Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard

Stefan Fenz, Gernot Goluch,
Andreas Ekelhart, Bernhard Riedl
Secure Business Austria
Favoritenstrasse 16
1040 Vienna, Austria
{sfenz, ggoluch, aekelhart, briedl}@securityresearch.at

Edgar Weippl
Vienna University of Technology
Favoritenstrasse 9-11
1040 Vienna, Austria
weippl@ifs.tuwien.ac.at

Abstract

This paper introduces an ontology-based framework to improve the preparation of ISO/IEC 27001 audits, and to strengthen the security state of the company respectively. Building on extensive previous work on security ontologies, we elaborate on how ISO/IEC 27001 artifacts can be integrated into this ontology. A basic introduction to security ontologies is given first. Specific examples show how certain ISO/IEC 27001 requirements are to be integrated into the ontology; moreover, our rule-based engine is used to query the knowledge base to check whether specific security requirements are fulfilled. The aim of this paper is to explain how security ontologies can be used for a tool to support the ISO/IEC 27001 certification, providing pivotal information for the preparation of audits and the creation and maintenance of security guidelines and policies.

1. Introduction

Nowadays companies increasingly rely on IT, which makes IT security a very important field for guaranteeing business continuity. Driven by laws such as Basel II [1] and the Sarbanes Oxley Act [13], IT security is no longer considered as a costly responsibility that generates no additional business benefits for the organization; management is compelled to pay more attention to securing an appropriate and certified IT security approach. Additionally, the majority of companies currently depend on collaboration with other firms (suppliers, subcontractors, etc.). Accordingly, certification of one's IT security approach assures collaborating companies a certain level of reliability and trust.

Corporations certify their ISMS (Information Security Management System) [12] following international standards in order to increase their equity. However, certification costs time and money, leading to a situation in which it is mostly large corporations that perform certification. Small and medium sized enterprises, in particular, can rarely bear the costs of a full certification procedure. Of the large enterprises in the U.K., 28 percent carried out such certification initiatives, in terms of BS7799 [2], ISO/IEC 17799 [9] and ISO/IEC 27001 [10], while the average for all companies is only 7 percent [12].

Thus, we propose an ontological mapping of the ISO/IEC 27001 standard to increase the degree of automation within the certification process, lowering the financial costs and time required for the certification procedure. In combination with our *Security Ontology* approach [4], we aim at an automatic partial audit preparation by extracting IT infrastructure knowledge from an established *Security Ontology*. Besides the automation, the ontological mapping of the ISO/IEC 27001 standard provides a foundation for an electronic tool, supporting the actual certification process by providing a central platform for all participating actors. Furthermore, we introduce the generic *OntoWorks* framework to access, visualize, and reason on ontological databases and provide an overview on its usage for the *ISO/IEC 27001 Ontology* and the *Security Ontology* (the corresponding ontology files are available at securityontology.securityresearch.at).

2. Previous Work

Recent projects related to the Common Criteria (CC) for Information Technology Security Evaluation carried out with our partner companies revealed the need for an automation of the certification process.

In a nutshell, the Common Criteria for Information Technology Security Evaluation provides comprehensive guidelines for the evaluation and certification of IT security regarding data security and data privacy. Our experiences re-

vealed that due to the very complex and time consuming certification process, a lot of companies abstain from a CC certification.

To conquer the expensive Common Criteria evaluation process for a specific CC evaluation assurance level, we presented in [3] a CC ontology, comprising the entire CC domain with special focus on security assurance requirements relevant for the evaluation.

Unlike the already available PDF or paper version of the CC standard, the ontology can be browsed easily with any standard RDF [16] or OWL [14] visualization tool. Second, our approach offers the possibility to query the data structure in an efficient way using SPARQL [17].

Our third contribution was the CC certification support tool; this tool takes the CC ontology as input and supports the evaluation process in several novel ways, such as tagging and linking relevant documents.

Several CC certifications revealed that certain components and the corresponding documents often contain similar keywords and concepts, hence we introduced the aforementioned *Tagging* approach in our *CC Ontology*, which supports the evaluator in the document review by reusing information, produced in earlier CC evaluation certification processes.

In the current paper we will extend our previous efforts with an ontological mapping of the ISO/IEC 27001 standard. Compared to [3], we raise the integration of the *Security Ontology* [4], [5] to enhance the evaluation efficiency and introduce the generic *OntoWorks* framework to access, visualize, and reason on ontological databases.

3. The ISO/IEC 2700x Standard Series

There are several certification initiatives, that attest to the viability of a corporation's ambitions within an addressed domain, which specialize in specific business aspects. However, the overall goal of such initiatives is to acknowledge the corresponding company's structured, methodical, and transparent performance.

Building on the British standard BS7799 [2] and the ISO/IEC 17799 [9], the ISO/IEC 27001 [10] standard provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS [10]. This standard is the first in the information security related ISO/IEC standards family. Awaited are a series of evolving and subsequent standards, e.g., ISO/IEC 27003, an ISMS implementation guide; ISO/IEC 27004, a standard for information security measurement and metrics; ISO/IEC 27005, a standard for risk management; and ISO/IEC 27006, a guide to the certification process.

The ISO/IEC 2700x process approach for information security management highlights the importance of: (1) understanding a company's information security requirements

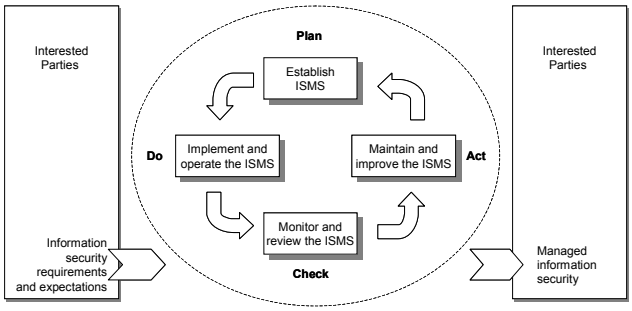

Figure 1. PDCA model applied to ISMS processes [10]

and the need for information security policies and objectives, (2) implementing and operating controls to manage a company's information security risks in the context of the corresponding overall business risks, (3) monitoring and reviewing the effectiveness and performance of the ISMS, and (4) continuous improvement based on objective measurement. This international standard adopts the model for structuring all ISMS processes.

Figure 1 illustrates the "Plan-Do-Check-Act" (PDCA) model and outlines how an ISMS uses the information security requirements and expectations of the stakeholders as input to produce accurate, functioning, and effective information security results.

4. The ISO/IEC 27001 Ontology

Due to the very flat structure of the ISO/IEC 27001 standard, we were able to map the entire standard to the ontology using only three classes. Figure 2 shows a typical ISO/IEC 27001 control objective and the corresponding controls.

A.9 Physical and environmental security

A.9.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.

A.9.1.1	Physical security perimeter	*Control* Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.
A.9.1.2	Physical entry controls	*Control* Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Figure 2. ISO/IEC 27001 A.9 control objectives and control subset

Figure 3 illustrates the ontological mapping of the *A.9* control objectives and controls shown in Figure 2 (to enhance the readability only a subset of the *A.9* controls is

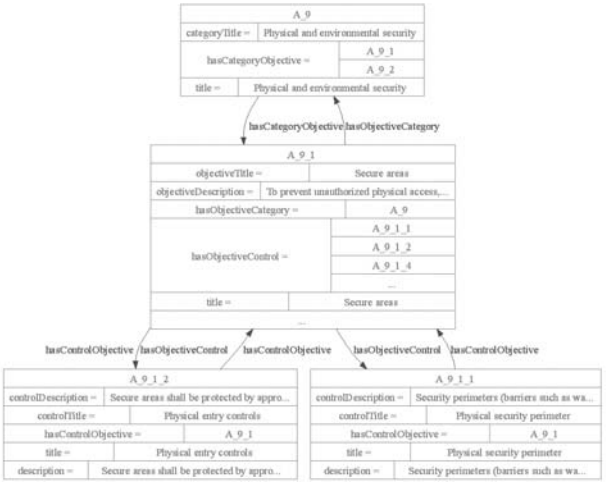

Figure 3. ISO/IEC 27001 A.9 category, A.9.1 instance and A.9.1 controls subset

illustrated in figures 2 and 3). Starting from category *A.9 - Physical and environmental security*, we connected the corresponding control objective *A.9.1 - Physical security perimeter* through the relation *hasCategoryObjective* and its inverse relation. The actual controls of a certain control objective are connected by *hasObjectiveControl*. Beside aforementioned relations, each element within the ontology is equipped with various attributes such as *title* and *description* to ensure that the entire standard and not only the structure is stored within the ontology.

The following itemization lists the advantages of using an ontology rather than a simple spreadsheet or database solution:

1. Standardized data structure gained by using OWL [14]
2. Possibility to use reasoners to generate new knowledge based on existing facts
3. OWL-based ontologies can be reused by other ontologies through merging or importing the relevant parts

Furthermore, the fact that it is possible to merge entire ontologies or just parts of them helped us in combining the *ISO/IEC 27001 Ontology* and our *Security Ontology* approach [4] (further information on the combination is presented in Section 6).

5. The Security Ontology

In addition to the organizational IT security aspects that are covered by ISO/IEC 27001, we must also consider the physical aspects of IT security, relevant to the company's physical environment. Servers that host company information and customer data or databases with private user-information must be secured in order to ensure reliable and secure IT services. Small and medium-sized enterprises, in particular, often oversee the need for a holistic IT security approach. Therefore, we developed the *Security Ontology* [4] to provide a proper knowledge base of threats and corresponding countermeasures. In [5] we extended the threat simulation approach with risk analysis methods in order to improve quantitative risk analysis. The current section summarizes the research results and proposes a combination of the *Security Ontology* and the *ISO/IEC 27001 Ontology* to enhance the overall IT security level.

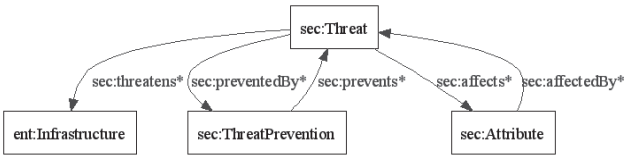

Figure 4. Sub-ontology: Threat

The most important parts of the *Security Ontology* are represented by the sub-ontologies *Threat*, *ThreatPrevention* and *Infrastructure*:

Figure 4 shows the *Threat* ontology with its corresponding relations: (1) to model the threats that endanger certain infrastructure elements we introduced the *sec:threatens* relation (every threat threatens *n* infrastructure elements) (2) of course we want to mitigate the threats, so we created the *sec:preventedBy* and *sec:prevents* relations (3) to enable companies to optimize their IT security approach to certain IT security attributes such as confidentiality or availability, we assigned affected attributes to each threat by the *sec:affects* and its inverse relation.

The building, with its corresponding floors and rooms, can be described using the infrastructure framework of the *Security Ontology*. To precisely map the entire building plan on the *Security Ontology*, each room is described by its position within the building. The ontology "knows" in which building and on which floor a particular room is located. The attributes *ent:nextToRoomHorizontal* and *ent:nextToRoomVertical* describe the exact location of each room; and furthermore each instance of *ent:ITAndTelecommunication* and *sec:TechnicalThreatPrevention* is located in a particular room. A room can, of course, also contain more concepts. The current ontology uses a flexible and easily extendable structure: additional concepts can be included without effort. The concept *ent:TechnicalThreatPrevention* is subdivided into *ent:CounterMeasure* and *ent:Detector*, which are used to model detectors (fire, smoke, noise, etc.) and their corresponding countermeasures (fire extinguisher, alarm system, etc.).

Table 1. Exemplary Organizational Controls in the Security Ontology

Class	sec:HumanResourcesSecurityControl
sec:Description	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their own and the organizations responsibilities regarding information security.
sec:controlDate	2007-02-02
sec:isImplemented	true
sec:controlCorrespondsTo	iso:A_8_1_3
sec:prevents	sec:SocialEngineering

Along with the mapping of technical infrastructure elements, crucial for acceptance of the *Security Ontology*, is the mapping the organizational aspects regarding policies, standards, and procedures. Therefore, based on the ISO/IEC 27001 standard, we implemented controls which are classified as administrative threat prevention elements.

Each element is associated with the following attributes: (1) *sec:description* describes the control in a human readable way (2) *sec:controlDate* stores the date on which the control was checked, to ensure that mechanisms such as an obligatory review of the controls can be implemented by the processing applications (3) *sec:isImplemented* indicates the implementation status of a certain control within the organization (4) *sec:prevents* holds a list of threats that can be prevented by the implementation of the current control (5) *sec:controlCorrespondsTo* allows us to map concrete controls of existing security frameworks to control-instances of the *Security Ontology*.

This feature is very useful for supporting a concrete certification process, such as the ISO/IEC 27001 certification, where the processing application is able to determine if a certain ISO/IEC control is fulfilled by checking the current state of the *Security Ontology*. To avoid that an organizational control is being misleadingly marked as implemented, the *sec:controlDate* attribute ensures that the control is only valid for a defined period of time. The example in Table 1 shows a concrete control implementation.

6. Combining the ISO/IEC 27001 Ontology with the Security Ontology

We now want to utilize the *ISO/IEC 27001 Ontology* by combining it with the *Security Ontology*, which acts as a knowledge base representing a company's infrastructural and organizational facts.

In our current research, we split the ISO/IEC 27001 controls into two groups:

1. *Hard Facts*: physical security aspects of the ISO/IEC 27001 standard

2. *Soft Facts*: organizational security aspects of the ISO/IEC 27001 standard

The reason for this split is the different characterization of the control's counterparts in the *Security Ontology*.

Table 2 shows an example of a hard fact and a soft fact "ISO/IEC 27001 control - *Security Ontology* item" mapping. The security door is part of the infrastructure sub-ontology, whereas the HR (Human Resources) policy and guideline are part of the administrative threat prevention sub-ontology. Every ISO/IEC 27001 control is certainly not representable by only one hard or soft fact of the *Security Ontology*. In fact, most controls consist of or are mapped to various hard and soft fact items.

To enhance understanding, we look at an example mapping of one hard fact and one soft fact, in the following sub-sections.

6.1. Mapping the "Hard Facts"

One of our major industry partners participating in the research center *Secure Business Austria* uses the *Security Ontology* to represent its IT infrastructure and the corresponding threats. In this section, we deal with the problem of secure areas in the company's data processing center and the corresponding security perimeters and access controls. The applicable ISO/IEC 27001 controls are: *A.9.1.1 - Physical security perimeter* and *A.9.1.2 - Physical entry controls* (see Figure 2 and Figure 3 for ontological representation). In the following, we concentrate on infrastructure and access control elements.

In our first example, we want to determine whether the *A.9.1.1* control, stating that "Security perimeters shall be used to protect areas that contain information and information processing facilities", is fulfilled. Therefore, we query the *Security Ontology* in the following way:

First, we determine which rooms are defined as secure areas. In the *Security Ontology*, each instance of class *Room* offers to mark secure areas within the data processing center by the boolean attribute *sec:secureArea*. Automatic marking is enabled by rule sets that define circumstances under which a room is to be marked as a secure area (e.g., business critical servers are located in the room or the room is used as a data archive). The following SPARQL [17] query generates a list of all secure areas within the main data processing building:

```
SELECT ?room
WHERE  {?room ent:secureArea true}

SPARQL result: R0104, R0201, R0202
```

Table 2. Hard and soft fact mapping

Mapping Type	ISO/IEC 27001 Control	Security Ontology Item
Hard Fact	Physical security perimeter	Security doors with biometric access control
Soft Fact	Screening (Human Resources - Prior to employment)	HR policy and guideline

Using the SPARQL query, as presented below, we gather a list of all safety doors that are installed in the secure areas of the data processing center.

```
SELECT ?room
WHERE {?room ent:secureArea true.
 ?x rdfs:subClassOf sec:SafetyDoor.
 ?insSafetyDoor a ?x.
 ?insSafetyDoor ent:locatedIn ?room.}

SPARQL result: R0104
```

The output shows us that only room *R0104* has implemented safety doors. The engine concludes that the rooms R0201 and R0202 lack adequate safety doors. It sends a corresponding message to the user interface to inform the human auditor of this situation in the following way:

- R0201 is not in compliance with ISO/IEC 27001 Control A.9.1.1: no safety door found
- R0202 is not in compliance with ISO/IEC 27001 Control A.9.1.1: no safety door found

Section 7 refers in more detail to the technical implementation of the engine and the user interface. In addition to the check for security doors, we have implemented several other checks such as secure window checks, wall type checks and doorman checks to cover large parts of the security perimeter domain.

If every secure area within the data processing center is secured with the defined security perimeters, the certification requirement pertaining to the control *A.9.1.1*, is fulfilled and a report will be generated to enable human auditors to understand the decision process of this specific ISO/IEC 27001 certification check.

In our second example we want to determine if the *A.9.1.2* control, stating that "Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access", is fulfilled. Therefore, we query the *Security Ontology* in the following way:

We know that room *R0104*, *R0201*, and *R0202* are defined as secure areas (see first SPARQL query) and that appropriate entry controls should ensure that only authorized personnel is allowed access. Therefore, we query those rooms that have already implemented such entry controls:

```
SELECT ?room ?accessControl
WHERE {
 ?x rdfs:subClassOf sec:AccessSystem.
 ?y rdfs:subClassOf ?x.
 ?accessControl a ?y.
 ?room ent:secureArea true.
 ?accessControl ent:locatedIn ?room.}

SPARQL result: R0202, Fingerprint0202
```

The output shows that only room *R0202* has implemented an access system. The remaining rooms *R0104* and *R0201* thus lack a proper access control system. Now the person who is running an ISO/IEC 27001 certification preparation, is aware that something must be done to meet the requirements of the *A.9.1.2* control. Therefore, suggestions derived from the *Security Ontology* are available, presenting possible access control system types, such as facial scans or smart card access systems. When every secure area within the data processing center is connected to an access control system, the certification requirement for the *A.9.1.2* control is fulfilled and a report will list the ontological decision steps to the human auditor.

6.2. Mapping the "Soft Facts"

In addition to "Hard Facts" such as infrastructure components, it is crucial for the acceptance of our certification approach to include the organizational aspects of the company environment. Existing policies, standards, guidelines, and procedures have to be mapped to the *Security Ontology* to ensure an efficient certification process. Due to the fact that the majority of policies, standards, guidelines, and procedures are not readable by machines, we had to develop some kind of mapping mechanism to ensure that the *Security Ontology* "understands" what is meant by a certain administrative statement. Therefore, we connected each certification control with those administrative statements that, if implemented, would fulfill the certification control. In order to clarify this idea, the following statement shows the connection of the *A.8.1.1* control and the corresponding company-internal, administrative control *HRSC1* (compare the following SPARQL query). The *A.8.1.1* control, regarding the aspect of roles and responsibilities in the human resources sector, states that "Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organizations information security policy." [10].

```
SELECT ?control ?bool ?date
WHERE {
 ?control sec:controlCorrespondsTo
```

```
   secont:A_8_1_1.
 ?control sec:isImplemented ?bool.
 ?control sec:controlDate ?date.}

SPARQL result: HRSC1, true, 2007-02-08
```

The query checks for the company-specific, administrative control that corresponds to the *A.8.1.1* control and determines the implementation status and the last control date. Although the initial effort for the manual compliance check of the company-internal paper-based administrative controls against the *Security Ontology* is high, savings in terms of time and money increase with every certification process through the central and machine readable storage of policy-, standard-, guideline- and procedure-modules.

7. OntoWorks

As we have seen in the previous sections, compliance with ISO/IEC 27001 controls is determined by reasoning, based on the established knowledge, hence we identify two pivotal elements: a knowledge base and corresponding rules. Due to the valuable semantic structure, we decided on an OWL-based knowledge store, realized by one OWL document instance. Furthermore, results must be presented to a user who runs the compliance software and is eager to uncover potential vulnerabilities. Summarizing our main requirements for such an ontological framework results in the following list:

- **Rule based**: We emphasize the development of rule based systems, especially in domains where the underlying logic changes often. The rule language used must be highly expressive due to the complexity of the compliance statements
- **Flexibility**: The framework should be useful for a broad semantic field of applications, requiring a minimum of customization
- **Maintainability**: A clear separation of components (rules, business logic, and interfaces) strongly supports this attribute
- **OWL Knowledge Base**: The framework has to operate directly on OWL files as this W3C standard has high potential and is now widely used
- **Multiuser Environment**: Applications built on the semantic framework should not be limited to one local store and installation, but should follow a client/server model where multiple clients connect to one server where the central knowledge repository is processed

In the paper [4] we developed a Java prototype for threat simulations facing similar requirements. SPARQL [17], a promising W3C specification for querying RDF graphs, has been integrated. Rather than rules, we implemented classes to handle the business logic. We soon realized that maintaining this program, especially when business logic has to be changed and also new logic is permanently added, is very cumbersome and complicated. While this implementation fulfilled our requirement of OWL file based knowledge stores, maintainability and flexibility were not satisfactory.

Dissolving rules from the core implementation promises greater flexibility and maintainability, therefore we searched for new technologies. The Semantic Web Rule Language (SWRL) [15], yet another W3C recommendation, was one of the candidates we examined. SWRL, based on a combination of OWL with the Unary/Binary Datalog RuleML sub languages of the Rule Markup Language, can be used to infer new knowledge from an existing OWL knowledge base. SWRL is a good solution for moving property values from one individual to another. However, it does not support using consequences of rules to communicate with other programs and is thereby not suitable for our ontological framework.

SWRL is only the language specification and relies on an underlying reasoning engine that processes the rules according to SWRL syntax. JESS [8], a rule engine based on the Rete algorithm [6], can be integrated into Java applications. Java Beans can be directly accessed, manipulated, and created in JESS rules, which facilitates the Java program and rule engine communication. The main problem with this engine has turned out to be that JESS relies on its own working memory for facts and rules, but our framework is built up on separate OWL files for knowledge representation. To feed the JESS memory with OWL knowledge, we have to convert OWL to JESS and back if the knowledge base is modified. In [11] Mei et al. presented an OWL2JESS transformation tool, which derives facts from an initial OWL file by one XSLT style sheet, while the RDF(S) and OWL Semantics are pre-defined as Jess rules. Since external OWL knowledge files that can be edited with alternative tools is an elemental requirement and permanent transformations from OWL to JESS add an inefficient factor, we decided not to use JESS as rule engine in our ontological application framework.

7.1. OntoWorks Architecture

OntoWorks represents the framework architecture we developed for semantic applications, on which the *ISO/IEC 27001 Certification Support Tool* is based. The requirements listed at the beginning of this section were our main concern during the design phase. Figure 5 depicts the *OntoWorks* architecture.

The knowledge store follows the OWL specification and can be a single OWL file or even a native OWL database so-

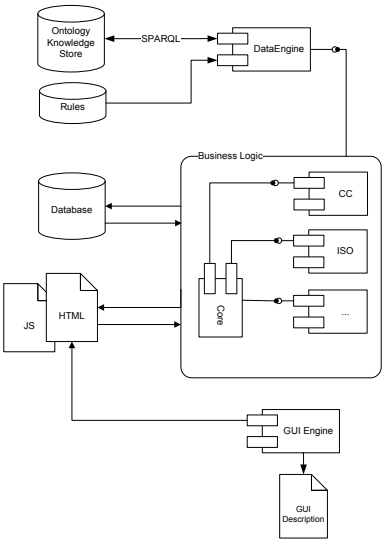

Figure 5. *OntoWorks* **Architecture**

lution, since the connection modules from the engine to the data store can be replaced, based on an interface definition. A topic for further studies is research on and development of OWL database solutions utilizing a relational database model. One of the main components is the engine itself, which establishes the connection to the database and rule repository. Rules are stored separately in XML files or in an XML database solution.

The rule structure is defined as follows: Each rule file starts with the root *rules* tag. *ruleset* tags can surround a set of rules to bundle them and makes it possible to fire rules in combination. The attribute *id* identifies a rule set uniquely. On the next level, rules are defined using the tag *rule*. Each rule consists of a description (*description*), SPARQL queries (*query* and *subquery*), and a consequence (*result*) and has a unique *id* attribute. It is possible to combine query results via the subquery option (an example operation would be the difference of result sets) thus making it possible to overcome the limitations of SPARQL queries. The *result* of a rule is the output of the processed retrieved data. For the *ISO/IEC 27001 Certification Support Tool* results are mostly generated compliance statements in natural language, including links to corresponding knowledge elements. Results are returned as trees in XML format, which makes it easy to operate in loosely linked applications. The following example shows an excerpt from a safety door rule definition for the *A.9.1.1* control (compare Subsection 6.1):

```
<rule id="ISOA911_1">
  <query op="minus">
    <subquery>
    ...
    </subquery>
  </query>
```

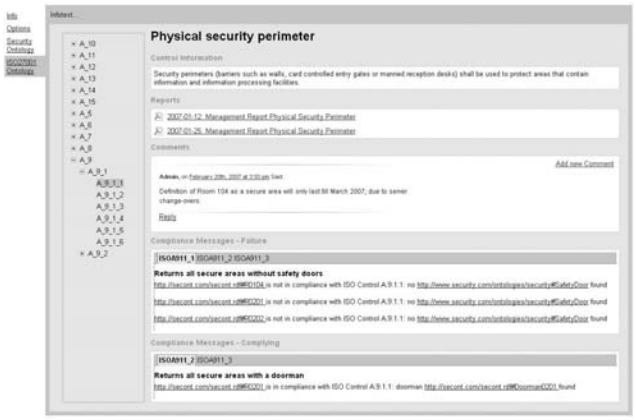

Figure 6. *OntoWorks* **User Interface - Control Area**

```
  <description>Returns all secure areas
   without safety doors
  </description>
  <result>[ ?room is not in compliance
   with ISO Control A.9.1.1: no
   { sec:SafetyDoor } found ]
  </result>
</rule>

Rule ISOA911_1 results:
[ http://secont.com/secont.rdf#R0104 is
not in compliance with ISO Control
A.9.1.1: no sec:SafetyDoor
found ]
...
```

sec:SafetyDoor references the corresponding class in the ontology and can be displayed as a link, which allows the user to inspect possible countermeasures. The *?room* instances are also displayed including the whole namespace, making it possible to access information on the specific rooms by navigating the ontology.

One core application has to exist which instances our *OntoWorks* engine and transfers the rule results to the user interface. Rules can be fired directly by calling the corresponding rule identifier or rule set identifier. A live system, in which changes on the knowledge based might fire rules is a possible further extension of our framework. Besides the core module in the main application, further application specific modules can be attached by an interface. The *Database* element in Figure 5 symbolizes a permanent data store for application specific information (e.g. setting and log files) which are not part of the ontological data store.

The *OntoWorks* user interface prototype is built in the GWT framework [7]. Besides the simple tree-based listing of all ISO/IEC 27001 categories, objectives and controls,

the interface provides necessary and vital information on the actual state of those items in combination with the company's corresponding *Security Ontology*.

Figure 6 shows the control area of the user interface. Besides general information, related former reports and comments, the user interface provides company specific information corresponding to the selected ISO/IEC 27001 control. This information consists of compliance messages, both regarding failing and complying control implementations (see the two areas at the bottom of Figure 6). Relevant parts of the message content, i.e. the *Room* instances or the *Safety Door* class of the *Security Ontology*, are linked to the corresponding elements in the *Security Ontology*.

The category and control objective area are designed in the same manner as the control area described above. Instead of specific compliance messages a tree-based overview of all sub items (control objectives or controls) and their compliance states is given. Resulting from this visualization a summarized view on the state of whole categories or objectives is provided, which raises usability of the prototype and the lucidity of the huge information amount produced during the certification process.

8. Conclusion

In this work we proposed an ontological mapping of the ISO/IEC 27001 standard and its appliance in combination with our *Security Ontology* approach. Furthermore we introduced the *OntoWorks* framework, which allows users to access, visualize, and reason on ontological data. Building upon this framework we provided an overview of its usage for the *ISO/IEC 27001 Ontology* and the *Security Ontology*. The main contribution of this work is on the one hand an automatic partial audit preparation, with the help of IT infrastructure knowledge from the *Security Ontology*, and on the other hand automatic rule-based compliance checks regarding ISO/IEC 27001 controls. Further research activities address the integration and combination of other standards and best practices, the refinement of the *Security Ontology*, and further the development of *OntoWorks* framework extensions.

Acknowledgment

This work was performed at the Research Center Secure Business Austria funded by the Federal Ministry of Economics and Labor of the Republic of Austria (BMWA) and the federal province of Vienna.

References

[1] BASEL2. Basel Committee on Banking Supervision (BCBS), Basel 2 - International Convergence of Capital Measurement and Capital Standards - A Revised Framework, 2001.

[2] British Department of Trade and Industry (DTI). BS7799-2:2002 Information security management systems - Specification with guidance for use, 2002.

[3] A. Ekelhart, S. Fenz, G. Goluch, and E. Weippl. Ontological mapping of common criteria's security assurance requirements. In *22nd IFIP TC-11 International Information Security Conference (IFIPSEC'07)*, 2007.

[4] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl. Security ontology: Simulating threats to corporate assets. In A. Bagchi and V. Atluri, editors, *Information Systems Security*, volume 4332 of *Lecture Notes in Computer Science*, pages 249–259. Springer, Dec 2006.

[5] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl. Security ontologies: Improving quantitative risk analysis. In *40th Hawaii International Conference on System Sciences, HICSS2007*, number 0-7695-2755-8, pages 156–162, Waikoloa, HI, USA, January 2007. IEEE Computer Society.

[6] C. Forgy. Rete: A Fast Algorithm for the Many Patterns/Many Objects Match Problem. *Artif. Intell.*, 19(1):17–37, 1982.

[7] Google. Web Toolkit Beta. http://code.google.com/webtoolkit/.

[8] E. F. Hill. *Jess in Action: Java Rule-Based Systems*. Manning Publications Co., Greenwich, CT, USA, 2003.

[9] International Organization for Standardization and International Electrotechnical Commission. Iso/iec 17799:2005, information technology – code of practice for information security management, 2005.

[10] International Organization for Standardization and International Electrotechnical Commission. Iso/iec 27001:2005, information technology - security techniques - information security management systems- requirements, 2005.

[11] J. Mei, E. P. Bontas, and Z. Lin. OWL2Jess: A Transformational Implementation of the OWL Semantics. In *ISPA Workshops*, pages 599–608, 2005.

[12] PriceWaterhouseCoopers. Information security breaches survey. www.dti.gov.uk/industries/information_security, 2006.

[13] SOX. One hundred seventh congress of the united states of america, sarbanes oxley act - to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes., 2002.

[14] World Wide Web Consortium. OWL Web Ontology Language. http://www.w3.org/TR/owl-features/, 2004.

[15] World Wide Web Consortium. SWRL: A Semantic Web Rule Language Combining OWL and RuleML. http://www.w3.org/Submission/SWRL/, 2004.

[16] World Wide Web Consortium. Resource Description Framework (RDF). www.w3.org/RDF/, 2006.

[17] World Wide Web Consortium. SPARQL Query Language for RDF. http://www.w3.org/TR/rdf-sparql-query/, 2006.