Information technology -- Security techniques -- Guidelines for information security management systems auditing

[7] ISO/IEC 27000, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

[8] ISO/IEC 27036, Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts

[9] Huang, Y., & Li, G. (2010). A semantic analysis for internet of things. In Intelligent computation technology and automation (ICICTA), 2010 international conference on (Vol. 1, pp. 336-339). IEEE.

[10] Cai, M. C., Xu, Q., Pan, Y. J., Pan, W., Ji, N., Li, Y. B., & Ji, Z. L. (2014). ADReCS: an ontology database for aiding standardization and hierarchical classification of adverse drug reaction terms. *Nucleic acids research*, 43(D1), D907-D913.

[11] Ramanauskaitė, S., Olifer, D., Goranin, N., & Čenys, A. (2013). Security ontology for adaptive mapping of security standards. *International Journal of Computers, Communications & Control (IJCCC)*, *8*(6), 813-825.

[12] Fenz, S., & Ekelhart, A. (2009). Formalizing information security knowledge. In Proceedings of the 4th international *Symposium on information, Computer, and Communications Security (pp. 183-194)*. ACM.

[13] Gonzalez-Perez, C., Henderson-Sellers, B., McBride, T., Low, G. C., & Larrucea, X. (2016). An Ontology for ISO software engineering standards: 2) Proof of concept and application. *Computer Standards & Interfaces*, 48, 112-123.

Additional information/questions

This appendix shows the XML representation of the ontology from Fig. 2. The representation was generated by the WebProtégé tool.

```
<?xml version="1.0"?>

<rdf:RDF xmlns="http://webprotege.stanford.edu/project/uiqsMk9z3Tzexx0FZiECd#"

     xml:base="http://webprotege.stanford.edu/project/uiqsMk9z3Tzexx0FZiECd"

     xmlns:webprotege="http://webprotege.stanford.edu/"

     xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"

     xmlns:owl="http://www.w3.org/2002/07/owl#"

     xmlns:xml="http://www.w3.org/XML/1998/namespace"

     xmlns:xsd="http://www.w3.org/2001/XMLSchema#"

     xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#">

    <owl:Ontology
rdf:about="http://webprotege.stanford.edu/project/uiqsMk9z3Tzexx0FZiECd"/>









    <!--


////////////////////////////////////////////////////////////////////////////////
///////

    //

    // Object Properties

    //


////////////////////////////////////////////////////////////////////////////////
///////

     -->
```

```
    <!-- http://webprotege.stanford.edu/R8DxK18cZNDyuuCxeZCxmyf -->


    <owl:ObjectProperty
rdf:about="http://webprotege.stanford.edu/R8DxK18cZNDyuuCxeZCxmyf">

        <rdfs:subPropertyOf
rdf:resource="http://www.w3.org/2002/07/owl#topObjectProperty"/>

        <rdfs:domain
rdf:resource="http://webprotege.stanford.edu/RfBn5aNHfrDDFMXGE7DlT9"/>

        <rdfs:range
rdf:resource="http://webprotege.stanford.edu/RfBn5aNHfrDDFMXGE7DlT9"/>

        <rdfs:label>part-of</rdfs:label>

    </owl:ObjectProperty>







    <!-- http://webprotege.stanford.edu/RCi625zhGwjShw2BsIbyzo3 -->


    <owl:ObjectProperty
rdf:about="http://webprotege.stanford.edu/RCi625zhGwjShw2BsIbyzo3">

        <rdfs:subPropertyOf
rdf:resource="http://www.w3.org/2002/07/owl#topObjectProperty"/>

        <rdfs:domain
rdf:resource="http://webprotege.stanford.edu/RfBn5aNHfrDDFMXGE7DlT9"/>

        <rdfs:range
rdf:resource="http://webprotege.stanford.edu/RDwdEITeUvbtMBco1XRCxZQ"/>

        <rdfs:label>category</rdfs:label>

    </owl:ObjectProperty>
```

```
    <!-- http://webprotege.stanford.edu/RDs9uwZwMQjwbMdmH4RmE2Z -->


    <owl:ObjectProperty
rdf:about="http://webprotege.stanford.edu/RDs9uwZwMQjwbMdmH4RmE2Z">

        <rdfs:subPropertyOf
rdf:resource="http://www.w3.org/2002/07/owl#topObjectProperty"/>

        <rdfs:domain
rdf:resource="http://webprotege.stanford.edu/RfBn5aNHfrDDFMXGE7DlT9"/>

        <rdfs:range
rdf:resource="http://webprotege.stanford.edu/RfBn5aNHfrDDFMXGE7DlT9"/>

        <rdfs:label>follows</rdfs:label>

    </owl:ObjectProperty>







    <!--


////////////////////////////////////////////////////////////////////////////////
///////

    //

    // Data properties

    //


////////////////////////////////////////////////////////////////////////////////
///////

     -->
```

```
    <!-- http://webprotege.stanford.edu/Ru15YEKU4rhbbGvnhN05GJ -->



    <owl:DatatypeProperty
rdf:about="http://webprotege.stanford.edu/Ru15YEKU4rhbbGvnhN05GJ">

        <rdfs:subPropertyOf
rdf:resource="http://www.w3.org/2002/07/owl#topDataProperty"/>

        <rdfs:label>has-title</rdfs:label>

    </owl:DatatypeProperty>









    <!--


//////////////////////////////////////////////////////////////////////////////
///////

    //

    // Classes

    //


//////////////////////////////////////////////////////////////////////////////
///////

     -->









    <!-- http://webprotege.stanford.edu/R82nZ0cFaduz9xlq68YpwVH -->



    <owl:Class
rdf:about="http://webprotege.stanford.edu/R82nZ0cFaduz9xlq68YpwVH">
```

```
        <rdfs:subClassOf
rdf:resource="http://webprotege.stanford.edu/R8ZjfCF9pA1aIrtIPXLcPpA"/>

        <rdfs:label>PreparationProcess</rdfs:label>

    </owl:Class>







    <!-- http://webprotege.stanford.edu/R8ZjfCF9pA1aIrtIPXLcPpA -->



    <owl:Class
rdf:about="http://webprotege.stanford.edu/R8ZjfCF9pA1aIrtIPXLcPpA">

        <rdfs:subClassOf
rdf:resource="http://webprotege.stanford.edu/RfBn5aNHfrDDFMXGE7DlT9"/>

        <rdfs:label>SemanticBuildingBlock</rdfs:label>

    </owl:Class>







    <!-- http://webprotege.stanford.edu/R9nV8M0GOsefl4qEwuIQC9H -->



    <owl:Class
rdf:about="http://webprotege.stanford.edu/R9nV8M0GOsefl4qEwuIQC9H">

        <rdfs:subClassOf
rdf:resource="http://webprotege.stanford.edu/R82nZ0cFaduz9xlq68YpwVH"/>

        <rdfs:label
rdf:datatype="http://www.w3.org/2001/XMLSchema#string">SecurityRiskManagementPro
cess</rdfs:label>

    </owl:Class>
```

```
    <!-- http://webprotege.stanford.edu/RB5quDfYvMScNzOpN76IBkl -->


    <owl:Class
rdf:about="http://webprotege.stanford.edu/RB5quDfYvMScNzOpN76IBkl">

        <rdfs:subClassOf
rdf:resource="http://webprotege.stanford.edu/R82nZ0cFaduz9xlq68YpwVH"/>

        <rdfs:label
rdf:datatype="http://www.w3.org/2001/XMLSchema#string">RiskManagementPreparation
Process</rdfs:label>

    </owl:Class>







    <!-- http://webprotege.stanford.edu/RDwdEITeUvbtMBco1XRCxZQ -->


    <owl:Class
rdf:about="http://webprotege.stanford.edu/RDwdEITeUvbtMBco1XRCxZQ">

        <rdfs:subClassOf rdf:resource="http://www.w3.org/2002/07/owl#Thing"/>

        <rdfs:label>Category</rdfs:label>

    </owl:Class>







    <!-- http://webprotege.stanford.edu/RfBn5aNHfrDDFMXGE7DlT9 -->


    <owl:Class
rdf:about="http://webprotege.stanford.edu/RfBn5aNHfrDDFMXGE7DlT9">

        <rdfs:subClassOf rdf:resource="http://www.w3.org/2002/07/owl#Thing"/>

        <rdfs:label>BuildingBlock</rdfs:label>
```

```
    </owl:Class>




    <!--


//////////////////////////////////////////////////////////////////////////////
///////

    //

    // Individuals

    //


//////////////////////////////////////////////////////////////////////////////
///////

     -->









    <!-- http://webprotege.stanford.edu/R7c50oKrlKwqT2zjCK1INY1 -->



    <owl:NamedIndividual
rdf:about="http://webprotege.stanford.edu/R7c50oKrlKwqT2zjCK1INY1">

        <webprotege:Ru15YEKU4rhbbGvnhN05GJ
rdf:datatype="http://www.w3.org/2001/XMLSchema#string">Guidance    on    managing
information security risks and opportunities</webprotege:Ru15YEKU4rhbbGvnhN05GJ>

        <rdfs:label>iso-iec27005</rdfs:label>

    </owl:NamedIndividual>
```

```
    <!-- http://webprotege.stanford.edu/R8qOu2TrMXNaGkyas9ZILHp -->


    <owl:NamedIndividual
rdf:about="http://webprotege.stanford.edu/R8qOu2TrMXNaGkyas9ZILHp">

        <rdf:type
rdf:resource="http://webprotege.stanford.edu/R9nV8M0GOsefl4qEwuIQC9H"/>

        <rdfs:label>RiskCriteria</rdfs:label>

    </owl:NamedIndividual>







    <!-- http://webprotege.stanford.edu/R9wOQAaOUjF6eacCCACgqrH -->


    <owl:NamedIndividual
rdf:about="http://webprotege.stanford.edu/R9wOQAaOUjF6eacCCACgqrH">

        <webprotege:R8DxK18cZNDyuuCxeZCxmyf
rdf:resource="http://webprotege.stanford.edu/R7c50oKrlKwqT2zjCK1INY1"/>

        <rdfs:label>clause8</rdfs:label>

    </owl:NamedIndividual>







    <!-- http://webprotege.stanford.edu/RB91fh9a4UzeMPbst0BgauS -->


    <owl:NamedIndividual
rdf:about="http://webprotege.stanford.edu/RB91fh9a4UzeMPbst0BgauS">

        <rdfs:label>iso-iec27007</rdfs:label>

    </owl:NamedIndividual>
```

```
    <!-- http://webprotege.stanford.edu/RBGKGKqfvXlNZqjVu39Exxa -->


    <owl:NamedIndividual
rdf:about="http://webprotege.stanford.edu/RBGKGKqfvXlNZqjVu39Exxa">

        <rdf:type
rdf:resource="http://webprotege.stanford.edu/R9nV8M0GOsefl4qEwuIQC9H"/>

        <webprotege:R8DxK18cZNDyuuCxeZCxmyf
rdf:resource="http://webprotege.stanford.edu/RCfYE40kODxBeInstODsfOh"/>

        <rdfs:label>RiskAssessmentProcess</rdfs:label>

    </owl:NamedIndividual>







    <!-- http://webprotege.stanford.edu/RCfYE40kODxBeInstODsfOh -->


    <owl:NamedIndividual
rdf:about="http://webprotege.stanford.edu/RCfYE40kODxBeInstODsfOh">

        <rdf:type
rdf:resource="http://webprotege.stanford.edu/RfBn5aNHfrDDFMXGE7DlT9"/>

        <webprotege:RCi625zhGwjShw2BsIbyzo3
rdf:resource="http://webprotege.stanford.edu/RUR4hlVkKytbgbwc9xFjCY"/>

        <rdfs:label>SecurityRiskManagement</rdfs:label>

    </owl:NamedIndividual>







    <!-- http://webprotege.stanford.edu/RDWN3rdDHALk9yK1M1sp6m -->
```

```
    <owl:NamedIndividual
rdf:about="http://webprotege.stanford.edu/RDWN3rdDHALk9yK1M1sp6m">

        <webprotege:R8DxK18cZNDyuuCxeZCxmyf
rdf:resource="http://webprotege.stanford.edu/R9wOQAaOUjF6eacCCACgqrH"/>

        <rdfs:label>clause8.4</rdfs:label>

    </owl:NamedIndividual>







    <!-- http://webprotege.stanford.edu/RDyKMANp1rT40U1h9wxAJlY -->



    <owl:NamedIndividual
rdf:about="http://webprotege.stanford.edu/RDyKMANp1rT40U1h9wxAJlY">

        <rdf:type
rdf:resource="http://webprotege.stanford.edu/R9nV8M0GOsefl4qEwuIQC9H"/>

        <webprotege:R8DxK18cZNDyuuCxeZCxmyf
rdf:resource="http://webprotege.stanford.edu/RBGKGKqfvXlNZqjVu39Exxa"/>

        <rdfs:label>RiskEvaluation</rdfs:label>

    </owl:NamedIndividual>







    <!-- http://webprotege.stanford.edu/RDybGTYVYlSSVNbVYXo3gJm -->



    <owl:NamedIndividual
rdf:about="http://webprotege.stanford.edu/RDybGTYVYlSSVNbVYXo3gJm">

        <webprotege:R8DxK18cZNDyuuCxeZCxmyf
rdf:resource="http://webprotege.stanford.edu/RDWN3rdDHALk9yK1M1sp6m"/>

        <rdfs:label>clause8.4.1</rdfs:label>
```

```
    </owl:NamedIndividual>




    <!-- http://webprotege.stanford.edu/RUR4hlVkKytbgbwc9xFjCY -->


    <owl:NamedIndividual
rdf:about="http://webprotege.stanford.edu/RUR4hlVkKytbgbwc9xFjCY">

        <rdf:type
rdf:resource="http://webprotege.stanford.edu/RDwdEITeUvbtMBco1XRCxZQ"/>

        <rdfs:label>RiskAssessment</rdfs:label>

    </owl:NamedIndividual>




    <!-- http://webprotege.stanford.edu/RdnRvfPBANK4H25alSY2RN -->


    <owl:NamedIndividual
rdf:about="http://webprotege.stanford.edu/RdnRvfPBANK4H25alSY2RN">

        <rdf:type
rdf:resource="http://webprotege.stanford.edu/RDwdEITeUvbtMBco1XRCxZQ"/>

        <rdfs:label>RiskPrioritization</rdfs:label>

    </owl:NamedIndividual>




    <!-- http://webprotege.stanford.edu/RhRv1QlZSii9m8MZ0XfKg6 -->
```

```
    <owl:NamedIndividual
rdf:about="http://webprotege.stanford.edu/RhRv1QlZSii9m8MZ0XfKg6">

        <rdf:type
rdf:resource="http://webprotege.stanford.edu/R9nV8M0GOsefl4qEwuIQC9H"/>

        <webprotege:R8DxK18cZNDyuuCxeZCxmyf
rdf:resource="http://webprotege.stanford.edu/RDyKMANp1rT40U1h9wxAJlY"/>

        <webprotege:RCi625zhGwjShw2BsIbyzo3
rdf:resource="http://webprotege.stanford.edu/RdnRvfPBANK4H25alSY2RN"/>

        <webprotege:RDs9uwZwMQjwbMdmH4RmE2Z
rdf:resource="http://webprotege.stanford.edu/R8qOu2TrMXNaGkyas9ZILHp"/>

        <rdfs:label>RiskAnalysis</rdfs:label>

    </owl:NamedIndividual>

</rdf:RDF>
```

Fig. 5. XML representation of the ontology from Fig. 2.