Computing and Informatics, Vol. 27, 2008, 131–155

TOWARDS SEMANTIC INTEROPERABILITY FOR IT GOVERNANCE: AN ONTOLOGICAL APPROACH

Alfred Wong, Frederick Yip, Pradeep Ray, Nandan Paramesh

School of Computer Science and Engineering
School of Information Systems, Technology and Management
University of New South Wales
Sydney, 2052, Australia
e-mail: {akyw389@cse., fyip@cse., p.ray@, paramesh@cse.}unsw.edu.au

Revised manuscript received 11 January 2007

Abstract. In today's IT-centric environment, businesses rely more heavily on IT technologies. Organizations are often obliged to satisfy different requirements demanded and imposed by customers, business partners and legal entities. With increasing regulatory requirements, various best practices and standards are phenomenally employed to benchmark organizational adherence to different regulations. In a heterogeneous, multi-regulated, multi-disciplined and global environment, corporations are often required to consult with multiple standards. Interoperability between the standards for heterogeneous compliance management in the forms of semantic data translation and data integration is subsequently required. Semantic translation between standards allows compliance efforts established on a standard to be based on another standard. On the other hand, semantic data integration enables an integrated view of multiple standards. We present in this paper an ontology-based approach to the semantic interoperability problem in the domain of IT governance.

Keywords: Ontology, ontology mapping, semantic interoperability, compliance management, IT governance

1 INTRODUCTION

In today's technology-centric, regulated and competitive environment, businesses rely more heavily on IT technologies. IT-related activities, their associated risk and security implications become both the concerns of the corresponding organizations and their stakeholders. In particular, the recent proliferation of regulations such as Sarbanes Oxley (SOX), Gramm Leach Bliley, Basel II, and HIPAA poses unprecedented challenges to participating organizations. The regulations are regional specific, distributed and span across multiple disciplinary domains such as banking and healthcare. Organizations are increasingly pressured by business partners and customers to demonstrate their due diligence in securing and efficiently utilizing their IT components. The requirments are increasingly associated with legal implications and implications on organizational reputation. Consequently, strong emphasis is now placed on IT governance that prompts organizations to implement controls for ensuring and measuring their compliance to the diverse pool of requirements. Phenomenally, corporations employ different best practices and standards to benchmark their adherence to the relevant requirements. Currently, there exist numerous standards such as CobiT [10], ISO 17799 [9], ITIL, and Baseline Protection Manual (BSI) [11]. While the number is on the rise, along with the differing scopes and granularities of the standards, interoperability between the standards becomes an evident problem for multi-disciplined (i.e. spans across multiple domains) and multi-regulated (i.e. international organization with different regional branches) corporations. In this paper we have investigated the semantic interoperability problem in two forms, namely semantic data translation and semantic data integration.

Semantic data translation. This form of interoperability is required when knowledge in a familiarized standard is to be reused for either understanding or its application on another standard. Examples:

- An organization accustomed to one standard (e.g. ISF's The Standard of Good Practice) would like to employ the compliance assessment tool proprietarily/officially developed for another standard (e.g. ISO 17799). Translation from the first to the latter is then required.
- An international organization that spans across UK and USA is subjected to different regulations such as Basel II, and SOX. The compliance efforts performed against ISO 17799 in USA would be best to be reused on understanding if the organization is also complying with CobiT in UK. Translation between ISO 17799 and CobiT is then required.

Data semantic integration. This form of interoperability is required when isolated pieces of knowledge are to be interpreted complementarily and supplementarily. Examples:

- An organization would like to be officially certified against a standard (e.g. AS7799.2); but due to incompleteness or abstraction of the standard, the organization would like to consult supplementary details from other standards that have an official certification process (e.g. ISO 17799). Mappings between the standards would then be necessary in order for the standards to be interpreted complementarily.

- An organization would want to consult CobiT as high level and conceptual guidelines (due to its abstractness), use ISO 17799 as complementary materials (for completeness, since ISO 17799 is more specific and its coverage differs slightly from CobiT), and employ ITIL to supplement knowledge on IT performance (which is not a focus of CobiT and ISO 17799). Semantic integration between the standards bridging their differences is then required to provide an integrated view.

The main challenges of the semantic interoperability problem center at the variations and heterogeneities in the compliance domain. New and existing regulations, best practices and compliance standards are constantly emerging and changing. The standards developed by different communities differ in scope, granularity and focus. These complications of semantic differences and uncontrollable quantity of regulations and standards will grow as corporate IT governance inevitably gains more and more momentum and becomes increasingly important.

In this paper we propose an ontology-based approach to the semantic interoperability problem in the domain of IT governance. As heterogeneous compliance requires interoperability at the semantic level rather than merely syntactic or structural level, an ontology-based approach becomes a natural semantic solution. Discussed in [18, 20, 21], an ontology-based approach is more scalable (i.e. multipoint mapping), flexibile (i.e. supports for intelligent reasoning) and dynamic (i.e. mapping results dynamically updated as ontologies evolve along with changes to compliance standards) than manual efforts in aligning the standards. This paper is an extended version of the workshop paper published in the 1st International Workshop on Semantic e-Science [21].

While the aforementioned generic scenarios of semantic interoperability are far from exhaustive, they are applicable to all organizations that are subjected to the jurisdiction of any regulations and regional influences such as geographical factor and cultural differences. Real live scenarios can easily be observed in some particular industries such as healthcare and banking where organizations are strictly controlled and multi-regulated. The requirements for semantic interoperability are unarguably essential as evident by the numurous existing professional community efforts [2, 3, 4, 5, 6]. Without loss of generality, we demonstrate in this paper our ontology-based approach to the interoperability between the two most common standards, namely CobiT [10] and ISO 17799 [9].

This paper is organized as follows: Section 2 details the background on IT governance, and Section 3 introduces the concepts of ontology and ontology mapping. Section 4 presents an ontology-based interoperability framework. Section 5 details the steps, techniques and tools used to transform the compliance standards into ontologies that are then used by our ontology mapping approach described in Section 6. Section 7 presents the experiments performed and Section 8 highlights some of the related work. This paper concludes with Section 9.

2 BACKGROUND: IT GOVERNANCE

IT governance involves the main task of "specifying a framework for decision making, with assigned decision rights and accountabilities, intended to consistently produce desired behaviors and actions" [1]. The process is often guided by industry standards and best practices and is designed to help organizations satisfy mandatory regulatory requirements. An integral part of IT governance, Compliance Management (CM), is a collective process of organizational attempts in demonstrating satisfaction of the different expectations and requirements. This process is a continuous and labor intensive task that involves business commitments in demonstrating organizational alignment and compliance to the prevailing regulations and requirements such as Sarbanes Oxley and Basel II. Compliance Management is phenomenally implemented as a standards-based question-answering process and is a crucial process for many organizations due to the increased emphasis on information security. It has been widely recognized that information security is as much a management problem as it is a technology problem. Management is delegated with increasing responsibilities and is accountable for corporate information security incidents. In general, IT governance concerns more than safeguarding and protection of the business processes, assets and resources while minimizing any disruptions that might occur in daily activities. Any controls and measure implemented to achieve information security should be managerially monitored, reviewed and enhanced on a regular basis.

A distinct challenge in compliance management is interoperability, in a recent survey conducted by Symantec; it was found that 3 out of 4 organizations needed to comply with multiple regulations are struggling to meet audits each year with a large amount of IT resources being spent specifically to demonstrate IT security compliance. On average, more than one-third of IT resources are being spent on satisfying multiple regulation compliance demands. While organizations are compelled to work with multiple standards to satisfy the different regulatory requirements, automating the compliance and governance process becomes a challenging semantic interoperability problem.

Relevant standards and best practices are employed to generate sets of compliance "checkpoint" items (a. k. a. questions) to benchmark an organizational adherence (a. k. a. answer) to applicable requirements and expectations. Requirements can take the form of policies, laws or regulations such as Sarbanes Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPAA) while expectations are related to organizational obligations to the stakeholders of the business.

In subsequent subsections, we will motivate the importance of compliance, provide background on some of the important regulatory requirements that mandate the task of compliance, introduce a few well known standards and best practices, and discuss the phenomenally adopted standards-based question-answering implementation of CM along with its limitations.

2.1 Importance of Compliance

The importance of compliance is motivated profoundly by the increasing emphasis on information security as evident in different surveys such as [33]. A key component of compliance management is the compliance auditing process. Compliance audit is a question answering process that reveal whether designed and specified controls are employed and used correctly. This audit function assesses the organization's level of adherence to the applicable laws and regulations and allows senior management to monitor and review the effectiveness or deficiencies of the controls and compliance program. In the case of information security, compliance auditors use standards and guidelines such as ISO 17799 and CobiT as baselines for compliance evaluation. An inadequate compliance program or non-compliance to relevant requirements may result in heavy fines, loss of industry licenses or the ban to be listed in the public stock exchange. In many case, senior managements are responsible for non-compliance of the regulations and are banned to hold further directorship of any company.

Nowadays, organizational computers do not merely record business transactions but in fact drive the key processes of the business. With information being the most important organizational asset, upper level management and business managers become very concerned with the risks of information system failures and the theft or loss of data. Effective and accurate compliance audits are crucial in terms of detecting any IT security processes that are not up to scratch and provide constructive feedbacks, assurances and suggestions to rectify any potential risks.

There are three types of activities involved in information security management. Firstly, management is performed in accordance to regulatory requirements. Enterprises, especially banking and public companies, are required to meet the requirements of regulations such as the Sarbanes-Oxley Act (SOX) which mandates that all public organizations demonstrate due diligence in the disclosure of their information and implement a series of internal controls and procedures to communicate, store and protect that data [7].

Secondly, in response to the growing security awareness of the public, security management function assumes the important role that ensures the satisfaction of the regulatory and ethical requirements demanded by stakeholders of the business. Such requirements are satisfied by organizations through their demonstration of compliance to different prevailing standards (e.g. CobiT [10]).

Lastly, management of information security activities encourage corporate security awareness and culture, strategies and processes to prevent and respond (e.g., business continuity and incident recovery) to potential security threats.

The above activities and issues collectively form the essence of compliance and corporate IT governance in general, as illustrated in Figure 1.

2.2 Government Regulations

We present in this section several prominent regulations that contribute to the importance of Compliance Management.

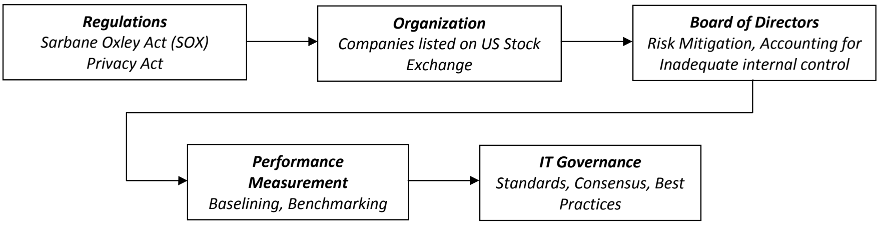

Fig. 1. IT governance process

Sarbanes Oxley (SOX): Sarbanes-Oxley Act is considered as the single most important piece of legislation affecting corporate governance, financial disclosure and the practice of public accounting since the US securities laws of the early 1930s [7]. SOX redesigned the accountability requirements of corporate governance officers, requiring senior management to certify their companies' financial results and be held personally accountable for the accuracy of the results. The penalties are very severe and potentially carry both criminal and class-action lawsuits. SOX aim at preventing corporate scandals such as those involving MCI and WorldCom. Public corporations will be accountable for their financial numbers and are required to implement a series of internal controls and audits to ensure compliance with the applicable regulations.

HIPAA: Health Insurance Portability and Accountability Act regulates the protection, portability and privacy of an individual's medical information [8]. HIPAA affects any organizations and its partners and vendors that maintain patients' personal medical information. Medical information is highly confidential, sensitive and prone to potential of data abuse. The HIPAA legislation mandates organizations to protect information from security breach and threats and rectify any problem when a breach occurs.

2.3 Information Security Standards

We present in this subsection several prominent standards and best practices that are implemented by organizations as guidance for complying with the relevant laws and regulations in the domain of information security.

ISO/IEC 17799:2005: ISO/IEC 17799:2005 established by the International Organization for Standardization is a popular internationally recognized standard which details guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization [9]. Within the document, the objectives are outlined to provide a general guidance and best practices for information security management that are commonly accepted. The requirements of risk assessment in a corporate environment are addressed by the control objectives and controls within the standard.

To assist organizations becoming compliant to the standard, assessment toolkits are made available. The toolkits consist of the standards and security policies templates that correspond to the controls outlined in the ISO 17799 document. Internationally, over 80 000 firms are said to be ISO 17799 compliant, firms from the US that use ISO 17799 appear to use it as a guideline and select specific controls applicable to their environment. In general, they do not seek certification of the entire standard. Instead, firms seek compliance with portions of the standard relevant to their business operations [12].

Control Objectives for Information and related Technology (CobiT): CobiT is a standard published by the IT governance Institute. CobiT has been developed as a generally applicable and industry accepted standard for good information security and control practices. It provides a reference framework for management, users, and information security audit, control and security practitioners. CobiT includes a framework that responds to the management's need for adequate control and measurement of IT by providing tools to assess, measure and benchmark the enterprise's IT capability for the 34 CobiT IT processes [10].

BSI – IT Baseline Protection Manual: The IT Baseline Protection Manual offered by the BSI group aims to guide organizations in achieving a security level for IT systems that is reasonable and adequate to satisfy normal protection requirements. BSI can also serve as a guideline for IT systems and applications requiring a high degree of protection. The protection is achieved through the suitable use of organizational, personnel, infrastructural and technical standard security safeguards [11].

3 PRELIMINARIES: ONTOLOGY AND ONTOLOGY MAPPING

A frequently referenced definition of ontololgy defines ontology as "an explicit specification of a shared conceptualization of a domain" [14]. It is constructed to capture implicit, explicit and commonsense knowledge of a domain such that the knowledge can be shared, reused and consumed by autonomous computer agents. Ontology can be formulated as a tuple $O(TBox, ABox, D)$ where

1. $TBox$ is the intentional knowledge of O; it can be formulated as a tuple of (C, R);
2. $ABox$ is the extensional knowledge of O; it can be formulated as a tuple of (C^I, RI);
3. D is the domain of the ontology – universe of discourse;
4. C is a partially-ordered set of concepts (or a taxonomy of concepts) from D;
5. R is a set of n-ary relationships defined over C, i.e. $R \subseteq C^n$ from D;
6. C^I is a set of class instances – $c(i)$ where $c \in C$, $i \in$ *instance-identifier*;

7. R^I is a set of relation instances – $r(i, \ldots, j)$ where $r \in R, i, \ldots, j \in$ *instance-identifier.*

The semantics of an ontological concept $c \in C$ is intentionally defined by its inherent attributes, its inward (i.e. relations with c as range) and outward (i.e. relations with c as domain) set of relationships $R^c \subseteq R$, and any axioms that refer to c; and extensionally the concept is defined by both its set of $c(i)$ and the set of $r(i, \ldots, j)$ where $c \in C$, $r \in R^c, i, \ldots, j$ instance-identifier.

Ontology mapping bridges the semantic differences between a pair of ontologies. It serves as a common platform for accessing heterogeneous ontologies. While there are different forms of ontology mapping such as ontology articulation elicitation, and integration of multiple ontologies in the field of ontology merging, the fundamental process involves the comparison between two atomic ontological concepts. We adopt the meaning of ontology mapping between a source and a target ontology as the process of finding the best matches for every source concept to a target concept(s) and vice versa [15, 16, 17].

For more treatments on logics (i.e. SLD Resolution, *model theory*, First Order Logic), please refer to [32].

4 ONTOLOGY-BASED INTEROPERABILITY FRAMEWORK

We present in this section an ontology-based approach to the semantic interoperability problem between the compliance standards. The core components include

Ontology Construction (Section 5) – for each standard s, an ontology $O_s(TBoxs, ABoxs, S)$ is constructed to model the semantics of s, where C, R, C^I and R^I are extracted from the domain s, and

Ontology Mapping (Section 6) – a technique that provides integrated access to different ontologies in order to bridge the semantic differences between the standards.

The two components facilitate the applications of standards translation and integration at the semantic level. Figure 2 depicts the IT governance interoperability framework. The main actors include:

Regulators – parties that impose legal requirements related to different regulations (e.g. [7, 8]) on the organization.

Business Partners – parties that are interested in the performance, professionalism and stability of the organization measured in terms of its adopted management and operational practices.

Customers – parties that are interested in the ability of the organization in securing and protecting their rights (e.g. personal information confidentiality).

Ontology Engineer – a solution provider independent of the organization and other actors. The engineer constructs the ontologies for the standards objectively.

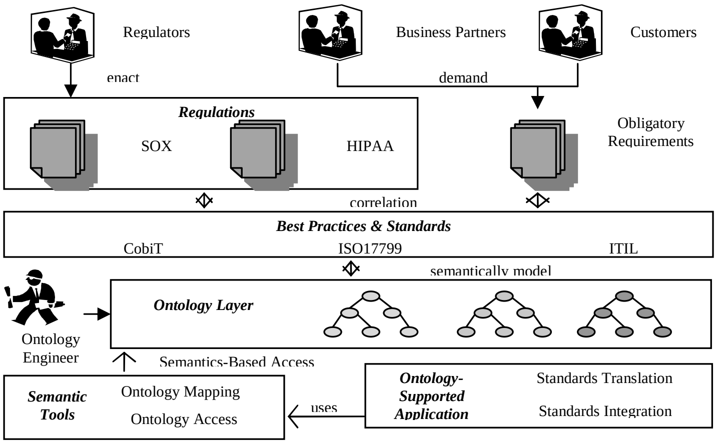

Fig. 2. Ontology-based interoperability framework for IT governance

5 ONTOLOGY PREPARATION

This section presents the techniques and steps used in converting the standards to their corresponding ontologies. The overall process of preparing the ontologies is depicted in Figure 3. The main conceptual steps include the following:

- Analysis of natural language found in the standards.
- Identification of words/terms as modeling primitives and concepts.
- Utilization of semantic models such as process model and RDF's subject-action-object model to formalize the semantics of higher level concepts.
- Adoption of ontology construction methodology with commonly followed steps of conceptualization, modeling, classification and so on.
- Taxonomy construction by categorization of the modeled concepts.
- Utilization of logical reasoners for assisting the completion of taxonomy with automatic "subsumption relationship" inference.
- Utilization of logical reasoners for validation of ontological consistency.

While there are numerous steps for ontology preparation, the step of converting th raw text standards document into machine interpretable data structures is the most challenging task. Such conversion requires natural language processing (NLP) techniques. A key task of NLP is word sense disambiguation, e.g. a polysemic word can have multiple interpretations or multiple synonymic words can have the same meaning. In order to minimize the chance of encountering ambiguities, on top of stop words, any non-content bearing words are filtered out, i.e. words that carry insignificant semantics. These words are filtered out using

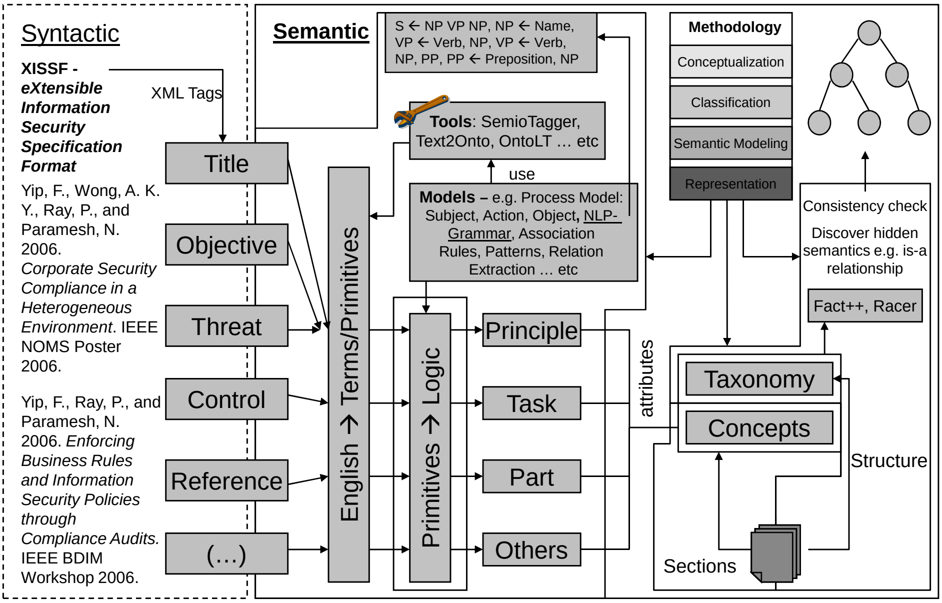
Syntactic
XISSF - eXtensible Information Security Specification Format
XML Tags
Yip, F., Wong, A. K. Y., Ray, P., and Paramesh, N. 2006. Corporate Security Compliance in a Heterogeneous Environment. IEEE NOMS Poster 2006.
Yip, F., Ray, P., and Paramesh, N. 2006. Enforcing Business Rules and Information Security Policies through Compliance Audits. IEEE BDIM Workshop 2006.
Title
Objective
Threat
Control
Reference
(…)
Semantic
S ← NP VP NP, NP ← Name, VP ← Verb, NP, VP ← Verb, NP, PP, PP ← Preposition, NP
Tools: SemioTagger, Text2Onto, OntoLT … etc
use
Models – e.g. Process Model: Subject, Action, Object, NLP-Grammar, Association Rules, Patterns, Relation Extraction … etc
English → Terms/Primitives
Primitives → Logic
Principle
Task
Part
Others
attributes
Methodology
Conceptualization
Classification
Semantic Modeling
Representation
Consistency check
Discover hidden semantics e.g. is-a relationship
Fact++, Racer
Taxonomy
Concepts
Structure
Sections

Fig. 3. Ontology preparation process overview

an exclusion list. Word stemming technique is then used to further reduce synonymic words i) suffix stripping – remove the suffixes, e.g. “going”, and “gone” becomes “go”, and ii) lemmatization for conflation – convert a word into its base form.

Furthermore, the words are converted into our modelling primitives by tagging them using a part-of-speech tagger – TreeTagger [30] that categorizes the words into noun, verb, adjective and preposition. The selected categories align intuitively with the semantic model we chose to represent the standards. The model is an extension to RDF’s subject-action-object model. We deepen the subject-action-object model by considering it as complex-subject-action-complex-object. That is, the “subject” or “object” is no longer merely described by a single term. Optionally, it can be described by a combination of sensible terms. The sensibility of the combination is determined by the following rule: Subject/Object ← $(j^*np)^*n$ or j^*n. Each concept of the standards is semi-automatically (i.e. automation by formal concept analysis – model primitives as formal concepts and their categories and roles as formal attributes; human intervention is required whenever ambiguities and inconsistencies are encountered) modeled in terms of the primitives accordingly and stored in an enriched bag of words (EBOW) format. EBOW is subsequently encoded in First Order Logic (FOL). The concepts are then categorized into a taxonomy. Figure 4 depicts the conversion process from standards to ontology (encoded in FOL).

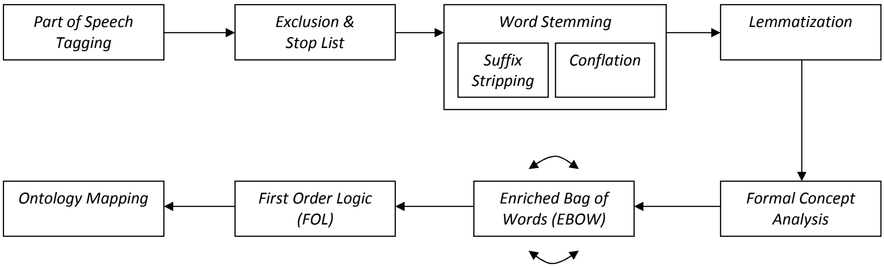

Fig. 4. Semi-automated conversion process from raw text into FOL

6 ONTOLOGY MAPPING

We present in this section the core component of our mapping approach. We have adopted a modified and enhanced version of our ontology mapping approach defined in details in [17, 18, 19]. Due to the scope of this paper, we will only highlight the key concepts required to understand the experiments presented in Section 7. The two main components of the mapping technique are defined in the following subsections.

6.1 Similarity Function

The first component is a similarity function S defined over two concepts C_1 and C_2. S is defined as a weighted summation of the similarities between the concepts from different perspectives (i.e. the different comparable semantic aspects – e.g. functional perspective, structural perspective). Mathematically, S is defined as:

$$S(C_1, C_2) = \sum_{i}^{N} \omega(i) \times S_L(L_i(C_1), L_i(C_2), S_p, \omega_p) \tag{1}$$

where i is the index of a semantic aspect, N is the number of comparable aspects, $L_i(C)$ is the FOL program that encodes the intentional meaning (i.e. c, R^c & axioms) of C from the perspective of i, S_L is a similarity function defined over two FOL statements, S_p is a similarity function defined over primitives, ω is a weight distribution defined over i that controls the significance of each perspective in influencing the similarity assessment, and ω_p is a weight distribution defined over the primitives.

We highlight some of the important properties of S, S_L, and S_p:

- $S(x, y) \in [0..1]$: bounded
- $S(x, x) = 1$: reflexive
- $S(x, y) = S(y, x)$: symmetric
- $S(x, y) = 1 - d(x, y)$, d is a distance function & $d(x, y) \in [0..1]$

In [16, 17, 18, 19], S$_L$ is modeled as two successive processes: quantification on successive predicate SLD resolutions (i.e. exact or approximate predicate resolution via substitution and unification) and normalization over total number predicates. While SLD resolution is a computational mechanism of logical inference, logical equivalence is inferred through refutation. In terms of *model theory*, this is conceptually equivalent to the process of firstly negating one of the concepts that are being compared, and secondly finding a logical model from the negated/normal concept that is not a valid logical model of the normal/negated concept. Such approach only considers the models that lead to refutation and overlooks the rest of the logical models. Since logical model represents the semantic essence of a logical statement, we develop S_L in this paper directly basing on *model theory* where every single logical model is considered and compared against (i.e. quantification on number of common/similar models, and normalization over total number of logical models) to ensure the similarity assessment is semantically grounded.

Furthermore, we have introduced the predicate weight distribution, i.e. ω_p. It is introduced to allow the ontology engineer to assign different degree of importance of different primitives to the semantics of a particular concept. Consequently, granular similarity assessment can be achieved.

6.2 Search Strategy

The second component is a search strategy that locates the best possible matches from the target ontology. It relies on a mapping classification scheme that categorizes a mapping relation as the following:

- $S^{\rightarrow}(C \rightarrow C) = S^{\rightarrow}(C \rightarrow C') = 1$: C is equivalent to C';
- $S^{\rightarrow}(C' \rightarrow C)$ greater than $S^{\rightarrow}(C \rightarrow C')$: C is a super-concept of C';
- $S^{\rightarrow}(C \rightarrow C')$ greater than $S^{\rightarrow}(C' \rightarrow C)$: C is a sub-concept of C';

$S^{\rightarrow}$ is the asymmetric version of S. S is made asymmetric through normalization of the similarity score by the size of the source concept, i.e. size of the FOL logic program. The scheme is derived to reduce the search space such that the target concepts can be strategically located from the target ontology. For more details, please refer to [16, 17].

7 EXPERIMENTS

We present in this section some experiments on the mapping between the two standards of CobiT and ISO 17799. We provide some analysis on the intuitiveness and quality of the results. Table 1 presents the test data (i.e. set of CobiT and ISO 17799 concepts) used in the experiments.

Experiments: For each pair of CobiT and ISO 17799 concept, we compute its similarity by using the ontology mapping technique outlined in Section 6. Since the set of primitives/terminologies used for CobiT is different from ISO 17799, we instantiate S_p as the WordNet-based lexicon similarity function developed by [31].

Code	Description
C_1	Cobit (DS4) – Ensure Continuous Service
C_2	Cobit (DS8) – Manage Service Desk and Incidents
C_3	Cobit (DS5) – Ensure System Security
C_4	Cobit (PO4) – Define the IT Organisation and Relationships
C_5	Cobit (PO6) – Communicate Management Aims and Direction
S_1	ISO 17799 (14.1) – Information Security Aspects of Business Continuity Management
S_2	ISO 17799 (13.1) – Reporting Information Security Events and Weaknesses
S_3	ISO 17799 (6.1) – Internal Organization
S_4	ISO 17799 (9.1) – Secure Areas
S_5	ISO 17799 (5.1) – Information Security Policy
S_6	ISO 17799 (9.2) – Equipment Security
S_7	ISO 17799 (10.1) – Operational Procedures and Responsibilities

Table 1. Test data: CobiT and ISO 17799

Configurations: Primitives as stated in Section 6 are categorized into n, v, j and p. The algorithm is configured to assign minimum similarity of 0 to primitives from different categories. The different experimental configuration settings are as follows:

a. ω_p is a uniform weight distribution; and only one semantic aspect is considered i.e. @objective.
b. ω_p is a non-uniform weight distribution where each primitive is weighted by 1/frequency(primitive) and frequency(primitive) is the number of occurrences of the primitive in the corpus of ISO 17799 and CobiT; and only one semantic aspect is considered, i.e. @objective.
c. Same as a. except that another semantic aspect is also considered i.e. @'threat; and ω is a uniform weight distribution.
d. Same as b. except that another semantic aspect is also considered i.e.@'threat; and ω is a uniform weight distribution.

Results: The similarity values are presented in Table 2 in the form of a matrix. Each cell presents the similarity values between the row and column concept with a., b., c. and d. separating the values for different configurations. The last line of each cell represents the similarity assessment by a domain expert where Similar, Relevant and Irrelevant denote very similar, related and irrelevant respectively. Some concepts do not have the @'threat-related semantics, hence only the @objective-related semantics is assessed.

Result Analysis: Evaluations of the results are based on human judgment by a domain expert and benchmarked against the manual alignment efforts between Cobit, ISO 17799 and ITIL [2]. We will now provide the following two forms of analyses on Table 2.

Concept	C_1	C_2	C_3	C_4	C_5
S_1	a. 0.730	a. 0.764	a. 0.750	a. 0.748	a. 0.735
	b. 0.773	b. 0.761	b. 0.761	b. 0.799	b. 0.730
	c. 0.705	c. 0.614	c. 0.732	c.0.711	c. 0.691
	d. 0.743	d. 0.643	d. 0.787	d.0.784	d. 0.716
Human Judgment	Similar	Relevant	Irrelevant	Relevant	Relevant
S_2	a. 0.724	*a.* 0.750	a. 0.765	a. 0.733	a. 0.732
	b. 0.718	*b.* 0.745	b. 0.750	b. 0.791	b. 0.706
	c. 0.682	*c.* 0.597	c. 0.730	c.0.723	c. 0.713
	d. 0.680	*d.* 0.633	d. 0.721	d.0.761	d. 0.703
Human Judgment	Relevant	Relevant	Irrelevant	Relevant	Irrelevant
S_3	a. 0.700	a. 0.764	a. 0.784	a. 0.740	a. 0.743
	b. 0.700	b. 0.729	b. 0.781	b. 0.751	b. 0.700
	c. 0.556	c. 0.615	c. 0.626	c.0.739	c. 0.602
	d. 0.624	d. 0.686	d. 0.706	d.0.751	d. 0.576
Human Judgment	Relevant	Irrelevant	Relevant	Relevant	Irrelevant
S_4	a. 0.604	a. 0.623	a. 0.621	a. 0.640	a. 0.640
	b. 0.702	b. 0.695	b. 0.627	b. 0.738	b. 0.706
	c. 0.574	c. 0.506	c. 0.589	c.0.610	c. 0.537
	d. 0.667	d. 0.576	d. 0.700	d.0.771	d. 0.646
Human Judgment	Irrelevant	Irrelevant	Relevant	Irrelevant	Irrelevant
S_5	a. 0.685	a. 0.751	a. 0.753	a. 0.771	a. 0.764
	b. 0.715	b. 0.756	b. 0.742	b. 0.773	b. 0.779
	c.0.668	c.0.748	c.0.742	c.0.771	c.0.772
	d.0.724	d.0.756	d.0.793	d.0.773	d.0.800
Human Judgment	Relevant	Relevant	Relevant	Relevant	Similar
S_6	a. 0.647	a. 0.691	a. 0.690	a. 0.679	a. 0.668
	b. 0.711	b. 0.713	b. 0.685	b. 0.750	b. 0.675
	c. 0.564	c. 0.473	c. 0.641	c.0.537	c. 0.567
	d. 0.626	d. 0.506	d. 0.710	d.0.620	d. 0.596
Human Judgment	Irrelevant	Irrelevant	Relevant	Irrelevant	Irrelevant
S_7	a. 0.674	a. 0.707	a. 0.728	a. 0.729	a. 0.683
	b. 0.671	b. 0.730	b. 0.702	b. 0.735	b. 0.674
	c. 0.578	c. 0.572	c. 0.601	c.0.728	c. 0.615
	d. 0.601	d. 0.595	d. 0.630	d.0.739	d. 0.608
Human Judgment	Relevant	Irrelevant	Relevant	Relevant	Irrelevant

Table 2. Experiment results

Incidental Anaylsis: The similarity vales between C_1 and S_1 are consistent with both the human assessment and [2]. This is highly intuitive since both are business continuity management related concepts. S2 is also intuitively being the second best match to C_1 as security incident has direct implication to business continuity management.

A good example of syntactically similar but semantically different concepts is the mapping between C_2 and S_2. Although their titles both appear to be related to security incident management, they are in fact addressing different aspects of incident management. Interestingly, this finding was initially picked up by the similarity values between C_2 and S_2, and later learnt by human through manual investigations.

While for concept C_2, there is no particular ISO 17799 concept that is very similar to it, its similarity values against ISO 17799 concepts that are humanly assessed as relevant are generally higher than the irrelevant ones. The only exception is the similarity value between C_2 and S_3 for configuration a. This is corrected in configuration b. when weights of primitives are taken into account.

Subsections of S_3 in ISO 17799 (i.e. Section 4.1 and 4.2 of ISO 17799) frequently appear as supplementary materials to C_3 in [2]. This is consistent with the similarity values obtained for C_3 and S_3, i.e. S_3 is the best match to C_3. When only @objective is considered, S_5 is sensibly best matched to C_3. However, C_3 similarity values against the irrelevant concepts S_1, S_2 are generally mistakenly higher than other relevant concepts.

The similarity values of C_4 against ISO 17799 concepts are uniformly overrated. This phenomenon can be explained by the fact that C_4 emphasizes on formal IT management rather than on information security specific processes. As a result, C_4 is described with generic terms (e.g. management framework, support for business requirements). Our [31] instantiated S_p will assign high similarity values between the generic primitives and the ISO 17799's primitives. Nevertheless, the overall result for the row of C_4 is consistent with human assessment in that C_4 similarity values against relevant concepts are higher than against irrelevant concepts.

Row C_5 displays promising results as the most similar concept S_5 is computed against C_5 with highest similarity values for all configurations. Furthermore, C_5 similarity values against the relevant concept S_1 are higher than against the rest of irrelevant concepts (i.e. a. and c. display incorrect results that are then corrected in b. and d. when weights are considered).

Summary Analysis: Figures 5 through 9 present the graphs plotted for configurations a. and b. of each column in Table 2. The plot-graphs are constructed by plotting the human judgment of each cell in Table 1 against the similarity value between the column concept and row concept of the corresponding configuration settings. The plot-graphs should be interpreted in such a way that as the value increases along the x-axis of similarity, the value of human judgment along the y-axis should increase as well, i.e. a higher similarity value should intuitively be consistent with more positive human judgment. While the plot-graphs are prepared by assigning human judgment "similar" a numeric value of 1.5, "relevant" a numeric value of 1.0, and "irrelevant" a numeric value of 0.5, the graphs provide an approximated visualization of the correlation between human judgment and similarity value. As there is no absolute similarity, the similarity values and their correlation with human judgment within each column are different from another column.

The *solid line* in each graph indicates the educated guess on the ideal ***correlation*** *between human judgments and similarity values* for the particular column and configuration. The closer the plotted dots are to the correlation line, the better the similarity values are in reflecting human judgement.

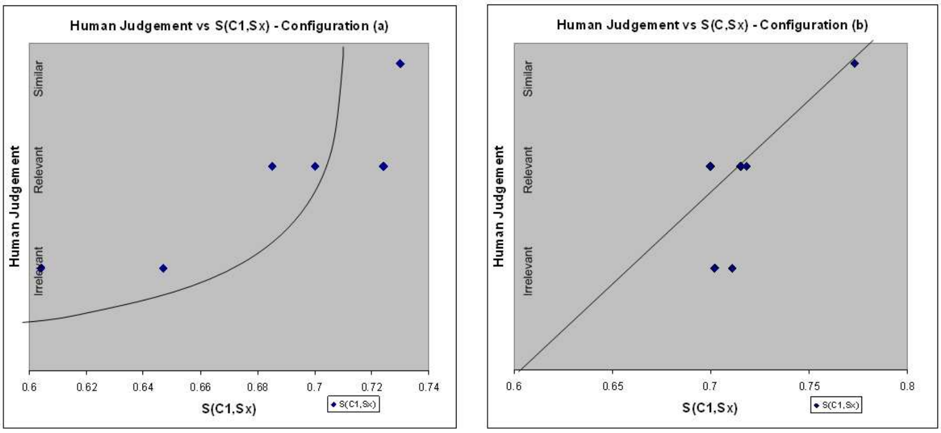

Fig. 5. Human judgement vs. $S(C_1, S_x)$: a) config a. (left), b) config. b. (right)

Figure 5 illustrates that the calculated similarity values for C_1 against the ISO 17799 concepts are generally clustered around the correlation line, with Figure 5 b) demonstrating better results than Figure 5 a). This indicates that the utilization of weights is associated with better similarity value correlation with human judgment.

Figure 6 illustrates a similar phenomenon as depicted in Figure 5. Figure 6 b) demonstrates better similarity value correlation with human judgment than Figure 6 a). This further reinforces the importance of weights to semantic similarity assessment.

Figure 7 illustrates non-ideal correlation between human judgment and similarity value. This phenomenon can be traced back to different limitations discussed below. Another potential cause to the non-ideal correlation might be the frequent appearance of “cliche” terms such as “security” and “system” in concept C_3. The terms dilute the accuracy of the modeled semantics of C_3.

Figure 8 a) illustrates good correlation between human judgment and similarity value. Although Figure 8 b) slightly disturbs the correlation, it demonstrates that weights are semantically useful in distinguishing the importance of different primitives i.e. the similarity values are more sensibly distributed and scattered apart.

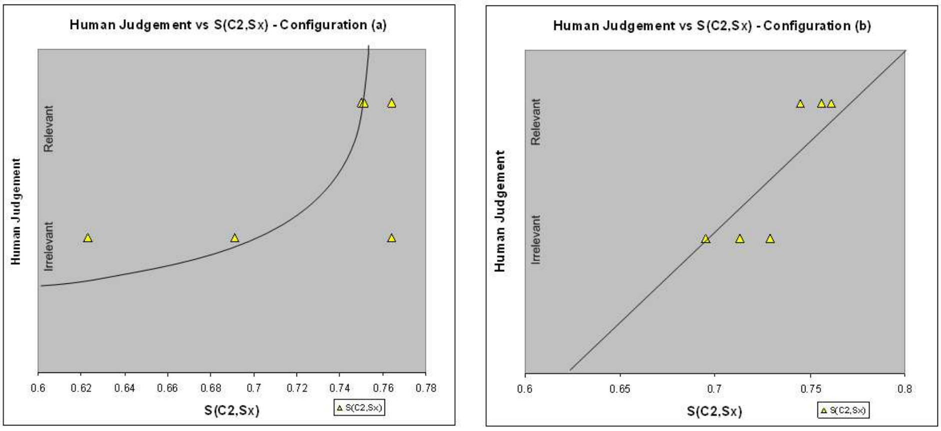

Fig. 6. Human judgement vs. $S(C_2, S_x)$: a) config a. (left), b) config. b. (right)

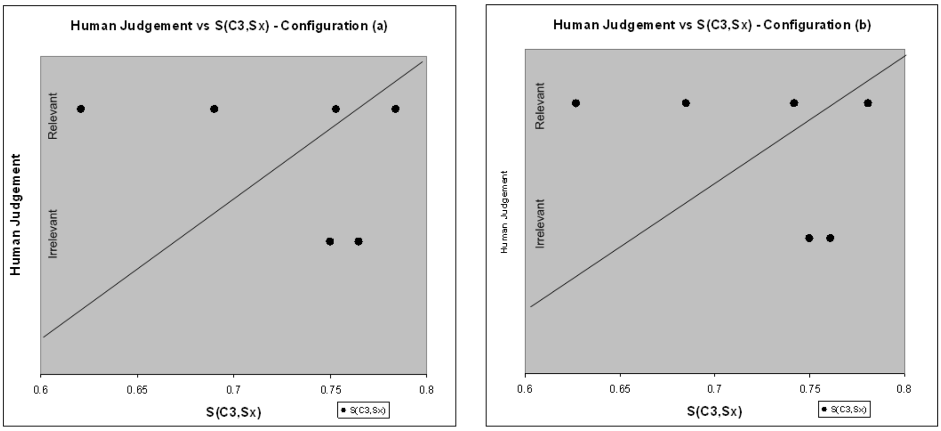

Fig. 7. Human judgement vs. $S(C_3, S_x)$: a) config a. (left), b) config. b. (right)

Figure 9 once again illustrates good correlation between human judgment and similarity value, especially with the utilization of weights as depicted in Figure 9 b).

Discussion: A lesson learnt from such experiments is that primitive weights are semantically important as indicated in different plot-graphs. They represent semantics of another dimension that primitives by themselves cannot express (as evident in the discussed occasions where the non-intuitive similarity values in a. and c. are corrected by the consideration of weights in b. and d. that better reflects the semantic importance of primitives).

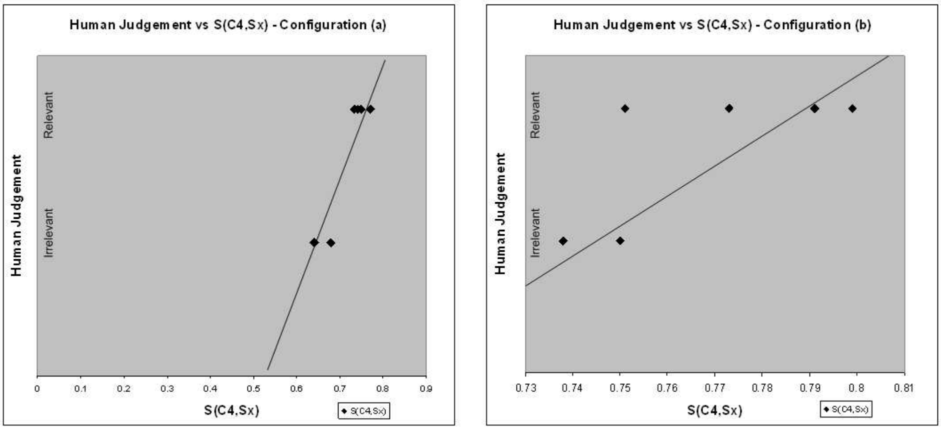

Fig. 8. Human judgement vs. $S(C_4, S_x)$: a) config a. (left), b) config. b. (right)

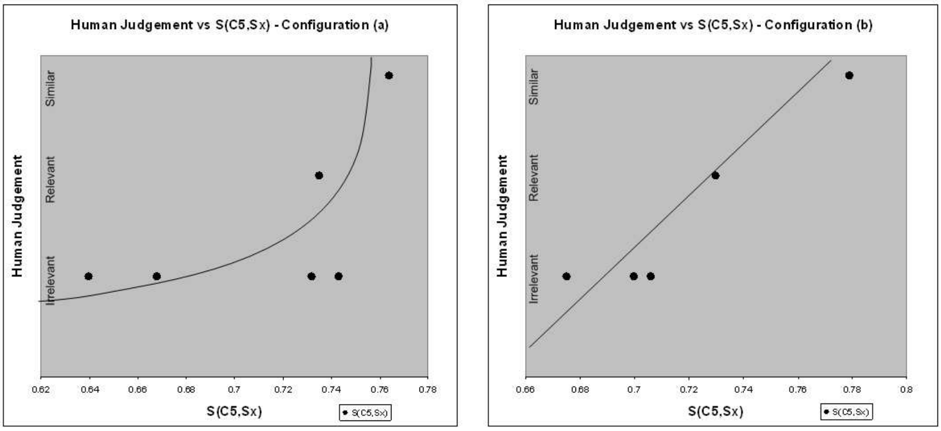

Fig. 9. Human judgement vs. $S(C_5, S_x)$: a) config a. (left), b) config. b. (right)

The results are promising, especially in cases where there is a highly similar target concept from a set of less-similar target concepts. This is evident in column C_1 and C_5 where the only "Similar" humanly assessed concepts S_1 and S_5 in the whole experiment are assigned with the highest similarity values. The outstanding results can also be observed in Figure 5 and Figure 9 as the highest top right dot. In other cases, where there is no outstanding target concept, our approach performs intuitively by assigning higher similarity values to the relevant target concepts than to the irrelevant concepts. This can be observed in Figures 5 through 9 as the rising y-value of the plotted dots as x-value increases (i.e. positive gradient).

However, there are also exceptions which can be traced back to the limitations of:

1. Primitive weight distribution – 1/frequency (primitive), weights are generated automatically for scalability and convenience reasons. Frequency is statistically useful, but semantically unreliable.
2. Instantiated S$_p$ – as [31] where words are not contextualized and situated specifically within the compliance domain. Therefore, similarities between primitives are only an approximate and best-effort guess.
3. Bottleneck at the ontology preparation phase:
    - Natural language processing remains an ongoing research problem, conversion from standards to ontology will inevitably suffer from the loss of semantic information.
    - Automatic ontology learning remains at its immature research stage, our semi-automatic approach that involves human interventions would unavoidably bias and inconsistently represent the intended semantics.

While the plot-graphs in Figures 5 through 9 illustrate overall intuitive correlation between human judgment and the computed similarity value, the correlation could be improved by more granularly assigning values to human judgments. Currently, Figures 5 through 9 plot human judgments as discrete values of 1.5 (a. k. a. Similar), 1.0 (a. k. a. Relevant) and 0.5 (a. k. a. Irrelevant). This coarsely approximates the actual correlation. The assignment of granular values such as 1.75 as "very similar", 1.25 as "minor similar" and so on will better approximate the correlation.

As part of our ongoing research, we are at our development stage in representing the similarity as a structure rather than simply a single numeric score. We argue basing on the lessons learnt from the experiments that similarity is biased and relative to different contexts, assumptions and interpretations. In order to support different applications, an objective presentation of the similarity values is necessary. While the numeric representation of similarity encapsulates many implicit assumptions and explicit assumptions such as weight distributions, a graphical representation, on one hand, supports intelligent processing of the mapping results for various intelligent IT governance applications, and on the other hand addresses the above limitations (especially 1. and 3. where weights and semantics can be biased and inconsistently misrepresented) by providing an objective illustration of the mapped and non-mapped components of the source and target concepts. Biased interpretations such as application of specific weights can then be applied individually for the particular application requirements. Figure 10 illustrates graphically the structure of the similarity between C_1 and S_7. The structure is massive due to the complexity of their FOL programs.

Figure 11 illustrates a cropped segment of Figure 10. The dashed links represent mapping links between modeling primitives of the source and target concepts, while solid links represent the relationships between the modeling primitives within their corresponding concept.

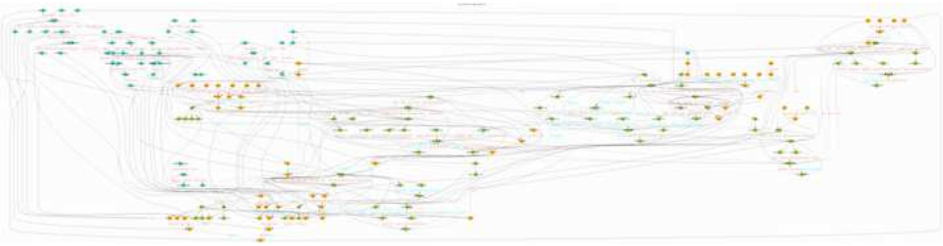

Fig. 10. Similarity structure for $S(C_1, S_7)$

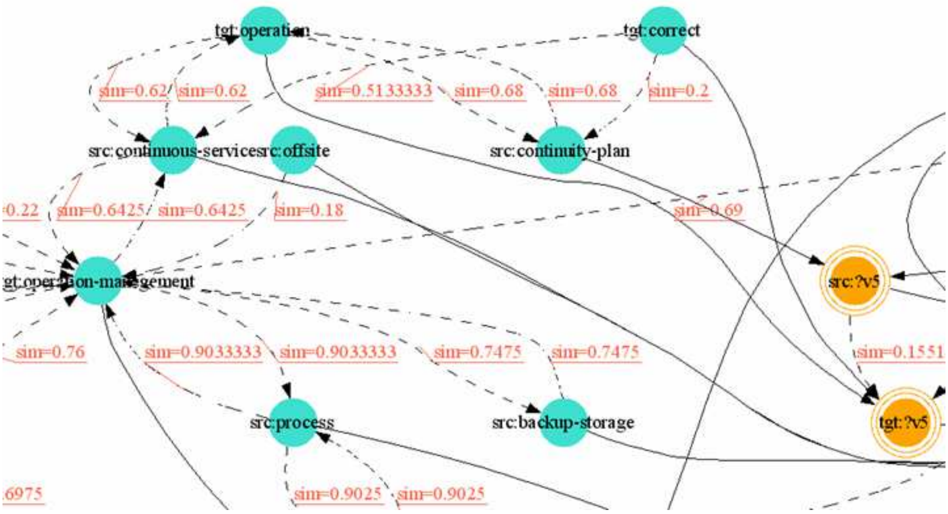

Fig. 11. Cropped & enlarged segment of Figure 10

8 RELATED WORK

The existing interoperability approaches to IT governance are mainly custom, point-to-point and manual efforts. Interoperability is restricted to specific standards. While the manual characteristics of the approaches hardcode the mappings for human consumption, the point-to-point characteristics limit the reusability of the underlying mapping techniques. [2] presents manual mappings only for high level objectives between Cobit, ITIL and ISO 17799, and [3] describes structural relevance between AS7799 and ISO 17799. There are other manual and community attempts in aligning between standards such as [4, 5, 6]. Undoubtedly, these works do not scale.

Our ontology-based approach dynamically adjusts the mappings when the ontologies evolve reflecting changes in the standards. The mappings are computed basing on formal ontology mapping techniques. Due to the mathematical nature and formal structure of the mapping technique, the mappings computed are machine-readable and machine-interpretable. Furthermore, the techniques for mapping can be generically applied across standards, without which N number of extra point-to-point mapping efforts would be required when a new standard is introduced to the existing pool of N number of standards. While there are many existing ontology mapping techniques [15], we have employed in this paper our noble technique that has been evaluated in other domains [16, 17]. An interoperability approach with comparable complexity to ours has also been presented in the legal domain [13].

Ontology mapping can be classified by different dimensional aspects such as autonomy (i.e. manual, semi-automatic or automatic), underlying technique (e.g. set, graph matching, machine-learning techniques), support for approximation (i.e. exact match only, or similarity supported), and grounding philosophy (i.e. semantic-based, statistics-based, syntactic-based, or hybrid). Our developed ontology mapping can be classified as automatic, logic-, similarity- and semantic-based approach. Given correct input, the similarity between ontological concepts is automatically computed without human intervention as opposed to methods such as PROMPT [22] that semi-automatically guides user in performing mapping, and MAFRA [23] that provides a framework for manually specifying mapping rules. We develop our approach around the technique of logical inference (i.e. SLD resolution and model theory) where formality and semantic expressiveness is maximally attained to facilitate machine-interpretation and intelligent reasoning. A logic-based approach allows comparison between concepts with more complex semantics than other techniques such as graph [26] and set based approach [25]. [24] describes a description logic based component for ontology mapping. However, it focuses mostly on the syntactic aspect of description logic (e.g. common “slots” implies similarity between two concepts), and only touches on limited semantic aspect of description logic (i.e. logical inference). [28] is another work that illustrates a logic-based approach, but it only supports exact-matching where concepts are either computed as equivalent or different. As ontology mapping is researched more actively in recent years, similarity-based approach becomes common and essential to facilitate many ontology-based tasks that require approximation in reasoning. Inheriting from our logic-based approach, our approach is semantic-based where comparison between concepts is based on the precisely modeled semantics. Such approach intuitively resembles human cognition during the process of object comparison where the meaning of objects (e.g. relations with other objects) is considered. Contrastively, syntactic-based (e.g. linguistic) approaches rely on controlled vocabularies (or symbols) for a restricted domain; statistics-based approaches (e.g. [27]) rely on large number of concept instances where mapping process can be conceptualized as assessment on concept similarity by examples. Depending on the requirements (e.g. complexity, instance availability, formalism), one approach might be more suitable than the others. There are also hybrid approaches that combine different methods, for example [24]. Furthermore, ontology and ontology mapping have been studied in the context of a distributed environment, e.g. Ontology Negotiation Protocol (ONP).

Example work would be [29]. [15] provides a survey on more ontology mapping approaches.

9 CONCLUSIONS

We have motivated in this paper the importance of the interoperability problem in the domain of IT governance. In this paper an ontology-based interoperability approach is presented that facilitates the applications of standards translation and integration in IT governance. The approach relies on an ontology mapping algorithm that bridges the semantic differences between ontologies of different standards.

The presented experiments display results that are cognitively intuitive. Overall consistent correlation is also illustrated between human judgment and similarity value. While the numeric representation of the similarity values encapsulates many implicit and explicit assumptions and biases, the assumptions and biases chosen for similarity assessment directly affect the intuitiveness of the similarity results.

This research lays the foundation for our ongoing research on automatic and intelligent IT governance. In particular, it adds value to the currently growing and significant domain of IT governance.

Acknowledgement

The work reported in this paper was partially supported by the ARC Discovery Grant 2007.

REFERENCES

[1] ITGI: Board Briefing on IT Governance. ISBN 1-893209-27-X, 2001.

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

[3] Pollard, M.: Developing an AS7799 and ISO 17799 Compliant Information Security Management System. Available on: `http://www.bridgepoint.com.au/Documents/7799paper.pdf`, 2005.

[4] ISACA: COBIT Mapping: Mapping of PRINCE2 With COBIT4.0. Available on: `http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/COBIT_Mapping1/COBIT_Mapping.htm`, January 2007.

[5] ISACA: COBIT Mapping: Mapping of RMBOK to COBIT4.0. Available on: `http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/COBIT_Mapping1/COBIT_Mapping.htm`, August 2006.

[6] ISACA: COBIT Mapping: Mapping of SEI's CMM for COBIT4.0. Available on: `http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/COBIT_Mapping1/COBIT_Mapping.htm`, Aug, 2006.

[7] SEC: Sarbanes Oxley Act 200. US Securities Exchanges Commission.

[8] US Depart of Health and Human Services: Health Insurance Portability and Accountability Act (HIPPA), 1996.

[9] International Organization for Standardization: ISO 17799:2005. Available on: `http://www.iso.org`, Last Accessed: October 31, 2006.

[10] IT Governance Institute: Control Objectives for Information and Related Technologies (CobiT). 2005.

[11] Bundesamt fr Sicherheit in der Informationstechnik (BSI): IT Baseline Protection Manual – Standard Security Safeguards. Available on: `http://www.bsi.bund.de`, 2001.

[12] Spears, J.—Barton, R.—Hery, W.: An Analysis of How ISO 17799 and SSE-CMM Relate to the S-vector Methodology. 2004.

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

[14] Gruber, T.: Towards Principles for the Design of Ontologies Used for Knowledge Sharing. Padua Workshop on Formal Ontology, March, 1993.

[15] Kalfoglou, Y.—Schorlemmer, M.: Ontology Mapping: The State of the Art. The Knowledge Engineering Review, Vol. 18, 2003, No. 1, pp. 1–13.

[16] Wong, A. K. Y.—Ray, P.—Paramesh, N.—Strassner, J.: Ontology Mapping for the Interoperability Problem in Network Management. IEEE Journal on Selected Areas in Communications (JSAC), Vol. 23, 2005, No. 10, pp. 2050–2058.

[17] Wong, A. K. Y.—Paramesh, N.—Ray, P.: Towards an Ontology Mapping Approach for Security Management (IJAIT). Vol. 15, 2006, No. 6, pp. 1071–1090.

[18] Yip, F.—Wong, A. K. Y.—Ray, P.—Paramesh, N.: Corporate Security Compliance in a Heterogeneous Environment. Short paper, Poster Session 2, NOMS, 2006.

[19] Wong, A. K. Y.—Paramesh, N.—Ray, P.: Similarity and Logic Based Ontology Mapping for Security Management. Proceedings of the 18th Florida Artificial Intelligence Research Society (FLAIRS) Conference, 2005, pp. 653–659.

[20] Wong, A. K. Y.—Paramesh, N.—Ray, P.: Towards an Ontology-Driven Approach for the Interoperability Problem in Security Compliance. 19th International FLAIRS Conference, Florida, USA, May 2006.

[21] Wong, A. K. Y.—Yip, F.—Ray, P.—Paramesh, N.: Semantic Data Integration for IT Governance. International Workshop on Semantic e-Science, Beijing, September 2006.

[22] Noy, N. F.—Musen, M. A.: The PROMPT Suite: Interactive Tools for Ontology Merging and Mapping. International Journal of Human-Computer Studies, Vol. 59, 2003, No. 6, pp. 983–1024.

[23] Maedche, A.—Motik, N. S.—Volz, R.: MAFRA – A Mapping Framework for Distributed Ontologies. Proceedings of the 13th European Conference on Knowledge Engineering and Knowledge Management (EKAW), Vol. 2473, 2000, pp. 235–250.

[24] Ehrig, M.—Sure, Y.: Ontology Mapping – An Integrated Approach. Proceedings of the 1st European Semantic Web Symposium (ESWS), Heraklion, Greece, May, Vol. 3053, 2004, pp. 76–91.

[25] Rodriguez, M. A.—Egenhofer, M. J.: Determining Semantic Similarity among Entity Classes from Different Ontologies, Knowledge and Data Engineering. IEEE Transactions, Vol. 15, 2003, No. 2, pp. 442–456.

[26] Culmone, R.—Rossi, G.—Merelli, E.: An Ontology Similarity Algorithm for BioAgent. NETTAB Workshop on Agents and Bioinformatics, Bologna, 2002.

[27] Doan, A.—Madhavan, P. D.—Halevy, A.: Learning to Map Between Ontologies on the Semantic Web. Proceedings of the 11th International Conference on the World Wide Web, 2002, pp. 662–673.

[28] Kalfoglou, Y.—Schorlemmer, M.: IF-Map: An Ontology Mapping Method Based on Information Flow Theory. Journal on Data Semantics, LNCS 2800, 2003, pp. 98–127.

[29] Gonzalez, E. J.—Hamilton, A. F.—Moreno, L.—Marichal, R. L.—Toledo, J.: Ontologies in a Multi-Agent System for Automated Scheduling. Computing And Informatics, Vol. 23, 2004, No. 2.

[30] Schmid, H.: Probabilistic Part-of-Speech Tagging Using Decision Trees. International Conference on New Methods in Language Processing, Manchester, UK, 1994.

[31] Dao, T. N.—Simpson, T.: Measuring Similarity between Sentences. Available on: `http://opensvn.csie.org/WordNetDotNet/trunk/Projects/Thanh/Paper/WordNetDotNet_Semantic_Similarity.pdf`.

[32] Brachman, R. J.—Levesque, H. J.: Knowledge Representation And Reasoning. Morgan Kaufmann, ISBN-1558609326, 2004.

[33] Computer Security Institute: CSI/FBI Computer Crime and Security Survey. 2005.

Alfred Wong is a Ph. D. candidate in the Computer Science department at the University of New South Wales. He earned his first-class honours Bachelor degree in software engineering from the University of New South Wales in 2004. His research activities began when he was completing his scholarship-based honours thesis with CMCRC in 2003. His research interests include ontology construction, ontology mapping, network management, and in particular, security management. In 2006, he participated in winning the ARC Discovery Grant 2007.

Frederick Yip is a Ph. D. candidate in the University of New South Wales. He graduated from University of New South Wales as a first-class honours graduate in software engineering in 2005. His current research interests are in IT governance, compliance management, ontology construction, ontology modularization and the semantic web.

Pradeep Ray is a senior member of the academic staff in the School of Information Systems, Technology and Management at the University of New South Wales. His research interests include the cooperative management of enterprise networks and services in various business areas, such as healthcare and telecommunications. He has more than ninety publications including two research books. He has been the Symposium Chair of IEEE Globecom 2004 Symposium on Security and Network Management, Globecom 2002 Symposium on Service Infrastructure for Virtual Enterprises (SIVE). He was the co-editor of the International Journal of Network and Systems Management Special Issue on E-Business Management in March 2003. He has been the Chair of the IEEE Technical Committee on Enterprise Networking (EntNet) that launched the flagship IEEE annual international event called the International Conference on Enterprise Networks, Applications and Services in 2001. He is the founder and the Advisory Committee Chair of IEEE Healthcom, an annual event that brings together IT and Health/medical sciences professionals and researchers in different parts of the world.

Nandan Paramesh is a senior lecuturer in School of Computer Science and Engineering, University of New South Wales, Sydney, Australia. He carries out research in the areas related to agent technology and applications in problem solving in dynamic situations. He is currently involved in the design and implementation of dialog based agents in enterprise applications.