Towards an Ontology-Driven Approach for the Interoperability Problem in Security Compliance

Alfred Ka Yiu Wong*, Nandan Paramesh† and Pradeep Ray‡

*†School of Computer Science and Engineering,
‡School of Information Systems, Technology and Management,
University of New South Wales, Sydney, 2052, Australia
*alfred.ky.wong@gmail.com, †paramesh@cse.unsw.edu.au and ‡p.ray@unsw.edu.au

Abstract

In today's IT-centric, regulated and competitive environment, businesses rely more heavily on IT technologies. Organizations are often challenged by customers, business partners and legal entities to demonstrate their compliance to different IT security and performance standards. The existence of heterogeneous standards and regulations raises the interoperability problem for organizations having to deal with multiple standards. As the issue will grow in complexity, we propose an ontology-driven interoperability approach where the standards can be integrated through the process of ontology mapping between ontologies constructed to model the standards. Consistency, reusability, autonomy and support for intelligent reasoning are prime features of the ontological approach over existing manual custom-designed solutions.

1. Introduction

In today's technology-centric, regulated and competitive environment, businesses rely more heavily on IT technologies. Consequently, IT-related activities, their associated risk and security implications become both the concerns of the corresponding organizations and their business partners and customers. Organizations are required to provide assurance and confidence to customers, business partners and regulators on the organizations' due diligence in securing their IT infrastructure. Demonstration of compliance to best practices and standards are recent trend businesses adopted to secure confidence from their interested parties. There currently exists numerous standards e.g. CobiT, ISO17799, ISF's The Standard of Good Practice. In a heterogeneous environment where the number of regulations e.g. Sarbanes Oxley (SOX), Heathcare Information Portability and Accountability Act (HIPAA) & Gramm Leach Bliley (GLB), and the complexity of the trading environment are on the rise, businesses are often required to work with multiple standards in order to satisfy the different requirements. Collectively, the complexity and heterogeneity poses the interoperability problem.

We propose in this paper an ontology-driven approach to the interoperability problem. Consistency, reusability, autonomy and support for intelligent reasoning (possibly, automates the compliance process) are the prime characteristics of an ontology-driven approach over existing interoperability solutions.

This paper is organized as follow: Section 2 presents some related work. Section 3 elaborates and formalizes the compliance interoperability problem. Section 4 introduces ontology into the interoperability scenario. Section 5 presents the strategies for ontology construction and mapping in the compliance domain. We analyze our approach and discuss on future works in Section 6. Finally, Section 7 concludes.

2. Related Work

The currently ongoing attempts to align and integrate specific standards to achieve interoperability are manually & custom designed and limited to specific standards e.g. (ITGI, OGC & itSMF 2005) documents only high level mappings between CobiT, ITIL and ISO17799, and (Pollard 2005) illustrates correspondences between AS7799 and ISO17799 only. They do not scale in the ever changing compliance environment where N standards could be considered for alignment and integration. Existing approaches will result in the explosions of N^2-N asymmetric or N symmetric custom-designed mappings.

This research utilizes techniques from the fields of ontology construction and mapping. A survey on some of the existing mapping approaches can be found in (Kalfoglou & Schorlemmer 2003). As part of the project, we have adopted our approach detailed in (Wong, Paramesh & Ray 2006).

Ontology have been researched in other domains to enable different tasks e.g. patience information exchange in the medical domain, fraud management (Leary, Vandenberghe & Zeleznikow 2003) in the financial domain, integrated router configuration in the network management domain (A. K. Y. Wong et al. 2005), and holistic & intelligent security management (Wong, Paramesh & Ray 2006), they can also be employed to achieve interoperability between compliance standards.

This research in fact elaborates on the ontology component of the conceptual interoperability framework for the security compliance domain (Yip et al. 2006).

To the best of our knowledge, there currently exists no work on compliance standards interoperability comparable to our approach in terms of autonomy, scalability and support for intelligent reasoning. The closest work will be (Lau, Law & Wiederhold 2005) that attempts to solve a similar problem in the legal domain.

3. Interoperability in Security Compliance

In response to the growing concerns on security issues, existing and emerging regulations (e.g. SOX, GLB, Basel II) across the globe are developed to cast direct impact on security management. As security responsibility and accountability are escalated to top management, managers are urged to conduct regular performance review and security assessment to satisfy the requirements imposed by the regulations and interested parties. Organizations employ different standards and best practices (e.g. CobiT) to demonstrate the quality of their security performance.

While the standards are not mutually exclusive to each other, they differ and overlap in terms of their scope, granularity and focus. For example, CobiT provides a high level compliance framework for an organization, while ITIL provides details on specific guidelines on service management processes. The complexity and heterogeneity of the standards and the compliance domain will grow as corporate IT governance inevitably gains momentum and becomes more and more important.

Organizations having needed to work with multiple standards, are faced with the interoperability problem. We present below the different interoperability scenarios:

For ease of reference and analysis, lets denote $org_1, ...org_n \in Org$ as the set of organizations, $reg_1, ... reg_n \in Reg$ as the set of regulations, $obl_1, ... obl_n \in Obl$ as the set of contractual obligations, $std_1, ... std_n \in Std$ as the set of compliance standards. The process of IT Governance can be viewed as the logical process of *ITGovernance(Reg ⊔ Obl, Org, Std) :- Satisfactory(Std, Reg ⊔ Obl), Compliance(Org, Std)*. *ITGovernance* firstly conducts the process *Satisfactory(Std, Reg ⊔ Obl)* to ensure that the standard *Std* employed helps the organization *Org* in meeting the minimal regulatory *Reg* or contractual *Obl* requirements. Secondly, *Compliance(Org, Std)* is used to ensure *Org* is performing according to the guidelines *Std*.

Interoperability associated with Reg* or *Obl

An international org_1 often has to satisfy different regulations. The different regulations with different requirements will prompt org_1 to demonstrate its compliance to the suitable standards. Consider the following scenario –

ITGovernance(SOX, org_1, CobiT) :- (1)
Satisfactory(CobiT, SOX), (1-S)
Compliance(org_1, CobiT) (1-C)
ITGovernance(GLB, org_1, ISO17799) :- (2)
Satisfactory(ISO17799, GLB), (2-S)
Compliance(org_1, ISO17799) (2-C)

Assume that org_1 has already been performing *(1)* to satisfy *SOX* and would like to perform *(2)* to satisfy *GLB*. Interoperability solution is required when org_1 would like to reuse totally or partially the *(1-C)* efforts on *(2-C)*. Translation from *CobiT* to *ISO17799* is therefore required.

org_1 needing to deal with different trade partners will result in different contractual obligations. Consider the following scenario (e.g. *obl_1 similar to those in HIPPA)* –

Satisfactory(BS7799, obl_1) (3-S)

A particular trade partner prefers *(3-S)*. org_1 accustomed to (1-C) would similarly translate *CobiT* to *BS7799* to achieve reusability.

Interoperability associated with Strategic Requirements

Due to strategic decisions by org_1, the following scenarios might occur:

a. std_1 (e.g. ISO17799) although is well suited to org_1, does not have an official certification process. It would then be convenient for org_1 to employ std_1 as the backbone guideline to aid org_1 in working towards being officially certified against another standard std_n (e.g. AS7799). Mapping is then required.
b. std_1 (e.g. CobiT) is an abstract guideline. org_1 would like to employ other more specific standards std_n and std_m (e.g. ITIL & ISO17799) as the complementary guidelines to strengthen its security compliance performance. Mappings are then required between std_1, std_n and std_m such that they can be consulted as an integrated guideline.
c. org_1 would like to employ the assessment tool designed for another standard std_2 and would like to retain std_1. Translation from std_1 to std_2 is required to apply the assessment tool on std_1.

4. Ontology-Driven Interoperability Framework

Ontology can be defined as a "specification of a conceptualization of a domain" (Gruber 1993). It is constructed to model the semantics (of implicit, explicit and common sense knowledge) of a domain to facilitate knowledge sharing, reuse and specific application tasks. It can be formalized as the tuple of $\bar{O}(\acute{C}, \acute{R}, I, D)$. $\bar{O}$ is an ontology that contains a taxonomy of concepts $\acute{C}$, a set of semantic relationships $\acute{R}$ defined over $\acute{C}$ (i.e. $\acute{R}: \acute{C} \times \acute{C} \ldots \acute{C}$ - a set of n-ary relationships) and a set of instances I (i.e. class instances – $c_n(x) \& c_n \in \acute{C}$; relationship instances – $r_n(c_1(x), \ldots c_n(y)) \& r_n \in \acute{R}$). $\acute{C}$, $\acute{R}$ and I are extracted from the subject domain D such that $\acute{C} \sqcup \acute{R} \sqcup I \subseteq D$.

Ontology mapping refers to the process of semantically bridging two ontologies such that instances from one ontology can be translated into instances of another ontology while preserving the original semantics.

The interoperability problem between compliance standards can be modeled as an ontological problem with the following realizations:

- The heterogeneous compliance problem *Compliance(org, std_n)* versus *Compliance(org, std_m)* can be modeled as the problem of *Compliance(*org, $\bar{O}_n$*)* versus *Compliance(*org, $\bar{O}_m$*)*.
- The translation task between the different standards (i.e. std_n $_{n\text{-}m}\rightarrow_{translation}$ std_m) has two components: syntactic and semantic counterparts (Yip et al. 2006). The semantic counterpart becomes the ontology mapping task $\bar{O}_n \rightarrow_{mapping} \bar{O}_m$.
- Ontological components Ć, Ŕ and I can be obtained from the standards documents *Std* i.e. *Std* scopes D.
- $\rightarrow_{mapping}$ generalizes the specific translations $_{1\text{-}2}\rightarrow_{translation} std_2$, … std_n $_{n\text{-}m}\rightarrow_{translation} std_m$.
- $\bar{O}_n \rightarrow_{mapping} \bar{O}_m$ cross-references $\bar{O}_n$ and $\bar{O}_m$ to facilitate standards alignment, integration and translation.

Figure 1 illustrates the role of ontology along with the key actors required for each component.

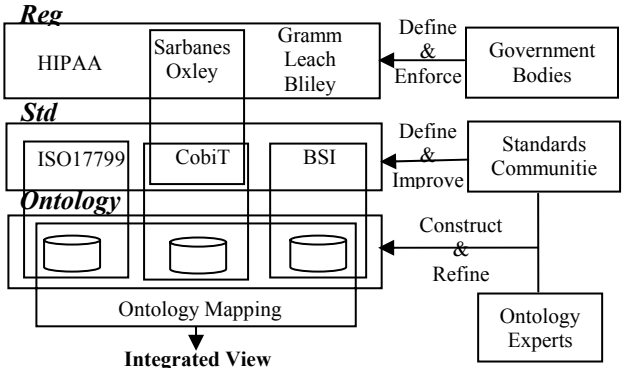

Figure 1. Ontology-Driven Interoperability Framework

As illustrated in Figure 1, interoperability at the *Std* layer is made possible by the ontology layer. (Lau, Law & Wiederhold 2005) promotes interoperability at the *Reg* layer by disambiguating and aligning different regulatory requirements (adds flexibility to *Satisfactory(Std,Reg)*). The integration of the two approaches would enhance the flexibility of standards choice and, hence reduce the complexity of *ITGovernance* (i.e. *reg_1's* can be translated into *reg_2's* requirements, and hence, *std* can be chosen and translated more flexibly).

5. Interoperability Framework Components

In this section, we present the two main components of the ontology-driven interoperability framework: ontologies for the standards and ontology mapping that forms the semantic counterpart of standards translation.

We present the first component as an ontology construction strategy and the second component as an instantiation of our ontology mapping approach (Wong, Paramesh & Ray 2006) with domain-specific parameters.

5.1 Ontology Construction for Standards

Although there is currently no de-facto standard for the process of ontology construction, we have adopted the common conceptual steps (resembling those of METHONTOLOGY). The steps include: knowledge acquisition, conceptualization, classification, semantic modeling and representation.

While knowledge acquisition is straightforward, the remaining steps concern domain specific issues.

Conceptualization involves the identification of concepts Ć within the compliance domain. While the concepts can be straightforwardly identified from the structure of the standards (e.g. sections: Incident Response Procedures, Business Continuity Plan, Security Responsibilities), they are of different abstraction levels. Compliance standards often vary in terms of scope and granularity, different forms of correspondence inevitably exist (e.g. ISF:SM-Security Management can be one-to-many mapped to more specific concepts ISO17799:5-Security Policy, 6-Organization of Information Security). Ć should be structured and prepared to support as many types of ontology-mapping as possible (1-to-1, 1-to-m, m-to-m). In the security compliance domain, Ć can be structured as the following abstraction hierarchy:

- Security Concept (SC): The high level concept that forms part of the security management process. This is usually identified as the sections of the standards (e.g. ISO17799:13- Incident Response Procedure).
- Process & Implementation (PI): Specific steps and procedures that should be performed in order to implement the high level security concepts. This is usually identified from the meaning of the textual descriptions of the different sections (e.g. the specific responsibilities that are specified within the Section ISO17799:13.2.1 Responsibilities and Procedures). Arguably, this layer can be further divided into more layers, depending on the granularity of the standards.
- Primitive: Terminologies that are commonly understood by the security compliance communities. The terms (e.g. information policy) are used as the fundamental building blocks to express higher level concepts. They can be harvested by using text mining tools such as Semio-Tagger, InfoMap … etc.

The identification of concepts from the first two layers is often implicitly guided by the standards structure. On the other hand, identification of *primitives* is a labor-intensive task that requires analyses on every term used within the standards. Methods and tools developed for the domain of natural language processing will alleviate the task. Example tool, Semio-Tagger, has been used and proved successful when applied to a very similar problem in another domain (Lau, Law & Wiederhold 2005).

Classification of Ć is a non-trivial task due to the broad scope and complex nature of the security compliance domain. Although the process of conceptualization may result in a weak taxonomy where some abstract and specific concepts are identified as parent-child classes, the

taxonomy's completeness cannot be guaranteed and its correctness cannot be systematically proved. A sound and complete classification process over Ć is a massive and labor-intensive task. Inconsistencies and errors are often the results of human interventions. In addressing these problems, we have employed the reasoners (e.g. Fact++, Racer) associated with description logic (DL) to automate the process of classification. Our approach relies on the use of OWL (a variant of DL) as the underlying ontology representation language. Automatic classification over Ć is achieved by exploiting the capability of any DL-compatible reasoner in inferring subclass relationship from any $c_n \in$ Ć to any *defined class* $c_{defined} \in$ Ć (*defined class* is any class $c_{defined}$ modeled in DL with a set of *necessary & sufficient conditions (nsc)* such that *nsc* $\rightarrow c_{defined}$ and $c_{defined} \rightarrow$ *nsc*; and *nsc* is essentially the semantics of $c_{defined}$ fully obtained in the next step). In order to maintain the traceability of the classification progress, we have implemented the process as an iteratively procedure where only a single class is flagged as a *defined class* at each iteration. The gradual inference of the subclass relationships can then be documented, reviewed and accepted successively.

Semantic modeling can be regarded as the generic process of capturing the meanings of Ć. The generalization relationships harvested earlier in fact partially dictate the meanings of Ć. While they form the basic semantics of Ć, other semantics are required to facilitate different forms of mapping. Hence, we have identified the following semantic relationships:

- *hasPrinciple*: captures the high level conceptual meaning (modeled in terms of the *primitives*) of a concept (SC or PI). It serves as the fundamental and initial comparison point between two concepts c_1 and c_2. Any decision on further advanced comparison between the two concepts relies on the positive result of this initial comparison. This relationship can be formalized as the following covering axioms:
  Range: $\forall$ *hasPrinciple Primitive*
  Domain: $\forall$ $hasPrinciple^{-}$ $SC \sqcup PI$
- *hasTask*: captures more specific meaning of a specific concept (PI). It is formalized as follow:
  Range: $\forall$ *hasTask Primitive*
  Domain: $\forall$ $hasTask^{-}$ *PI*
- *hasPart*: captures the structural semantics of a concept. It is essential in enabling one-to-many mapping where a section in one standard can be mapped to many subsections distributed over different sections in another standard. The semantics embedded in *hasTask* and *hasPart* together should provide rigorous comparison between c_1 and c_2. *hasPart* can be formalized as:
  Range: $\forall$ *hasPart PI*
  Domain: $\forall$ $hasPart^{-}$ *SC*

Note that the range of *hasPrinciple* and *hasTask* are filled by concepts (range-fillers) defined in terms of *primitives*. The *primitives* extracted by tools (e.g. Semio-Tagger) include nouns (compliance items), verbs (actions) and so on. We have organized the *primitives* into a taxonomy (e.g. noun has direct subclasses of management item, role, utility … etc, and the subclasses are further specialized, with all leaf nodes ultimately populated by *primitives*) such that *primitives* can be correctly and more consistently selected to be part of the range-fillers. Correct selection simply concerns the selection of *primitives* that do not misrepresent the intended semantics. Chances for inconsistency arise when number of correct selections is greater than 1 (e.g. *Information Policy* and *Information Security Policy* are both correct *primitives* to model ISO17799:5- *Security Policy*). Independent selectors might inconsistently choose different correct selections for the same semantics. While correctness of *primitive* selection is guaranteed by the taxonomy (i.e. a *primitive* and its selection are semantically bounded by its precise taxonomic category), we attempt to further enhance the consistency of *primitive* selection by imposing a structure for the range-fillers. We have employed a subset of the English grammar as the structure to reduce the number of possible correct selections in order to minimize the chance for inconsistency:

1. Sentence ← Noun Phrase (NP), Verb Phrase (VP);
2. NP ← NAME; 3. VP ← VERB, NP;
4. VP ← VERB, NP, Preposition Phrase (PP);
6. PP ← PREPOSITION, NP.

Ranger-fillers defined by this grammar are therefore bounded by the following structures (the paths of the tree represented by the grammar subset):

(a) NP1 VP NP2 (b) NP1 VP NP2 PP NP3

For example, (a) imposes that VP *primitive* selection is correct only if there are two correct NP *primitive* selections that correlate to VP. The following OWL-DL compact notation demonstrates the modeling of the partial semantics of the ISF concept of High Level Direction (*underlined* are *primitives* and *hasNP1* *primitive* → *primitive*$\in$*NP* … etc):

$\exists$ *hasPrinciple (Sentence* $\sqcap$ *(*$\exists$ *hasNP1 TopLevelManagement)* $\sqcap$ *((*$\exists$ *hasVP Demonstrate)* $\sqcap$ *((*$\exists$ *hasNP2 ManagementCommitment)* $\sqcap$ *((*$\exists$ *hasPP to)* $\sqcap$ *(*$\exists$ *hasNP3 InformationSecurity)))))*

The above models the semantics: top level management (management role) should demonstrate (action) its commitment (object) to information security (theme).

Representation encodes ontology in a format suitable for the application task. Our ontology mapping approach requires ontology to be encoded in first order logic (FOL) (Wong, Paramesh & Ray 2006). Consequently, we have chosen OWL as the underlying ontology representation language. OWL is a popular ontology language standardized in the semantic web. As existing and emerging ontologies are likely to be encoded in OWL, encoding our ontologies in OWL will ensure their durability, adaptability and expandability. Furthermore, OWL is a decidable fragment of FOL. Conversion from OWL to FOL can be easily achieved. Tools supporting OWL are readily available (e.g. reasoners – Racer, Fact++, ODE – Protégé, OIL Editor).

5.2 Ontology Mapping for Standards Translation

We have adopted our ontology mapping approach (Wong, Paramesh & Ray 2006) to facilitate the task of standards translation. The key components of our approach include

- A similarity function S that bases on SLD resolution to assess the semantic similarity between two concepts. *S* is defined as the weighted summation of the similarity between the comparable semantic aspects of the concepts c_1 and c_2:

$$S(c_1, c_2) = \sum_{i}^{N} \omega(i) \times S_L(L_i(c_1), L_i(c_2))$$

  where *i* denotes a semantic aspect, N is the number of comparable aspects, $L_i(c)$ is the FOL representation of the meaning of *c* with respect to semantic aspect *i*, S_L is a similarity function defined over two FOL logical statements, and ω is a weight distribution function that controls the significance of each semantic aspect *i* in affecting the similarity assessment;
- An ontology traversal strategy that guides the search of the target concept within the target ontology for the source concept.

Mapping between concepts identified in the security compliance domain is based on the semantics defined in their respective ontologies. The three comparison points *hasPrinciple, hasTask* and *hasPart* serve as the different semantic aspects required for the similarity computation. Due to the heterogeneity and voluminous nature of the different standards (i.e. large search space), similarity computation between all concepts basing on all aspects (rigorous semantics) is computationally expensive and not scalable.

To address such mapping challenges, the three comparison points are specially designed and the ω function is carefully studied. The analysis is presented with respect to three mapping stages.

Preliminary Screening performs comparison between c_1 and c_2 to detect minimal correspondence. The associated computational cost is at minimum – $O(P^2)$ where P is the number of predicates used to model all principles. *hasPrinciple*, is designed to capture high-level and simple semantics. Consequently, the configurations: ω(*hasPrinciple*) = 1 ⊓ ω(¬*hasPrinciple*) = 0, should be applied during the traversal process within the target ontology to efficiently scale down the search space.

Concrete Mapping compares c_1 with c_2 basing on their in-depth semantics with computational complexity of $O(T^2)$ where T is number of predicates used to model all tasks, and T is generally much larger than P. The semantic aspect, *hasTask*, is designed to capture specific and detailed semantics. While *hasPrinciple* can be used in conjunction with *hasTask*, *hasPrinciple* is redundant in that *hasTask* should have already covered the semantics embedded in *hasPrinciple*. Depending on the settings, if computational power is strictly limited, ω(*hasTask*) = 1 ⊓ ω(¬*hasTask*) = 0 should be used. Otherwise, ω(*hasTask*) > ω(*hasPrinciple*) > 0 could be used. Such configurations should be applied when searching for definite one-to-one mapping at the leaf layer or at important traversal decision points where traversal basing on the *preliminary screening* configurations results in multiple concepts (paths) with similar or same similarity values.

Advanced Mapping stringently compares c_1 with c_2 basing on their full-fledged semantics. The semantic aspect, *hasPart*, captures the structural semantics which when applied in similarity assessment, can be viewed partially (there are other factors such as section *cross-reference*) as the factor of *neighbor inclusion* (used in some other approaches to model the intuition of: close proximity of the neighbors of c_1 and c_2 implies high probability of the concepts being similar.). While *neighbor inclusion* is generally viewed as additional semantics, the core semantics embedded in *hasTask* should be more dominant than *hasPart*. Hence, the following configurations should be applied: ω(*hasTask*) > ω(*hasPart*) > ω(*hasPrinciple*) > 0 ⊓ ω(*hasTask*) + ω(*hasPrinciple*) + ω(*hasPart*) = 1. Again, *hasPrinciple* can be waived.

Recursively, *hasPart* would lead to comparisons between individual component concepts (the parts). The part-comparisons could adopt any of the discussed configurations. The choice depends on the available computation power and application requirements. For example, in searching for one-to-many mapping, the part-comparisons should at least adopt the *concrete mapping* configurations such that successful comparisons between the components imply one-to-many mapping between c_1 and the components embedded c_2's *hasPart*. On the other hand, part-comparisons could adopt the *preliminary screening* configurations if they are simply used to strengthen the similarity comparison between c_1 and c_2 in the sense of *neighbor inclusion*. The computational complexities are $O(P^2R)$ and $O(T^2R)$ respectively, where R is the number of parts.

For illustration purposes, we present below some mapping examples for the different configuration settings.

Preliminary Screening

S(CobiT:DS5.8 Data Classification → ISO17799:5. Information Classification) = 1 & S(ISO17799:5. Information Classification → CobiT:DS5.8 Data Classification) = 0.68.

Concrete Mapping

S(ISF:SM1.2.2 → ISO17799:5.1.1 Information Security Policy Document) = 0.23 & SM(ISO17799:5.1.1 Information Security Policy Document → ISF:SM1.2.2) = 1.

Advance Mapping

S({ISF:SM1.2.1, ISF:SM1.2.2, ISF:SM1.2.3, ISF:SM1.2.6, ISF:SM1.2.7} → ISO17799:5.1.1 Information Security Policy Document) = 0.81

The result figures are consistent with the facts that *Cobit:DS5.8* covers more concepts than *ISO17799:5*; *ISF:SM1.2.2* includes only subset features of *ISO17799:5.1.1*; and *ISF:SM1.2.1…ISF:SM1.2.7* collectively covers a larger subset features of *ISO17799:5* than *ISF:SM1.2.2* covers by itself.

6. Discussion

We have implemented our approach in Java and selectively constructed ontologies for different standards (e.g. SC concepts for CobiT, SC & PI concepts of SM1,2&3 of ISF and selective modeling of ISO17799 concepts to strategically overlap with CobiT and ISF for experimental purposes). The ontologies are developed using Protégé as the ODE environment. They are interfaced with the ontology mapping approach by converting their OWL-DL representations into FOL.

The experiments performed on running through the modeled ISO17799 concepts for target matches (in ISF and CobiT) indicate conceptual consistency between the meaning of the similarity figures and the actual facts. However, the similarity figures in some cases could have been lower or higher to better reflect the actual facts. Such discrepancies are due to the chance for inconsistency during *primitive* selection (e.g. security-policy-related source concept uses *Information Policy*, while target concept uses *Information Security Policy*, rendering the former being more abstract). Further studies are required to minimize such chance. A possible enhancement is to further reduce the number of possible correct selections by employing statistics and linguistics means e.g. words correlation, frequency of word usage that can be obtained from tools such as Oxford Wordsmith. Formal techniques from data mining and natural language processing might possibly enhance the quality of the standards ontology.

The study in section 5.2 is particularly important. Imagine the search path from the root to the target concept in the target ontology. The search passes through M traversal decision point (intermediate nodes), and at each point, there are N possible choices (siblings/paths). The computational complexity of the search performed by (Wong, Paramesh & Ray 2006) in its native form is $O((P^2+T^2+T^2R)N(M+1))$. Section 5.2 refines the search with domain-specific strategies to attain a much better computational complexity of $O(P^2(1+NM)+T^2(1+R))$ - assuming that the *screening* configuration is used at decision points and *advanced* configuration is used between the source and final target concept.

Furthermore, ontology is definitely not limited to the interoperability problem. Current *Compliance(org, std)* is a manual checklist process performed by a specialist (e.g. CISO). The introduction of the ontology layer would translate the process into *Compliance(org,* $\bar{O}_{std}$*)*. If the process is further modeled as *Compliance(*$\bar{O}_{org}$*,* $\bar{O}_{std}$*)*, it could be automated as the intelligent ontology mapping process between $\bar{O}_{org}$ and $\bar{O}_{std}$, where $\bar{O}_{org}$ is obtained as a distributed (*org*'s) knowledge collection process.

7. Conclusion

We have presented in this paper an ontology-driven interoperability framework for the security compliance domain. We have laid the background on security compliance, formalized different interoperability scenarios and motivated the ontological approach.

Specific issues, challenges and implementation details of our ontological approach are presented in its two main components: ontology construction and ontology mapping for security compliance.

Performed experiments demonstrate conceptually correct results promising the role and benefits of ontology in automating and solving the interoperability problem. This research adds value to the currently growing and significant domain of IT Governance. And it lays the foundation for possible future researches on automatic and intelligent security compliance.

References

ITGI. 2001. *Board Briefing on IT Governance*. ISBN 1-893209-27-X.

Yip, F., Wong, A. K. Y., Ray, P., and Paramesh, N. 2006. *Corporate Security Compliance in a Heterogeneous Environment*. Forthcoming in IEEE NOMS Poster 2006.

ITGI, OGC, and itSMF. 2005. *Aligning COBIT, ITIL and ISO 17799 for Business Benefits*. Whitepaper [online] http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22490

Pollard, M. *Developing an AS 7799 and ISO 17799 Compliant Information Security Management System*. Whitepaper [online]: http://www.bridgepoint.com.au/Documents/7799paper.pdf

Gruber, T. 1993. *Towards principles for the design of ontologies used for knowledge sharing*. Presented at the Padua workshop on Formal Ontology, March.

Leary, R. M., Vandenberghe, W., and Zeleznikow, J. 2003. *Towards A Financial Fraud Ontology A Legal Modelling Approach*. ICAIL Workshop on Legal Ontologies & Web based legal information management.

Wong, A. K. Y., Paramesh, N., and Ray, P. 2006. *Towards an Ontology Mapping Approach for Security Management*. Forthcoming in IJAIT 2006.

Wong, A. K. Y., Ray, P., Paramesh, N., and Strassner, J. 2005. *Ontology Mapping for the Interoperability Problem in Network Management.* IEEE Journal on Selected Areas in Communications (JSAC), Oct, vol. 23, no. 10, pp. 2050-2058.

Kalfoglou, Y., and Schorlemmer, M. 2003. *Ontology mapping: the state of the art*. The Knowledge Engineering Review, vol. 18, no. 1, pp. 1-13.

Lau, G. T., Law, K. H., and Wiederhold, G. 2005. *Legal Information Retrieval and Application to E-Rulemaking*. Proceedings of the 10th International Conference on Artificial Intelligence and Law (ICAIL), Bolongna, Italy, pp. 146-154, Jun 6-11.