Towards the Ontology of ISO/IEC 27005:2011 Risk Management Standard

V. Agrawal

NTNU, Norwegian University of Science and Technology, Gjøvik, Norway
e-mail: vivek.agrawal@ntnu.no

Abstract

The purpose of this paper is to present a solution to manage the concepts related to ISO/IEC 27005:2011 standard in such a way that different stakeholders could access and understand them without misleading their meanings. This paper presents an ontology to structure and organize core concepts of risk assessment phase of ISO/IEC 27005:2011 standard. The method of ontology development ontology follows seven steps guideline. A case scenario of a health clinic is developed to apply the proposed ontology where each entity and relation of the ontology is described. The paper provides a reference point for professionals and researchers by presenting an ontology to describe various concepts of ISO/IEC 27005:2011 in the field of information security risk management.

Keywords

ISO/IEC 27005:2011, Ontology, Security Ontology, Risk Management

1. Introduction

A professional risk practitioner or a security expert in an organization usually carries out the task of ISRM. Most of the risk practitioners or security expert follow their own interpretation of the security standards based on their subjective experience (Pereira and Santos, 2012). In the risk management task, wrong decisions are often made by risk practitioners and other stakeholders (decision maker, product owner) due to the lack of knowledge about the security domain, assets, potential countermeasures of the organization (Arbanas and Čubrilo, 2015). The main reason behind this problem is the confusion among risk practitioners and users as the security terminology is not well defined (Singhal and Wijesekera, 2010), (Herzog et al., 2007). Managers in an organization mainly take the decision related to a risk management task. Managers do not have complete understanding of the underlying IT infrastructure and concepts related to a risk management task. An ontology can mitigate the above mentioned problem by providing a common repository of precise definition of entities and their relationships (Singhal and Wijesekera, 2010). The term *ontology* comes from the Greek words *Ontos* (being) and *logos* (word). Currently, there are several definitions of ontology in the literature, and there is no standard definition of ontology. However, we adopted the definition of ontology for our work from (Ehrig, 2006), (Nguyen et al., 2011). It defines ontology as, "An ontology is a formal, explicit specification of a conceptualization of common areas of interest." *Conceptualization* denotes an abstract world; *explicit* means that the elements/entities must be clearly defined, without any ambiguity; *formal* means that

the definition must be machine-readable. *Shared* indicates that an ontology captures consensual knowledge. *Common* means that a group must accept the given ontology. An *area of interest* indicates that an ontology should not try to capture the knowledge of the entire world, but model only relevant part of a particular domain (Arbanas and Čubrilo, 2015). In this context, we propose an ontology for ISO/IEC 27005:2011 (27005, 2011) standard (it will be called as ISO27005 from now onwards in this paper) to visualize the core concepts and their relation in a formal and structured format to provide better communication, re-usability, high level reasoning and better decision-making. ISO27005 standard provides guidelines for information security Risk Management. This standard builds on the knowledge concepts, models, processes and terminologies of ISO/IEC 27001. It assists implementation by taking a risk management approach.

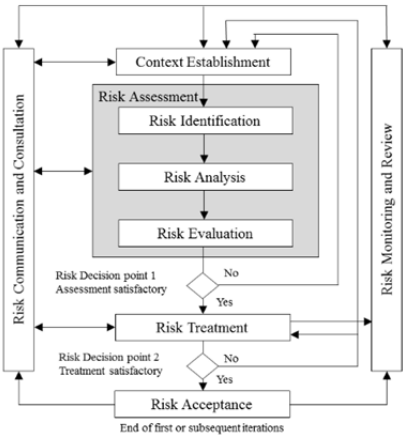

Figure 1: Overview of ISO27005, taken from (27005, 2011)

The structure of the paper is as follows: Section 2 includes a list of work that identified the challenge in risk management and indicated a need of formal and structured way to represent different concepts. Section 3 presents the proposed ontology for ISO27005 standard and describes its development through seven steps guideline. Section 4 presents a fictitious scenario of health clinic and application of proposed ontology to the given scenario. Section 5 presents a discussion on the findings of this study. The paper ends with conclusion and future work in section 6.

2. Related Work

There are many approaches that have been established to explain and develop ontology for a variety of concept development, knowledge sharing activities (Gruber, 1993), (Neches et al., 1991), (Genesereth, 1997), (Gruber et al., 1992), (Patil et al., 1992). There are several literature available to explain the principles, methodology and applications of ontology (Corcho et al., 2003), (Uschold, 1996), (Uschold and Gruninger, 1996), guideline to create ontology (Noy and mcguinness, 2001), (Booch et al., 2005), to evaluate an ontology (Gómez-Pérez, 1996), (Gómez-Pérez, 2001),

(Guarino and Welty, 2000), (Kalfoglou and Robertson, 1999). (Pereira and Santos, 2009) presented a conceptual implementation model of an ontology defined in the security domain. They used the methodology presented by (Noy and mcguinness, 2001) to develop the ontology. The ontology comprises a set of concepts and their relations based on the standards ISO/IEC_JTC1. The ontology was formalized with Web Ontology Language (OWL) for modeling ontology. Everett mentioned in her article (Everett, 2011) that risk management task is still not a well-understood and widely employed discipline today. Very few organizations have senior managers who either are trained in or have been made accountable for risk management. The author also pointed out towards the absence of any common framework that forces different parts of the business employ their own jargon to describe various terminology related to risk and assess risk in a subjective manner. Author introduced the concern to establish a formal, structured way of collecting data, recording it and reporting on the findings to management team for ISO27005 standard (27005, 2011). Authors in (Moreira et al., 2008) discussed the difficulties involved in dealing with quantity, diversity and the lack of semantics security information. They proposed a general methodology to create security ontology and illustrated the case with design and validation of system vulnerabilities and security incidents. The authors have described ontology examples for three management levels i.e. strategic, tactical and operational.

3. Proposed Ontology

In our proposed ontology, there are 11 main concepts and 15 relationships. Figure 2 presents the ontology to capture core concepts of ISO27005 standard and relationship among them. The rationale behind the ontology is structured as follows: Organization *has* Objective and *owns* some Assets. An Asset *hasSecurityProperty* named as CIA (Confidentiality, Integrity and availability). An Asset *has* some Vulnerability that *leadsTo* risk in the system, while a control *mitigates* the vulnerability. A risk *contains* consequence that *affects* Objective of Organization. A potential risk *harms* the organization. Event *has* a likelihood of occurrence and it *modifies* consequence. Risk *isRealizedBy* Event in the system. A threat *affects* an asset as it *exploits* the Vulnerability of the Asset and *causes* an event (An event is also known as security incident) in the system.

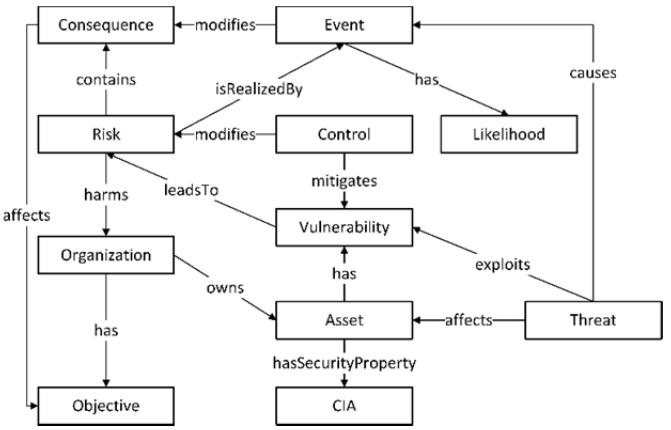

Figure 2: The proposed ontology for ISO27005 standard

3.1. Ontology Development

Our proposed methodology is drawn from (Noy and mcguinness, 2001). This is a high level and simplified methodology. It proposes ontology development through seven essential steps. The detailed description of each step of development is as follows:

Step 1. Determine the domain and scope of the ontology: This work proposes an ontology for ISO27005 risk management standard, which will represent the terms and relations related to the Information security risk management domain. The domain of the proposed ontology is marked as a Grey box in Figure. This ontology will be used for sharing common understanding of concepts associated to the risk assessment phase of ISO27005. The proposed ontology can be used to obtain information and provide common, unambiguous semantic models of risk management domain concepts. The ontology will serve as a reference point for communication between different stakeholders (decision-maker, experts, and users). An employee/user can identify a particular instance based on the ontology. For instance, an instance of Brute-force attack on the password can be quickly identified as a **Threat**. The proposed ontology can also be useful for the system administrators and automated tool to compute risk. The ontology will include the information on various threat and vulnerability types, list of assets, classification of control that matter for choosing an appropriate risk.

***Step 2. Use of existing ontologies*:** There is no existing ontology for ISO27005 standard. However, there are several ontologies based on the concept of Information security, risk management (Pereira and Santos, 2012), (Moreira et al., 2008), (den Braber et al., 2007), (Arbanas and Čubrilo, 2015), (Herzog et al., 2007) These ontologies served as a good starting point for our ontology. We have implemented our ontology in OWL (Web Ontology Language), a markup language based on RDF/XML (Resource Description Framework/Extensible Markup Language) and used the Protégé OWL tool to create it. This web language has been developed by

the Web Ontology Group as a part of the W3C Semantic Web Activity (Smith et al., 2004), (Powers, 2003). Our ontology uses a commonly accepted notation to describe the concept. Therefore, it supports querying and acquisition of new knowledge using OWL reasoners and OWL query languages.

Step 3. List the relevant terms of the domain: In this step, we captured terms that are important in describing the concept of ISO27005. It is a tedious task to go through the whole document (ISO27005 standard in this case) manually to capture all the relevant words. We may also fail to notice an important word if we scan the document manually. Therefore, we used an automated process to generate a list of all the relevant terms for ISO27005 standard. We used java API, MaxentTagger (*Class MaxentTagger*, n.d.) to run, train, and test the part of speech (POS) tagger. We supplied the standard document of ISO27005 to the automated Process to extract all the distinct word from it. We tagged each word to its POS using English tagger *english-bidirectional-distsim.tagger*. Later, we prepared a list of all nouns and verbs to select the relevant class entity, and relationship entity respectively. Some of the words contained in the list of noun includes - Risk, Asset, Event, Security incident, Threat, impact, likelihood, probability, consequence, control, mechanism, confidentiality, integrity, availability, objective, motive, media, organization, stakeholder, person, owner, industry, etc. Similarly, the words contained in the list of verb includes - mitigate, modify, cause, exploit, lead, affect, arise, become, begin, capture, allow, etc.

Step 4. Define the classes and the class hierarchy: In this step, we defined each class/entity through a definition. The definition of classes of ontology are taken from ISO27005 (27005, 2011) and ISO/IEC 27000:2014 (27000, 2014).

- *Organization*: This class represents a single person or a group that achieves its objectives by using its own functions, responsibilities, authorities, and relationships to achieve its objectives
- *Objective*: This class represents the result to be achieved by an organization
- *Asset*: This class represents any resource that has value and importance to the owner
- *Threat*: This class represents a potential cause of an unwanted incident, which may result in harm to a system or organization
- *CIA*: This class represents the security properties i.e. confidentiality (C), integrity (I) and availability (A) to be ensured
- *Risk*: This class represents an effect of uncertainty on objectives
- *Consequence*: This class represents an outcome of event affecting the security properties of asset
- *Likelihood*: This class represents a chance of an event to occur
- *Event*: This class represents an occurrence or change of a particular set of circumstances
- *Control*: This class represents a measure that is modifying risk
- *Vulnerability*: This class represents any weakness of an asset that can be exploited by one or more threats

All the above-mentioned classes are implemented using OWL language. The OWL representation of the Threat class implies that Threat affects some Asset, causes Event and exploits Vulnerability. We can infer the same information from the ontology diagram in Figure, but OWL representation gives it a formal structure and makes it as machine-readable.

Step 5. Define the object properties of the class: In this step, we identified object properties of all the classes selected in step 4. The property expresses a general fact about a class. Object Property relates a class to another class. The following OWL sample presents the relation between Threat and Vulnerability. The object property 'exploits' on range 'Threat' and domain 'Vulnerability' explains that threat class and vulnerability class are related to each other through the relation 'exploits'.

```
<owl:ObjectProperty rdf:about="#exploits">
        <rdfs:range rdf:resource="#Threat"/>
        <rdfs:domain rdf:resource="#Vulnerability"/>
</owl:ObjectProperty>
```

Step 6. Define the datatype properties: In this step, we identified data property of all the classes selected in step 4. Data Property relates a class to a literal. The data property 'value' on 'Asset' defines that every asset has some value measured in integer.

Step 7. Create instances: In this step, we created instances of the classes. We created both generic and specific instance (based on the case scenario, given in next section). The individuals in the class extension are called the instances of the class. NamedIndividual represents instances in OWL representation.

4. A case scenario of a health clinic

This section presents a fictitious case scenario of a health clinic. The health clinic is responsible for providing healthcare services to the citizen. They host general practitioners (GP) in their clinic. The organizational structure of the health is composed of a CEO, an HR manager and an IT expert. There are 22 staff consists of 18 doctors (9 male, 9 females), 2 ladies at reception, 2 nurses work in the clinic. The task of these receptionists is to provide information related to doctors, (e.g. appointment date, details). They are also responsible to register a new patient in the health system. The clinic uses the IT services in the form of Email server, file server, patient records, billing database, medical records. The printers are used to print out document related to patient's treatment. It is possible to book an appointment through website and SMS. The IT strategy and information security policy is outdated. The last modification took place in 2010. An attacker can try to gain access to the healthcare system to steal personal information of a patient (patient record). Receptionist uses preferably simple password to log into the system.

4.1. Application of Ontology

In this section, we apply our proposed ontology to the case scenario of health clinic. Table 1 presents the overview of all the classes of ontology and instances of each class based on the case scenario. The objective of this task is to show the potential data that can be used to populate the classes of the ontology based on the domain of application.

Class	Instances based on case study
Organization	the health clinic
Objective	Annual revenue of USD 10 million, provide 24x7-treatment facility to the patients.
Asset	Patient database, treatment process, doctors, medical equipment
Threat	Brute Force, DDOS, data corruption, failure of medical equipment
CIA	Confidentiality of patient's records, integrity of billing data and availability of treatment process
Risk	database corruption, denial of service
Consequence	loss of patient's data, lawsuit against organization
Likelihood	qualitative : very low, low, medium, high, very high; quantitative: range in
Event	Denial of service attack, theft of electronic medical data
Control	updated security policy, strong encryption and hash algorithm
Vulnerability	outdated security policy, simple password used by receptionist

Table 1: A list of classes and instance based on the case scenario of health clinic

Table 2 presents the list of relationships in the ontology, classes associated with the relations and instances based on the case scenario. This table provides a detailed information about different scenario that can occur in the setting of a health clinic, and how to categorize these incidents under proper category using the concepts from ontology. Tables 1 and 2 help to understand the application of the proposed ontology towards a given scenario.

Relation	Class involved	Instances based on case study
has	Organization, Objectives	The health clinic has an objective to maintain annual profit of USD 1 million, provide quality treatment, maintain productive and positive employee environment
owns	Organization, Asset	The health clinic owns asset in the form of 1) Personnel: doctors, nurses, receptionist, 2) business process: treatment process, billing process, 3) Hardware: medical equipment, computers, servers, 4) information: patients record, medical record
hasSecurity Property	Asset, CIA	Medical record must remain confidential, remain unchanged by any illegitimate action and remain available whenever it is required by the concerned entity
affects	Threat, Asset	Equipment failure affects medical equipment, corruption of data affects medical records, and password brute force attack affects the registration process.
has	Asset, Vulnerability	Personnel has lack of security awareness, information has outdated security policy hardware has insufficient maintenance
exploits	Threat, Vulnerability	failure of medical equipment exploits insufficient maintenance, brute force attack exploits simple password policy
mitigates	Control, Vulnerability	incident response mitigates equipment failure, privacy law, security policy mitigates simple password, outdated policy

modifies	Control, Risk	user authentication, firewalls modifies unauthorized data access, security policy modifies denial of service
causes	Threat, Event	malware causes denial of service, incorrect prescription generation/distribution
modifies	Event, Consequence	unauthorized access modifies the risk of data breach, abuse of personal rights modifies the chance of happening an identity theft
isRealizedBy	Risk, Event	unavailability of a medical equipment is realized by theft of hardware, database corruption is realized by data breach
harms	Risk, Organization	denial of service harms the medical service of health clinic, database corruption harms the medical service of health clinic
affects	consequence, Objective	loss of patient's data affects the financial objective and core values as it may face fine or lawsuit
has	Event, Likelihood	Denial of service has the low likelihood, theft of electronic medical data has very low likelihood
leadsTo	Vulnerability, Risk	Outdated security policy leads to database corruption, data breach, insufficient maintenance/faulty installation of devices leads to denial of service.

Table 2: A list of relationships, their associated classes, and instances based on the case scenario of health clinic

5. Discussion

In this section, we analyze and discuss the findings from the section 3 & section 4 to obtain an understanding of the importance of the proposed ontology. An ontology is proposed using a seven-step guideline to address the challenges associated with establishing a common understanding of the core concepts of risk assessment phase of ISO27005. Figure 2 gives an overview of the core concepts and their relationship. The ontology is further applied to a case scenario of a health clinic to extract the useful information relevant for an ISRM task. Table 1 presents the possible instances/values of the ontology classes in the domain of the given health clinic case scenario. Table 2 gives a detailed information on the relationship of the classes of the ontology. A person, who is engaged in the task of ISRM in any organization, can use the proposed ontology to quickly identify a number of threats, assets, vulnerability, event, consequence, etc. The presence of detailed information on the relation between classes can enable answering the various questions related to ISRM task. In the context of proposed scenario of health clinic, the ontology will help answering the following types of competent questions, such as a) Is outdated security policy a threat or vulnerability? b) What is the potential consequence of having an unauthorized access to data? c) What are the assets owned by an organization? d) Is user authentication control sufficient to combat unauthorized data access?

6. Conclusion and Future work

Ontology provide an effective mechanism to understand, describe, communicate and exploit knowledge in a given domain. This paper presents the necessity of having an ontology for ISO27005 standard. Later, it proposes an ontology to cover the core concepts. The development of ontology is conducted using the seven steps guideline. The details provided in the ontology development will be helpful for the readers to further enhance the proposed ontology as well as develop a similar ontology in other

domain. Our ontology is developed using OWL standard in Protégé tool. Hence, it enables the possibility to be used by an automated tool to provide advanced services such as more accurate risk assessment and knowledge management. The core concept of the ontology is based on asset, threat, vulnerability, control, risk, etc. All the concepts and relations are instantiated with the help of a case scenario of health clinic to provide domain knowledge and vocabulary. Our future work includes: a) A revised version of the proposed ontology i.e. to include concepts from other phases of ISO27005, b) Use the ontology to compare different Information security risk management standard. There are many well-established risk management approaches e.g. CORAS, ISRAM, ISO31000 are available. We can evaluate the role of ontology to compare ISO27005 to other standards. c) Development of the necessary application to query information from the ontology. We are in a discussion to use SPARQL protocol (Harris and Seaborne, 2013), which is an RDF query language, to use as a query language for our ontology. SPARQL is also available as a plug-in for protégé ontology tool. d) The knowledge obtained from this ontology will be helpful for the risk practitioners (professional experts, students, researchers). The next step will be to distribute this ontology to these practitioners and encourage them to use it in their practical task. We can gather their experience using this ontology. We can collect information related to simplicity, usefulness of this ontology. e) We would like to explore the possibility of using the ontology in the development of tool based on ISO27005 concepts. The objective is to eliminate the manual intervention as much as possible in the risk management task.

7. Acknowledgments

The author recognizes the contribution and comment made by Prof. Einar Arthur Snekkenes. The author is also thankful to Gaute Wangen for fruitful discussion on the concepts of ISO27005, and structure of ontology; Roberto Rigolin Ferreira Lopes for providing assistance on latex; Vasileios Gkioulos for his input on ontology and Protege tool. The author acknowledges the sponsorship from COINS research school for information security.

8. References

27000, I. (2014), Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary, ISO No. ISO/IEC 27000:2014, BSI.

27005, I. (2011), ISO/IEC 27005 Information Technology – Security Techniques – Information Security Risk Management, ISO, ISO copyright office Case postale 56 • CH-1211 Geneva 20, p. 68.

Arbanas, K. and Čubrilo, M. (2015), Ontology in Information Security, Faculty of Organization and Informatics University of Zagreb.

Booch, G., Rumbaugh, J. and Jacobson, I. (2005), Unified Modeling Language User Guide, The (2Nd Edition) (Addison-Wesley Object Technology Series), Addison-Wesley Professional.

den Braber, F., Hogganvik, I., Lund, M.S., Stølen, K. and Vraalsen, F. (2007), "Model-based security analysis in seven steps – a guided tour to the CORAS method", BT Technology Journal, Vol. 25 No. 1, pp. 101–117.

Class MaxentTagger. (n.d.). , available at: http://www-nlp.stanford.edu/nlp/javadoc/javanlp/edu/stanford/nlp/tagger/maxent/MaxentTagger.html.

Corcho, O., Fernández-López, M. and Gómez-Pérez, A. (2003), "Methodologies, tools and languages for building ontologies. Where is their meeting point?", Data & Knowledge Engineering, Vol. 46 No. 1, pp. 41–64.

Ehrig, M. (2006), Ontology Alignment: Bridging the Semantic Gap, Springer US, available at: https://books.google.no/books?id=nxzBZonEF50C.

Everett, C. (2011), "A risky business: {ISO} 31000 and 27005 unwrapped", Computer Fraud & Security, Vol. 2011 No. 2, pp. 5–7.

Genesereth, M.R. (1997), "Software Agents", in Bradshaw, J.M. (Ed.), , MIT Press, Cambridge, MA, USA, pp. 317–345.

Gómez-Pérez, A. (1996), "Towards a framework to verify knowledge sharing technology", Expert Systems with Applications, Vol. 11 No. 4, pp. 519–529.

Gómez-Pérez, A. (2001), "Evaluation of ontologies", International Journal of Intelligent Systems, Vol. 16 No. 3, pp. 391–409.

Gruber, T.R. (1993), "A Translation Approach to Portable Ontology Specifications", Knowl. Acquis., Vol. 5 No. 2, pp. 199–220.

Gruber, T.R., Tenenbaum, J.M. and Weber, J.C. (1992), "Artificial Intelligence in Design '92", in Gero, J.S. and Sudweeks, F. (Eds.), , Springer Netherlands, Dordrecht, pp. 413–432.

Guarino, N. and Welty, C. (2000), "Ontological analysis of taxonomic relationships", Conceptual Modeling – ER 2000, Springer, pp. 210–224.

Harris, S. and Seaborne, A. (2013), SPARQL 1.1 Query Language, available at: https://www.w3.org/TR/sparql11-query/.

Herzog, A., Shahmehri, N. and Duma, C. (2007), "An ontology of information security", International Journal of Information Security and Privacy (IJISP), Vol. 1 No. 4, pp. 1–23.

Kalfoglou, Y. and Robertson, D. (1999), "Knowledge Acquisition, Modeling and Management: 11th European Workshop, EKAW'99 Dagstuhl Castle, Germany, May 26–29, 1999 Proceedings", in Fensel, D. and Studer, R. (Eds.), , Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 207–224.

Moreira, E. dos S., Martimiano, L.A.F., Brandã, A.J. dos S. and Bernardes, M.C. (2008), "Ontologies for information security management and governance", Information Management & Computer Security, Vol. 16 No. 2, pp. 150–165.

Neches, R., Fikes, R.E., Finin, T., Gruber, T., Patil, R., Senator, T. and Swartout, W.R. (1991), "Enabling technology for knowledge sharing", AI Magazine, Vol. 12 No. 3, p. 36.

Nguyen, V., Science, D. and (Australia), T.O. (2011), Ontologies and Information Systems [Electronic Resource] : A Literature Survey / Van Nguyen, Defence Science and Technology Organisation Edinburgh, S. Aust, available at: http://nla.gov.au/nla.arc-24764.

Noy, N.F. and mcguinness, D.L. (2001), Ontology Development 101: A Guide to Creating Your First Ontology, available at: http://www.ksl.stanford.edu/people/dlm/papers/ontology101/ontology101-noy-mcguinness.html.

Patil, R.S., Fikes, R., Patel-Schneider, P.F., McKay, D.P., Finin, T.W., Gruber, T.R. and Neches, R. (1992), "The DARPA Knowledge Sharing Effort: A Progress Report.", KR, Vol. 92, pp. 777–788.

Pereira, T. and Santos, H. (2009), "Metadata and Semantic Research: Third International Conference, MTSR 2009, Milan, Italy, October 1-2, 2009. Proceedings", in Sartori, F., Sicilia, M.Á. and Manouselis, N. (Eds.), , Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 183–192.

Pereira, T.S.M. and Santos, H.M.D. (2012), "An Ontology Approach in Designing Security Information Systems to Support Organizational Security Risk Knowledge", KEOD 2012 - Proceedings of the International Conference on Knowledge Engineering and Ontology Development, Barcelona, Spain, 4 - 7 October, 2012., pp. 461–466.

Powers, S. (2003), Practical RDF, O'Reilly & Associates, Inc., Sebastopol, CA, USA.

Singhal, A. and Wijesekera, D. (2010), "Ontologies for modeling enterprise level security metrics", Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, ACM, p. 58.

Smith, M.K., Welty, C. and McGuinness, D.L. (2004), OWL Web Ontology Language Guide.

Uschold, M. (1996), "Building ontologies: towards a unified methodology", Expert Systems '96, Cambridge, UK, available at: http://www.cs.toronto.edu/ nernst/papers/uschold96building.pdf.

Uschold, M. and Gruninger, M. (1996), "Ontologies: principles, methods and applications.", Knowledge Eng. Review, Vol. 11 No. 2, pp. 93–136.