CrossMark

Compliance management ontology – a shared conceptualization for research and practice in compliance management

Norris Syed Abdullah[1] · Marta Indulska[2] · Shazia Sadiq[3]

Abstract The diversity of stakeholders in compliance management initiatives contributes to the challenges organisations face when managing compliance, and consequently adds to the cost of compliance. In particular, there is evidence that the lack of a common or shared understanding of compliance management concepts is a barrier to effective compliance management practice. Taking an information-centric view to addressing this challenge, this paper reports on the development of an ontology intended to provide a shared conceptualisation of the compliance management domain for various stakeholders. The ontology is based on input from domain experts and practitioners, validated and refined through eight case studies, and subsequently evaluated for its usability in practice.

Keywords Domain ontology · Compliance management · Compliance vocabulary · Semiotics

1 Introduction

Compliance refers to ensuring that business processes, operations, and practice are in accordance with a prescribed and/or agreed set of norms (Sadiq et al. 2007). Compliance requirements are typically associated with regulations that may be introduced externally or internally for an organisation itself. However, compliance requirements may stem from a variety of sources, including legislature and regulatory bodies (e.g. Sarbanes-Oxley, Basel II, HIPAA), standards and codes of practice (e.g. SCOR, ISO9000), organisational policies and business partner contracts (Sadiq et al. 2007). Indeed, at a minimum, enterprise compliance and risk management includes financial reporting compliance (e.g. Sarbanes-Oxley compliance), and support for other types of compliance, such as ISO 9000, PCI (i.e. payment card industry), industry-specific regulations, service-level agreements, trading partner requirements and compliance with internal policies (Caldwell 2008). To provide an appreciation of the scope of compliance requirements, various sources are listed in Table 1 along with some related examples.

The obligations to meet compliance requirements span across many, if not all, industry sectors and applications, such as financial services, environment, healthcare, and manufacturing (Syed Abdullah et al. 2009; Hoffmann et al. 2012), to name a few. These obligations are predominantly viewed as a burden by organisations (Lu et al. 2008), however, failing to comply is no longer an option (Pershkow 2003; Anon et al. 2007). Breaches of compliance may result in serious and sometimes disastrous consequences for the organisations and individuals concerned. A number of high profile corporate scandals - Enron, WorldCom (USA), Parmalat (Italy), HIH (Australia), and Tyco International (France), to name a few - were associated with significant market and reputational damage (Syed Abdullah et al. 2009). The negative publicity around such incidents further motivates organisations to ensure compliance to requirements. A key feature of these requirements, however, is that they are often non-prescriptive in nature and require interpretation in the

✉ Norris Syed Abdullah
  norris@utm.my

1 Faculty of Computing, Universiti Teknologi Malaysia, 81310 Johor Bahru, Johor, Malaysia

2 UQ Business School, University of Queensland, QLD 4072, Australia

3 School of Information Technology & Electrical Engineering, University of Queensland, QLD 4072, Australia

Springer

organisational context and considering the organisational vocabulary. Thus the mapping of the requirements to actual practices within organisations is a subjective process, and is often driven by organisational culture and risk appetite.

Several frameworks (Lahti et al. 2005; Gupta 2008) have emerged that provide guidelines to organisations on how to plan and implement compliance regimens. However, organisations still struggle to measure the adequacy of their compliance efforts (Deloitte 2013). The inter-disciplinary nature of the domain of compliance management holds both the cause as well as the solution to addressing the problems associated with effective compliance management. Earlier studies (Syed Abdullah et al. 2010b; Esteban 2009) observed that a disconnect between various functions of an organisation is an area of concern within the compliance management practitioner community. This disconnect is attributable to the diversity of stakeholders in the compliance management domain, and partially stems from the lack of common vocabulary with which to communicate compliance management concepts to different stakeholders within and outside of an organisation (Syed Abdullah et al. 2010b; Clayton Utz 2013; Esteban 2009; Protiviti 2013). At the same time, analysis of research literature reveals a diversified interpretation and presentation of core concepts in the domain, leading to a lack of shared understanding and an unclear impact of the contributions (Syed Abdullah et al. 2010b; Boella et al. 2013; Butler and McGovern 2012). Due to this lack of common ground, synergies within and between research and practitioner communities in compliance management remain largely unexploited.

To address this gap in the body of knowledge, we take an information-centric view to compliance management and posit that any effort towards providing holistic compliance management solutions demands a common understanding of compliance management concepts among the different stakeholders. Accordingly, in this paper, we develop a shared conceptualisation of the compliance management landscape in the form of a Compliance Management Ontology – named CoMOn. To do so, we turn to ontology – a branch of philosophy concerned with the nature of reality (Wand and Weber 1995). Specifically, in our work we aim to develop a domain ontology. Domain ontologies have been used in various fields to capture relevant domain knowledge and describe the vocabulary relevant to that domain. For example, in biology, ontologies have been used as vocabularies and classification of genes (Horrocks and Patel-Schneider 2011). More broadly, in business, domain ontologies have been used to provide a shared understanding of terms important to describing the domain (for example, to model knowledge required to configure products – see Yang et al. (2009)). In a similar way, we aim for CoMOn to be an ontology of relevant concepts that can facilitate a shared understanding of compliance management within any organization.

To ensure industry relevance, CoMOn is derived from interviews and surveys of compliance management experts and practitioners. The ontology is developed following the ENTERPRISE ontology building methodology (Uschold and King 1995; Uschold 1996) and validated using a case study approach that incorporates a semiotic framework proposed for ontology quality evaluation (Burton-Jones et al. 2005). Eight case studies are used to conduct the quality evaluation and subsequently refine the ontology with compliance management experts, before a final usability evaluation with six Australian organisations from the public and private industry sector.

The remainder of the paper is structured as follows. In section 2 we provide a brief analysis of related work on

Table 1 Compliance Requirements

Sources of Compliance Requirements	Examples
Regulation	SOX: Sarbanes-Oxley Act of 2002 (Coates 2007) GLB: Gramm-Leach-Bliley Act of 1999 (Cuaresma 2002) CAN-SPAM: Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (Grimes 2007) AML/CTF: Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cozens 2009) New Zealand Privacy Act 1993 (Mount 1993) EUDPD: European Union Data Protection Directive 1995 (McCorkell 1998) FCRA: Fair Credit Reporting Act 1970 (Pacini and Barker 2010) CFIP: Code of Fair Information Practice (Schwaig et al. 2006) HIPAA: Health Insurance Portability and Accountability Act of 1996 (Frimpong and Rivers 2006) EMAS (Eco-Management Audit Scheme) (Wenk 2005)
Standard	ISO 31000:2009 Risk Management - Principles and Guidelines (EMC 2010) AS/NZS 17799:2001 - Australia's Standard for Information Security Management (Smith et al. 2006) AEC: American Election Committee Voting System Standards (Williams and King 2004) PCI Data Security Standard (Bonner et al. 2011)
Policy	Security Policy (Hu et al. 2011) Privacy Policy (Mont and Thyne 2008) Electronic Record Management Policy (Volonino 2003)
Contract	SLA: Service Level Agreement (Hasan and Stiller 2007) Trading Partner Requirements (Deloitte 2013) Contract Terms (Tan and Thoen 2000)

compliance management from an Information Systems perspective. The review aims to highlight the diversity of contributions and confirm the lack of a common vocabulary within the compliance management domain. In section 3 we discuss the methodology utilized to develop the shared conceptualization, namely the compliance management ontology - CoMOn, which is adapted from the ENTERPRISE ontology development methodology and extended to accommodate multiple sources of input as well as usability evaluation. The section also outlines the approach used to validate and refine the ontology, as well as the approach used to evaluate the usability of the refined ontology in an organisational setting. Section 4 presents the validated, refined, ontology and introduces the key concepts. In section 5 we outline the results of the usability evaluation. We conclude the paper in section 6 with a summary of the paper's contributions, a discussion of potential impact of the ontology, as well as an outline of planned future research.

2 Related work

Compliance management is generally positioned within the broader Governance, Risk and Compliance (GRC) function of organizations. GRC is of increasing importance to organizations worldwide (Deloitte 2013) due to the negative implications of non-compliance - for example, reduced market confidence, reduced investor confidence, and reduced business performance (KPMG 2005b). GRC frameworks in general, and compliance management specifically, are, by necessity, multi-disciplinary, spanning legal/legislative, health and safety, management, social, behavioural and technological aspects. Whereas all aspects are important, our review of literature was conducted with the aim of understanding contributions to compliance management from an information centric perspective. Thus, we were interested in understanding the role and impact that the Information Systems community has in compliance management.

Over the past decade, compliance management has received relatively scarce yet increasing attention from the academic Information Systems community (Syed Abdullah et al. 2009). The increasing focus is not surprising given that a high percentage of solutions for compliance management are likely to be technology supported. To better understand the landscape of research in this domain, we conducted a literature review of articles that address relevant compliance management topics. In the following, we describe the literature review process and explain how its outcomes evidence the need for a compliance management ontology.

The literature review explores the content of all articles published in premium Information Systems journals (as promoted by the Association for Information Systems), reputed Information Systems conferences, and some additional popular journals in the discipline,[1] between 2001 and 2011 - a total of 27,640 articles. Each article was prepared and included in a full text search for the purposes of identifying contributions relevant to the compliance management domain. Full text searches were conducted on the data set, using a keyword of "compliance", "compliant", and "conformance". Articles that included three or more instances of the target keywords were considered to be of relevance to the review. This step reduced the set of relevant articles to 1151. With the reduced set of articles, a review of each article was carried out. This review included reading the abstract, introduction, and scanning through the main contributions of the remainder of the article as well as its conclusions. Despite the articles having more than three references to the selected keywords, many were found to not present a contribution to the domain of compliance management (e.g. technical papers considering compliance to a network protocol). Accordingly, the analysis reduced the set of articles from 1151 to 537.

The literature review indicated the presence of two themes of research, namely (i) exploratory articles and (ii) articles that provide specific solutions to a compliance management problem. The exploratory articles typically present empirical inquiry investigating contemporary phenomenon in depth and within their real life context (Yin 2009) or articles that contained studies undertaken to better comprehend the nature of the problem (Sekaran and Bougie 2010). The solution articles offer methods, frameworks, techniques or tools to solve compliance management issues. As is expected in an emerging research domain, the majority of the publications were found to be exploratory in nature – 413 (77 %) of the articles were exploratory articles and 110 (20 %) were solution oriented. The review suggests that research offering compliance management solutions has been initiated but remains still in the early exploratory stages, not yet progressing to a stage where many Information Systems based solutions are proposed or discussed, despite the information centric nature of compliance management problems (Kim et al. 2007; Berente et al. 2010). Figure 1 presents the breakdown of the articles by year and type of contribution, showing an increasing interest in the topic. Tellingly, however, our review of the solution papers in particular revealed the diverse and inconsistent nature of the terminology used to describe the compliance problem, solution and the compliance management domain as a whole. For example, discrepancies were discovered in referring to compliance frameworks vs. regulations in a number of articles (Ghanavati et al. 2007; H. A. Smith and McKeen 2006). In Ghanavati et al. (2007), the authors state "… framework we introduce here demonstrates how compliance can be tracked by defining and managing external

---

[1] Conference venues: ACIS, AMCIS, BPM, CAiSE, ECIS, ER, HICSS, ICIS and PACIS.
    Journal venues: BPMJ, CACM, CAIS, EJIS, I&M, IS, ISF, ISJ, ISR, JAIS, JIS, JMIS, and MISQ.

links between two models: a model of the health information custodian's policies and business processes in terms of GRL and UCM notations, and a model of privacy legislation in terms of GRL notation" and imply that a "compliance framework" is a solution or method to manage compliance. In H. A. Smith and McKeen (2006), however, the authors "explore how new compliance frameworks and governance reforms, mandated by governments and/or industry groups, are changing IT work." and imply that "compliance framework" is a form of a regulatory mandate or reason for the need to manage compliance. Such observations of inconsistent understandings of key compliance management concepts in research are also confirmed in practice through the study with compliance management experts and practitioners (Syed Abdullah et al. 2010a).

Accordingly, researchers have argued that the benefit of any proposed solution is unlikely to be realised in full without a shared conceptualisation of the compliance management domain (Syed Abdullah et al. 2010a). Shared conceptualisations are widely used to facilitate understanding in many domains e.g. environment, software engineering, and healthcare – to name a few. Earlier research also highlighted that shared conceptualisation for a particular domain is typically being presented in domain ontology form (Buttigieg et al. 2013; Mellouli et al. 2010; WenJun et al. 2009; Zeshan and Mohamad 2012). Hence, the development of such a conceptualisation is posited to be central to improving compliance management practice, where efforts are hampered by the lack of consistent communication of compliance management concepts between stakeholders. A shared model of compliance management concepts will also provide a foundation on which industry-relevant compliance management research and solutions can be developed, and is hence an important stepping stone towards advancing the compliance management body of knowledge. Despite the need for such a shared model of concepts, however, our review of compliance management literature across all domains indicates that, at the time of writing, such a conceptualisation does not exist.

Accordingly, in this paper we address this gap and develop a conceptualisation of the compliance management domain.

To undertake the conceptualisation of the compliance management domain, we turned to the branch of philosophy known as ontology. Ontology is a subset within the philosophy domain, which specifically deals with models of reality. It is a well-established field of research, the utility of which has been shown in a variety of real-world applications (M Grüninger and Lee 2002). In addition to its use in domain specific research, e.g. gene ontology (B. Smith et al. 2003) and mass gathering ontology ((Haghighi et al. 2013), ontology has been extensively used in the Information Systems domain to aid the evaluation and development of conceptual models e.g. (Weber 1997; Recker et al. 2005; Shanks et al. 2008; Opdahl and Henderson-Sellers 2002). The underlying argumentation stems from the understanding that ontology specifies a finite set of defined ontological constructs to describe real-world phenomena within a domain. Accordingly, it provides an excellent foundation on which the expressiveness of a conceptual model (notation) can be evaluated. In a similar manner, ontology can be useful for knowledge management purposes, where a set of common constructs is required for classification (McCorkell 1998). To develop such a set of common constructs for the compliance management domain, capable to facilitate a shared understanding within the stakeholders of the domain, is the central goal of this work and resulted in the development of an ontology for compliance management – CoMOn.

3 Ontology development

Our study is guided by the over-arching Design Science paradigm (Hevner et al. 2004) given our focus on the development and evaluation of an artefact – an ontology. Ontology development is a difficult and time-consuming process (Gruber 2009; Syed Abdullah et al. 2011), one that requires a structured approach. A review of methods and techniques for ontology development indicates that several methodologies are available - these include Cyc (Knight and Luk 1994), TOVE (M. Grüninger and Fox 1995), ENTERPRISE (Uschold and King

Fig. 1 Distribution of compliance management related articles per type per year
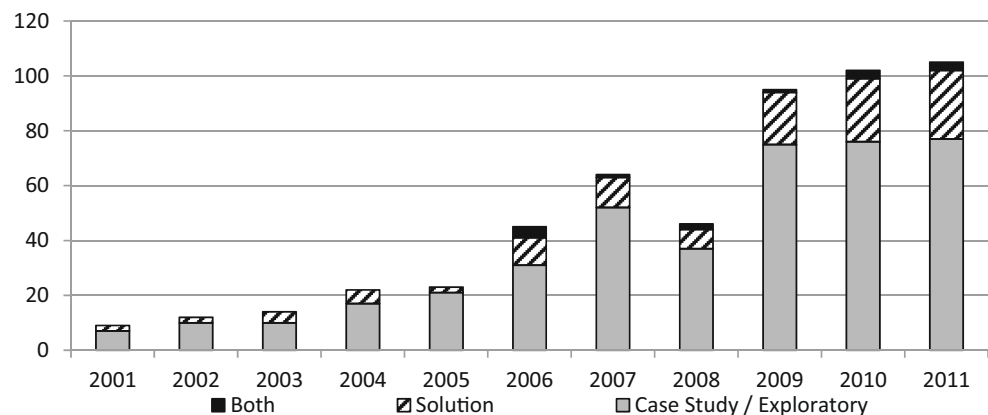
1995; Uschold 1996), METHONTOLOGY (Fernández et al. 1997), ontology integration methodology (Pinto and Martins 2001), OntoClean (Guarino and Welty 2009), and semantic interoperability methodology (Paredes-Moreno et al. 2010), to name a few. These methodologies mainly include the same high-level steps of specification, conceptualization, formalization, knowledge acquisition, and evaluation, with differences in the amount of detail in each step (for a comparison of methodologies please see Gómez-Pérez et al. (2004)). To guide the development of CoMOn, we selected the ENTERPRISE methodology (Uschold and King 1995; Uschold 1996). Our selection of the methodology was based on four main arguments. First, ENTERPRISE provides a good balance between development guidance and freedom of representation of the domain. This trade-off offered by the ENTERPRISE methodology affords a clear direction on the development front, while allowing the selection of the most appropriate representation (Pinto and Martins 2004). Second, ENTERPRISE provides a stage based approach that is well suited to the development of ontology that has a clear purpose and requirements (Jones et al. 1998), as is the case of CoMOn. Third, ENTERPRISE is a well-accepted methodology. It is one of the most popular ontology development methodologies (based on Citations), and has been established as one of the most widely used ontology development methodologies in the ontology engineering field (Fensel 2001; Fernández-López and Gómez-Pérez 2002; Gómez-Pérez et al. 2004; Noy and McGuinness 2001). ENTERPRISE has also been widely utilised as a credible approach for ontology development (Paredes-Moreno et al. 2010; Lim et al. 2011). In fact, it has influenced many other methods or approaches in ontology community (Sure et al. 2009). Forth, and finally, in our review of existing methodologies, we noted that while many methodologies were similar (Corcho et al. 2003), they lacked guidance for how to identify, gather, and use input to identify ontology concepts, as well as comprehensively evaluate the ontology. Therefore, in our work we selected an authoritative methodology and chose to extend it with guidance for use of input as well as empirical evaluation. Accordingly, we incorporated a rigorous coding process that includes a variety of sources of input. One of the few existing research contributions addressing concept identification guidance is that of Velardi et al. (2001), who describe a text mining technique that aids an ontology engineer in identifying the important concepts in a domain ontology. Similarly, Brusa et al. (2006) discuss their experience in developing a government budgetary ontology based on inputs from the provincial budgetary application, its related documentations, and a group of experts within an organisation. However, while both contributions utilize inputs from a particular domain, they do not provide sufficient detail on how the concepts should be identified, captured and coded. In contrast, these aspects are considered in detail in our extended methodology, thus also providing guidance for other developers in the future. Second, we

extended ENTERPRISE to include a rigorous validation step, incorporating an existing semiotics framework as a foundation for refinement of the ontology to ensure a higher quality outcome, which is then followed by ontology evaluation through a usability study with practitioners. Fig. 2 outlines the overall approach utilized in our study, which is described in detail in the following sub-sections.

3.1 Identify purpose and scope

Identifying the purpose and scope of an ontology is critical to ensure a clear understanding of its intended use(s) and users (Uschold and King 1995). In our study, the literature review as presented in section 2, identified the need and consequently the purpose of CoMOn, that is to provide practitioners, as well as the research community, with a shared conceptualisation of constructs in the compliance management domain. In terms of the users, we note that the most likely users of this ontology are compliance management professionals, regulators, and researchers, with the intended use being a reference for describing, documenting, communicating, and implementing compliance related tasks.

3.2 Ontology building

The building of CoMOn is based on a synthesis of interviews with senior compliance management experts (Syed Abdullah et al. 2010a), open-ended surveys with compliance management practitioners (Syed Abdullah et al. 2010b), as well as industry reports. We selected these three sources to ensure good representation of compliance management practice, and use them as a basis for the development of a well-informed and industry-relevant ontology, thus minimising the risk of missing ontological concepts. The qualitative data was gathered through semi-structured interviews with eleven Australian compliance management experts (Table 2 shows the demographics of the participants). To identify senior and well-reputed compliance management experts, who have insight into both the mature and immature stages of compliance management in organisations, we enlisted the help of the Australasian Compliance Institute (ACI).[2] Eleven participants were invited to participate - all eleven agreed with no incentives for participation. Typical roles of the involved experts were those of senior compliance management advisors and consultants in large organizations that provide both advisory and auditing services in the context of regulatory compliance. Among the eleven participants, nine have over 10 years of

---

[2] The Australasian Compliance Institute (ACI) is the premier member organization for compliance and risk professionals across the Asia Pacific region. ACI connects its members with continuing education, accreditation, publications, networking and advocacy, and is devoted to supporting the profession by increasing its awareness within the Asia Pacific community. ACI website: www.compliance.org.au.

Fig. 2 Methodology for ontology development
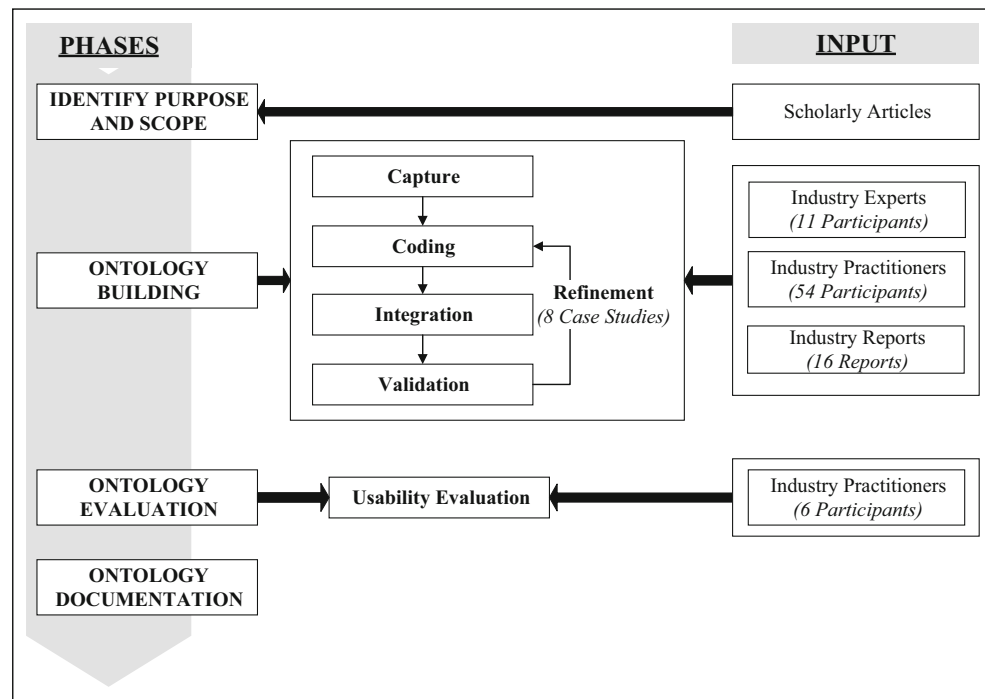
experience in the field, with the others having five and seven years of experience, respectively, providing the study with a good representation of roles in practice.

In addition to the above eleven interviews with experts, we also utilised data collected from practitioners using an open-ended survey protocol. The data was collected from compliance management practitioners during an ACI education seminar the practitioners attend as part of their ACI accreditation. The demographics of the participants are summarised in Table 3, with their experience ranging from one to over 30 years, in a wide variety of roles that well reflect compliance management structures in organisations. Overall, 54 practitioner responses were collected.

Table 2 Compliance Management Experts - Demographics

Participant's no.	Field/ background	Roles	Years of experience
1	Legal	General manager	10–19
2	Finance	Director	10–19
3	Finance	Consultant	30+
4	Compliance	Consultant	10–19
5	Legal	Director	10–19
6	Compliance	Head of compliance	20–29
7	Compliance	Branch manager	10–19
8	Compliance	Head of compliance	5–9
9	Finance	Consultant	30+
10	Electronic engineer	Director	30+
11	Sales & marketing	Senior manager	5–9

Our two data sets, consisting of expert interviews and practitioner survey responses, were complemented with a set of relevant industry reports. Table 4 summarises the list of industry reports that were included in the study. While the experts and practitioners were based in Australia, incorporating relevant industry reports allowed us to ensure that the concepts and concept naming was internationally accepted rather than following regional customs.

With the identified set of three main inputs we embarked on the three core steps of the ontology building phase prescribed by the ENTERPRISE methodology (Uschold and King 1995; Uschold 1996) - viz. capturing, coding and integrating existing ontologies, with an addition of a 4th ontology validation step prior to the next phase of ontology evaluation. We discuss the four steps below.

Capture Ontology capture includes identifying key concepts and relationships in the domain, producing precise and unambiguous text definitions for such concepts and identifying terms to refer to such concepts (Uschold and King 1995). To facilitate this step, we used the three sources described earlier – i.e. compliance management experts, practitioners, and industry reports, as the basis for CoMOn concept identification through iterative coding and analysis of the relevant data. The coding and analysis were facilitated by a tool typically used for analysis of large bodies of text - NVivo.[3] NVivo was used to code the concepts and relationships that make up the

---

[3] A qualitative data analysis software package that is used to code and analyse qualitative data gathered from surveys, interviews, observations, document analysis, or other text-based data. www.qsrinternational.com.

Table 3 Compliance management practitioners - demographics

Roles	Average years of experience	Number of participants
Regulator	14	3
Consultant	13	10
Compliance officer	6	15
	Undisclosed	2
Compliance manager	6	14
Head of compliance	18	2
Undisclosed/Other roles	8	4
	Undisclosed	4
TOTAL		54

ontology, while maintaining a link between each coded concept and its underlying data. The coding process started with loading of all interview transcripts, open ended survey answers and industry reports into NVivo. One researcher coded a fragment of the data sources when it represented a concept related to compliance management. A node was created in NVivo to represent a group of fragments from the data sources that were relevant to a particular concept – the node structure, therefore, evolved out of the coding process. This process continued through three iterations until all data was coded, which resulted in 254 initial concept nodes. In addition to the initial coder, two other researchers coded the data as a single team, using the node structure developed by the first coder, thus resulting in a dual-coder approach. We calculated the reliability of our coding process by using Cohen's Kappa - an index commonly used to measure the level of agreement between two sets of dichotomous ratings (Cohen 1960; Viera and Garrett 2005; Wood 2007). Our Cohen's Kappa value of 0.743 exceeds the threshold required for research work (at least 0.60 or 0.70 (Wood 2007)), nevertheless the single coder and the team coders met in several meetings to revise the coding and reach 100 % agreement.

After the capture of the 254 concept nodes, concept identification was followed by a review process with the view to remove redundancy of nodes, and thus concepts represented by the nodes. Where synonyms were found, one of the synonyms was selected based on its frequency of use in the data, or a new, more representative term was defined for the concept. This process resulted in a duplicate free and broader set of concepts, reducing the number of concepts from 254 to 64 – which became the constructs of the first version of CoMOn. After another round of coding to ensure that the 64 constructs are good representations of the coded fragments, the constructs were clustered thematically. This clustering resulted in 10 most prominent (or core) generalized ontological constructs. Based on this clustering approach, all ontological constructs were arranged in a hierarchy, using the 10 most prominent ontological constructs as parent nodes. Thus, the process resulted in 10 ontological constructs as tier 1 in the ontology and 54 ontological constructs structured in tiers 2 through to 4.

Table 4 List of relevant industry reports

Relevant Industry Reports	Sources
Understanding the components of compliance. (Bace and Rozwell 2006)	Gartner Research
Understanding the costs of compliance. (Bace et al. 2006)	
The enterprise governance, risk and compliance platform defined. (Caldwell 2008)	
Magic quadrant for enterprise governance, risk and compliance platforms. (Caldwell and Eid 2008)	
Risk management and business performance are compatible. (Caldwell and Mogull 2006)	
Use IT governance to leverage business objectives and to support compliance requirements. (Dreyfuss 2008)	
An overall risk and compliance management framework for government agencies. (McClure et al. 2009)	
The compliance journey: balancing risk and controls with business improvement. (KPMG 2005a)	KPMG
The compliance journey: making compliance sustainable. (KPMG 2005b)	
The compliance journey: leveraging information technology to reduce costs and improve responsiveness. (KPMG 2006)	
Compliance framework. (KPMG 2007)	
Understanding and articulating risk appetite.(KPMG 2008)	
AS 3806:2006 compliance programs. (Standards Australia 2006)	Standards Australia
AS/NZS ISO 31000:2009 risk management - principles and guidelines. (Standards Australia and Standards New Zealand 2009)	
GRC capability model "Red Book" 2.0. (Mitchell and Switzer 2009)	OCEG
GRC technology solutions guide version 2.1(OCEG 2011)	

Table 5 Participant demographics – ontology validation

Participants	Industry domain	Organisation size	Roles	Years of experience
1	Financial & insurance services	51–200	Compliance counsel	10+
2	Financial & insurance services	1001–5000	Compliance manager	0–4
3	Financial & insurance services	11–50	Compliance manager	5–9
4	Financial & insurance services	201–500	Compliance manager	10+
5	Legal	1001–5000	Counsel	5–9
6	Public works & utilities	1001–5000	Head of compliance	10+
7	Gaming	1001–5000	Head of compliance	5–9
8	Gaming	1001–5000	Compliance manager	0–4

During the concept identification process, the coding also focused on identifying relationships between the compliance management concepts. Accordingly, a node was created in NVivo to represent a group of fragments from the data sources that provided evidence of a particular relationship between concepts. The relationship nodes were then further classified by referring to the category of relationship i.e. specialization, aggregation and association (Booch et al. 2005). Specialization and aggregation were used to structure the hierarchy of the identified concepts, whereas association was used to depict non-hierarchical relationships, e.g. dependency or impact. These three relationship types are referred to as type-of (specialization), part-of (aggregation), and assoc. (association) in the remainder of this paper.

Coding Coding involves an explicit formal representation of the conceptualisation captured in the earlier stage. Formal representation is required to restrict the possible misinterpretations of a particular concept. Furthermore, ontological constructs are usually hierarchically organized through a structuring relation, such as is-a (class-superclass, instance-class) or part-of (Pinto and Martins 2004). Typical representations that are available for ontology documentation are Web Ontology Language (OWL), KIF, Cyc, Ontolingua, and FLogic (Pulido et al. 2006).

In our work, we employ the use of OWL (Web Ontology Language) (W3C OWL Working Group 2009) - a de facto standard for ontology representation on the web - to provide a formal representation of CoMOn.[4] The result is a formal representation of the ontological constructs and their associated relationships and attributes. The OWL representation serves multiple purposes of further disambiguation/checking, relationship structuring, version management and a foundation for future tool support.

Integration with existing ontologies Integration of ontologies is the process of reusing and synthesizing one or more

relevant ontologies to develop a new ontology (Pinto et al. 1999). Ontology integration typically involves aggregating, combining, and assembling together several source ontologies to form a resulting ontology, possibly after source ontologies have been subjected to changes, such as, extension, specialization, or adaptation (Pinto and Martins 2001). The ENTERPRISE methodology (Uschold and King 1995; Uschold 1996) indicates that this step is important where existing related ontologies are available. However, our review of ontology literature suggests that, at this point in time, there are no ontologies related to the compliance management topic at hand. Accordingly, at this stage, we do not consider integration with existing ontologies.

Validation Ontology building requires the developer to have the necessary domain expertise to ensure that the ontology constructs, as well as the relationships between them, are precisely defined and capable of being mapped to an end user's needs (Nawoj and Goniak 2004). It also requires the developer to have the appropriate set of research, methodology and analytical skills. Together, this set of skills is rare, and we envision ontology building to be carried out by a developer in conjunction with domain experts for target users. Accordingly, we extended the building phase of the ENTERPRISE methodology to include a validation step. This validation step is akin to a quality check to ensure fit and relevance. In the case of CoMOn, this validation centres on the perception of compliance management experts and practitioners in terms of the quality of the ontology and facilitates refinement of concepts. To obtain detailed feedback and refine the ontology, we conduct this validation step through a case study approach with a targeted set of questions based on the semiotic framework (Burton-Jones et al. 2005). A case study approach is appropriate in this context as it allows the participant to reason about the application of the ontology in their organisational setting, and has the flexibility for discussion of related issues, as well as review of related organisational documents. We adopt the semiotic framework (Burton-Jones et al. 2005) as a means of ontology validation because it provides a proven set of metrics for ontology

---

[4] OWL specification of CoMOn is omitted from this paper due to space constraints.

Fig. 3 An excerpt of validation for penalty cost construct from workbook

5. *Cost >> Cost of Non-Compliance >> Penalty Cost*

<u>Definition:</u> The cost that need to be paid as a result of compliance violation. This may include exemplary fine, damage cost, and cost of redevelopment.

Properties:	Penalty Name	Penalty Description	Recipients	Amount
Example of Concept Realisation:	*Exemplary Fine 01*	*Pay due to negligence of conduct with regard to Fair Information Practice Code*	*Individual: <undisclosed>*	*$150,000*

CRITERIA	LOW 1	2	3	4	5	6	HIGH 7
Clarity **(C)**	O	O	O	O	O	O	O
Interpretability **(I)**	O	O	O	O	O	O	O
Comprehensiveness **(M)**	O	O	O	O	O	O	O
Accuracy **(A)**	O	O	O	O	O	O	O

Relevance (R)	O YES O NO

Table 6 The statements and sources of references

No.	Statements	Sources of References
1.	Background knowledge in ontology usage is essential to effectively use this ontology.	(Davis 1989; Davis et al. 1989)
2.	Compliance management experts would understand this ontology with little effort.	
3.	I can easily master the use of this ontology.	
4.	I find it is easy to use the ontology to describe compliance management in my organisation.	
5.	I find the ontology is flexible to apply.	
6.	Learning to use the compliance management ontology is easy for me.	
7.	The ontology is difficult to use.	
8.	The ontology is presented in a way that allows me to easily locate/identify a concept to instantiate.	
9.	The ontology is unnecessarily complex.	
10.	This ontology is cumbersome to understand.	
11.	I find this ontology useful for representing my organisation's compliance management situation.	(Davis 1989; Davis et al. 1989)
12.	I needed to ask a lot of questions before I could start using this ontology.	
13.	I find the ontology useful for my job.	
14.	I have the knowledge necessary to use the ontology.	(Venkatesh 2000; Mathieson 1991; Taylor and Todd 1995)
15.	I have the resources necessary to use the ontology.	
16.	The hierarchy (progressive refinement of concepts) in the ontology is helpful.	(Davis et al. 1992)
17.	The ontology is able to capture the compliance management structure in my organisation.	
18.	The ontology is not compatible with current compliance management practices in my organisation.	
19.	It scares me to think that I could end up with a lot more problems after using this ontology to describe compliance management in my organisation.	(Venkatesh 2000; Casellas 2009)
20.	Further theoretical knowledge on ontology design is needed to enable understanding of this ontology.	
21.	I am confident that I understand the design of the ontology.	
22.	I feel apprehensive about using the ontology.	
23.	The ontology is somewhat intimidating to me.	
24.	I believe it would be a good idea to use this ontology for compliance management in my organisation.	(Davis 1989; Davis et al. 1989)
25.	I have generally favorable attitude toward using this ontology.	
26.	I intend to use this ontology for my compliance management needs.	
27.	I like the idea of using this ontology.	
28.	I will refer to this ontology often.	

Springer

Table 7 Participant demographics – ontology usability evaluation

Participants	Industry domain	Organisation size	Roles	Years of experience	Level of training
1	Financial & insurance services	10,001+	Head of compliance	10+	Industry certification, On Job Training
2	Financial & insurance services	10,001+	Head of compliance	5–9	Professional training, industry certification, on job training
3	Financial & insurance services	10,001+	Compliance manager	0–4	Professional training, industry certification, on job training
4	Financial & insurance services	1001–5000	Compliance manager	10+	Industry certification
5	Consumer protection	501–1000	Head of compliance	10+	Professional training, on job training
6	Education	5001–10,000	Compliance manager	10+	Professional Training, On Job Training

assessment (as acknowledged by (Leukel and Sugumaran 2009; Eessaar 2013; Dividino and Sonntag 2008).

The semiotic framework (Burton-Jones et al. 2005) specifies four metrics to validate the quality of ontology; namely, Syntactic Quality, Semantic Quality, Pragmatic Quality and Social Quality. Syntactic Quality is measured through Lawfulness (correctness of syntax) and Richness (breadth of syntax used). The second metric, Semantic Quality, is measured through Interpretability (meaningfulness of terms), Consistency (consistency of meaning of terms) and Clarity (average number of word senses). The third metric, Pragmatic Quality includes Comprehensiveness (number of classes and properties), Accuracy (accuracy of information), and Relevance (relevance of information for a task). Finally, the fourth metric Social Quality includes Authority (extent to which other ontologies rely on this ontology) and History (the number of times the ontology has been used).

We were motivated to ensure that participants involved in the validation step involved practitioners directly involved in compliance management practice in their organisation and experts who provide compliance management advisory services to clients. To that end, we again enlisted the ACI to obtain a set of eight experienced participants with insight into compliance management in organisations, ensuring there was no overlap

between these eight participants and the participants interviewed and surveyed for the purpose of concept identification. Given that CoMOn must be relevant to all organisations with an interest in compliance management, we selected participants from different industries (including legal, financial and insurance services, gaming, public works and utilities), and organisations of different sizes. Their typical roles included: head of compliance, compliance manager, and compliance counsel. The participant details are summarised in Table 5.

To conduct the validation case studies, our research team consisted of three experienced empirical researchers, one with the role of the main interviewer and two with a support role of note taking, related document analysis, and further probing. The case studies utilized several data gathering instruments, as described in the following, which facilitated feedback from practitioners in both quantitative and qualitative forms.

The case studies were structured with the help of a workbook guiding the participant through the ontology. The workbook was developed to capture participant feedback with respect to clarity (C), interpretability (I), comprehensiveness (M), accuracy (A), and relevance (R) of an individual concept in ontology (as derived from the semiotic framework (Burton-Jones et al. 2005)). Four remaining criteria from the semiotic framework, viz. consistency, lawfulness, richness and social

Table 8 Mean score for ontology validation of core concepts

Concepts	Clarity (C)	Interpretability (I)	Comprehensiveness (M)	Accuracy (A)	Relevance (R)
Business process	6.0	6.4	5.8	6.1	1
Cost	5.5	5.8	4.5	4.6	1
Culture	5.0	5.6	5.5	5.0	1
Program	6.0	6.1	5.5	5.4	1
Regulator	5.3	6.0	5.6	4.8	1
Regulatee	6.3	6.5	6.1	5.9	1
Requirements	5.5	6.1	5.6	5.5	1
Risk management	5.8	5.8	5.6	5.5	1
Solutions	5.6	5.9	5.9	5.6	1
Service provider	5.5	5.6	5.5	5.0	1

quality, were excluded for this stage of the study. While these four criteria remain significant to our overall evaluation of the ontology, we leave these for future work because validation based on those criteria is not feasible for the participants targeted in this study. The four criteria demand familiarity with the ontology after some period of use. In particular, consistency requires exploration of the concepts within CoMOn and careful observation to detect the occurrence of inconsistencies, an observation best made after a period of ontology use. Richness and lawfulness, on the other hand, focus on the syntax of the ontology - thus require assessment of the types of terms (e.g. class, subclass, type, property, and relationships types). Again, this only can be done if the participants have been introduced to ontology jargon and have experience applying it.

The interview protocol was implemented through the workbook structure, which contained instructions to the participant as well as the definition for each ontological construct. For each construct, a table was provided in which the participants could specify their perception on the five criteria for quality evaluation, namely clarity (C), interpretability (I), comprehensiveness (M), and accuracy (A) for each of the concepts on a 7-point Likert scale representing the level of their agreement for a particular criteria associated with a particular concept. The table also captured the relevance of each

ontological construct, through a binary measure (is relevant or not). See Fig. 3 for an example excerpt of the workbook. The evaluation of the five criteria resulted in a quantitative rating for each concept. Simultaneously, the verbal feedback on the ontology concepts and relationships was recorded during the sessions and provided qualitative data used for the refinement of CoMOn.

Each session started with a presentation of ontology in general, and the introduction of CoMOn specifically, as well as the rationale/motivation behind the development of CoMOn. Following this introductory session, the participant was provided with a copy of the workbook. The participants were also provided an easy to understand overview of the structure and content of CoMOn (see Appendix A), and a catalogue of CoMOn construct definitions, including all construct attributes (which were not shown in the workbook).

The interviewer guided the participant through filling out the workbook with instantiations of the participant's organisational compliance management activities, while also probing for supporting organisational documentation and examples as necessary. A number of open-ended questions were included at the end of the session to gather deeper insights and to ensure that any missing constructs were probed and identified.

Our validation approach allowed us to reason about the need for refinement of CoMOn before testing the utility of

Fig. 4 Refinement of requirement concepts
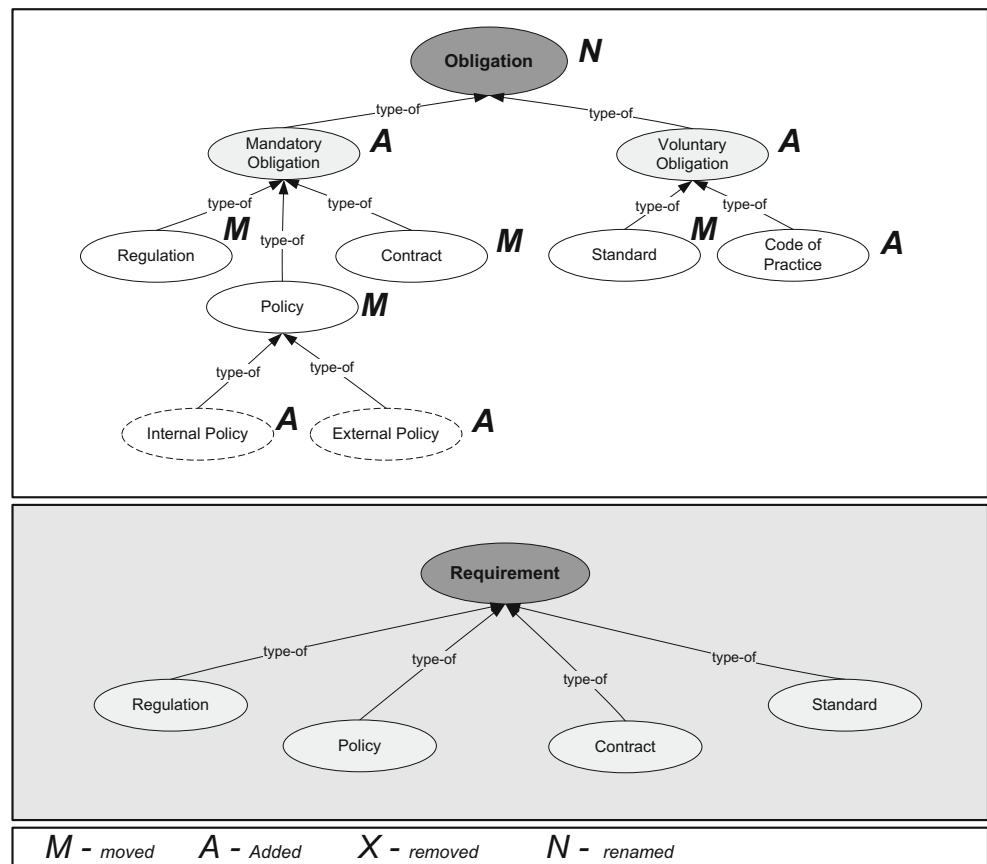
the ontology. To this end, each of CoMOn's concepts was inspected and reviewed for its weaknesses with respect to the semiotic framework's measures of clarity, interpretability, accuracy, comprehensiveness, and relevance. Data from our validation stage indicated that the ontology had redundant concepts and was also missing concepts that were thought to be of importance. Accordingly, based on feedback of participants in the validation stage, we refined CoMOn by making changes that include (but are not limited to) introduction of new concepts, deletion of concepts, refinement of definitions, refinement of relations, and renaming of concepts. Following this validation and resulting refinement, which was aimed at identifying the quality of the ontology and ensuring no concepts were missing, the refined ontology was then subjected to an evaluation of usability with its intended audience. Hence, all changes made can be traced back to consensus between the eight case studies.

3.3 Ontology evaluation

All ontology building methodologies recognize the importance of evaluation (Pinto and Martins 2004), as does the Design Science approach inherent to our research (Hevner et al. 2004). While guidance for evaluation is

mostly lacking in ontology development methodologies, there are a number of approaches studied in literature for evaluating a domain specific ontology (Burton-Jones et al. 2005; Brewster et al. 2004; Guo et al. 2009; Porzel and Malaka 2004; Brank et al. 2005). A review of ontology evaluation techniques by Brank et al. (2005) suggests that ontology evaluation approaches fall into one of the following categories: (1) those based on comparing the ontology to a "golden standard" (which may itself be an ontology); (2) those based on using the ontology in an application and evaluating the results; (3) those involving comparisons with a source of data (e.g. a collection of documents) about the domain to be covered by the ontology; or (4) those where evaluation is done by humans who try to assess how well the ontology meets a set of predefined criteria, standards, requirements, etc. Since we included a validation and refinement step in our ontology building process – which aimed at judging and improving the comprehensiveness of the ontology, in this phase, we select a usability evaluation to understand users' intentions to use the refined ontology, its fit with user needs, and related aspects.

The usability evaluation was conducted with a targeted set of questions acquired from Technology Acceptance Model (TAM) (Venkatesh and Bala 2008). Initially developed to predict individual adoption and use of new Information Technology (Davis
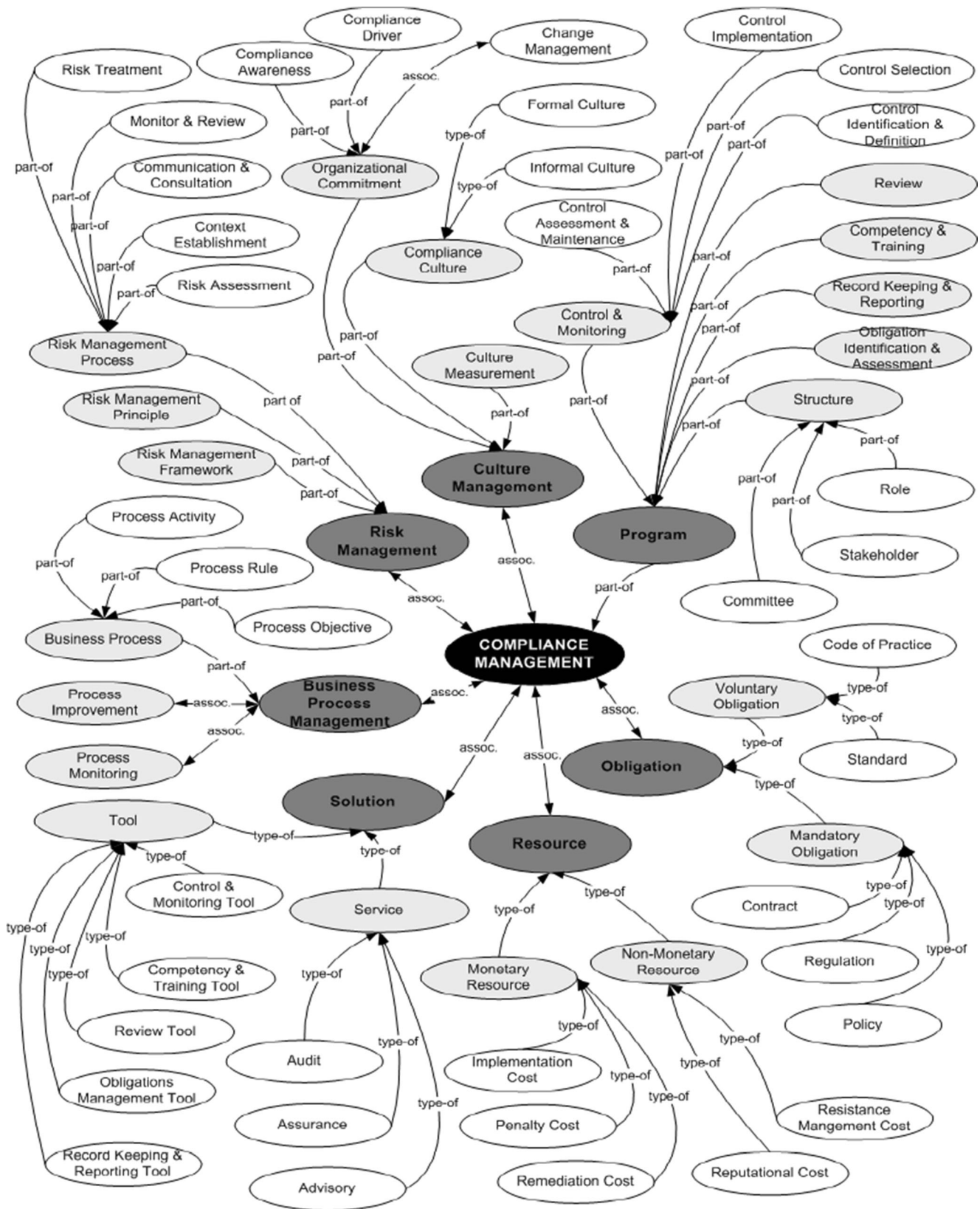

Fig. 5 Refinement of resource concepts
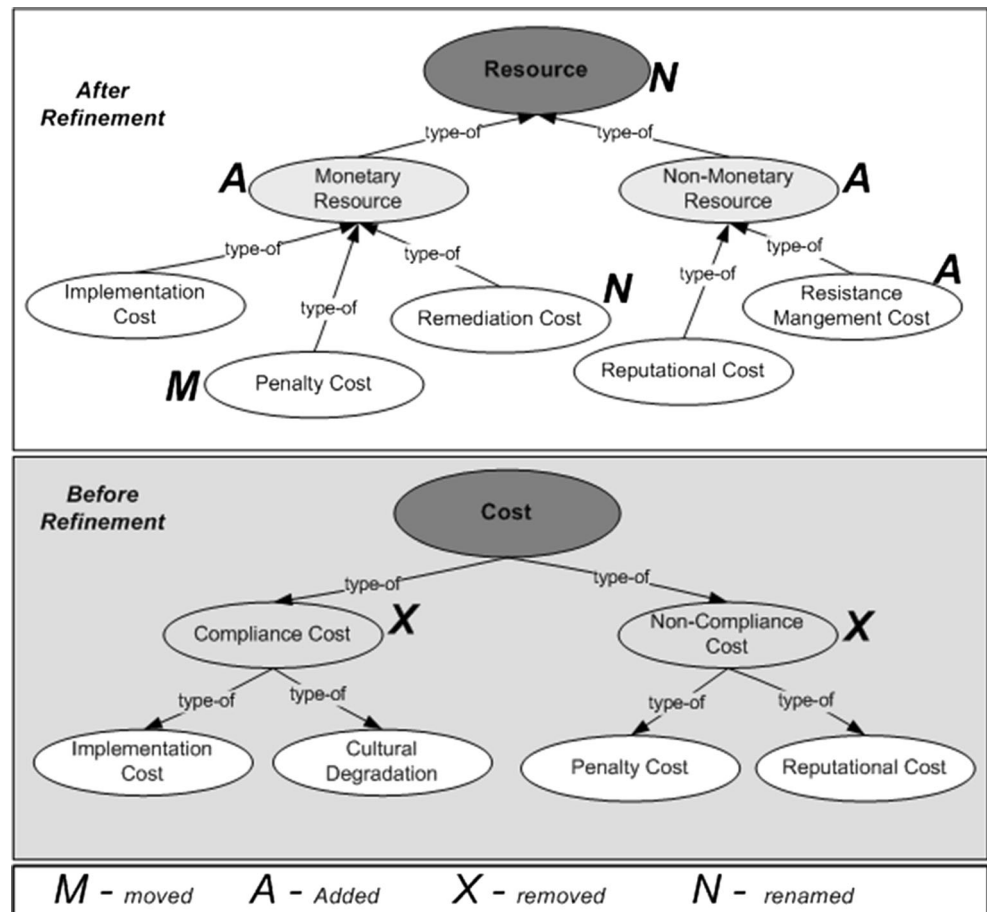
Fig. 6 CoMOn, showing first, second and third tier constructs

1989; Davis et al. 1989), TAM (Venkatesh and Bala 2008) is now recognized as one of the main IS theories that contributes to

understanding of users' acceptance of information systems (IS)/ information technology (IT). In our work we utilize six factors

Table 9 Definition of the refined core CoMOn constructs

Construct	Definition
Business process management	A holistic management approach focused on aligning all aspects of an organization with the wants and needs of clients. It promotes business effectiveness and efficiency while striving for innovation, flexibility, and integration with technology.
Culture management	The way the organization cultivates compliance culture.
Obligation	The prescribed and/or agreed set of norms that are mandated or voluntarily adopted by an organization or individual.
Program	A series of activities that, when combined, are intended to achieve the desired level of compliance.
Resource	Monetary and non-monetary resources allocated to meet compliance obligations.
Risk management	Coordinated activities to direct and control an organization with regard to risk.
Solution	A particular method, tool or service that provides assistance to the regulated organization in meeting their compliance obligations.

from TAM that include Perceived Ease of Use (PEOU), Perceived Usefulness (PU), Perception of External Control (PEC), Job Relevance (REL), Technology Anxiety (ANX), and Behavioural Intention (BI), as follows:

(1) PEOU is used to determine the degree of ease associated with the use of the ontology;

(2) PU is used to determine the degree to which a person believes the ontology would enhance his or her performance in compliance related activities;

(3) PEC is used to determine the degree to which an individual believes that organisational and technical resources exist to support the use of the ontology;

(4) REL is used to determine the degree to which an individual believes that the target ontology is applicable to his or her job.

(5) ANX is used to determine the degree of an individual's apprehension, or even fear, when she/he is faced with the possibility of using the ontology;

(6) BI is used to determine the degree to which a person has formulated conscious plans to use the target ontology.

Measures for these factors were adopted from prior literature and reworded to fit the compliance management context (as shown in Table 6).

To conduct the usability evaluation we recruited, with the help of the ACI, a further six experienced compliance management professionals with insight into compliance management in organisations. The participants were from different industry domains (including four from financial and insurance services, one each consumer protection, and education), had varied years of experience (see Table 7) and were employed in roles including Head of Legal, Risk and Compliance, Head of Compliance, as well as Compliance Managers and/or Risk Managers. Again, we ensured there was no overlap between these participants and the participants involved in the initial interviews and survey, as well as the eight participants involved in the validation case studies.

For the conduct of the evaluation, a research team consisting of two experienced empirical researchers was formed, one with the role of the main interviewer and the other one with a support role of note taking and further probing. This study utilized data gathering instruments that facilitated feedback from practitioners in both quantitative and qualitative forms. Following a protocol somewhat similar to that used in the validation step, in that we developed a workbook intended to capture examples of applied ontological constructs. The workbook contained a catalogue of all CoMOn constructs, together with their detailed definitions. Space was provided for each construct to be instantiated by the participant into their own organisational context – i.e. for each construct the participant was asked to discuss and provide an example of the application of the ontological construct. In addition, we also developed a survey instrument[5] to capture participant feedback on the usability of the ontology with respect to Perceived Ease of Use (PEOU), Perceived Usefulness (PU), Perception of External Control (PEC), Job Relevance (REL), Ontology Anxiety (ANX), and Behavioural Intention (BI).

In a similar manner to the validation conducted for the purposes of ontology refinement, each session started with a presentation of ontology in general, and the introduction of CoMOn specifically, as well as the rationale/motivation behind the development of CoMOn. The participants were also provided with a complete diagram of the CoMOn constructs (refined ontology). After the completion of the workbook, and handover of any relevant organisational documents, the participants were provided with a paper-based usability survey used to capture their perception of CoMOn usability. The questionnaire consisted of two sections. The first section aimed to gather the demographic details of the participants (such as role, experience and organisation classification, etc). The second section consisted of 28 statements representing

---

[5] The survey instrument was pilot tested with three academics familiar with the compliance management domain.

Table 10 Usability evaluation results

Construct	P1	P2	P3	P4	P5	P6	Mean
Perceived ease of use (PEOU)	5.4	5.6	4.0	6.0	5.5	5.9	5.4
Perceived usefulness (PU)	5.3	6.3	3.3	6.0	5.7	5.7	5.4
Perception of external control (PEC)	5	7	4	5.5	6	6	5.6
Job relevance (REL)	5.3	6.3	4.3	6.0	6.0	5.7	5.6
Ontology anxiety (ANX)	4.2	7.0	5.0	5.8	5.8	4.8	5.4
Behavioural intention (BI)	4.8	6.6	2.8	6.2	6.0	6.0	5.4

the six usability criteria to be measured (10 statements for PEOU, 3 statements for PU, 2 statements for PEC, 3 statements for REL, 5 statements for ANX, and 5 statements for BI). Each statement used a 7-point Likert scale. These statements and its origin sources of references were presented in Table 6.

3.4 Ontology documentation

To ensure future utility of the ontology, the developed ontology needs to be adequately documented such that it can be accessible to the target users. Given that the target audience of CoMOn is a set of business users, a user-friendly manual was prepared to describe the ontology. The manual consists of an A3 size diagram of CoMOn's concepts, and the catalogue of concepts that provides concepts definition, relationships details, as well as attributes for each concept. The manual underwent a number of revisions as a result of ontology evaluation. The most recent documentation manual is available from the authors upon request, with an online version currently under development. Moreover, the ontology was also documented formally using OWL (Web Ontology Language) (W3C OWL Working Group 2009).

Having presented the ontology development process, in the following we outline the results of the ontology refinement, introduce the refined ontology and its core concepts, and present the results of the usability evaluation of the refined ontology.

4 The compliance management ontology (CoMOn)

In Table 8, we provide the results from the validation of the core CoMOn constructs, in the form of mean scores of the five quality criteria for each of the individual core ontological construct. Recall from section 3.2 that for each construct, a table was provided in which the participants could specify their perception on the five selected criteria for quality evaluation, namely clarity (C), interpretability (I), comprehensiveness (M), and accuracy (A) for each of the concepts. These scores were used to identify CoMOn constructs that may need refinement. For example, low accuracy and low comprehensiveness scores for the Cost construct ($A = 4.6$ and $M = 4.5$) suggests that the definition of Cost as a construct that requires improvement. We note that agreement is reached in terms of the relevancy of all core CoMOn constructs. Apart from quantitative feedback, the refinement process also involved the use of qualitative verbalised feedback (which was recorded and transcribed for analysis).

The ontology validation and subsequent refinement process identified missing ontological constructs, as well as existing constructs that were considered superfluous or unclear. The validation stage resulted in the removal of some concepts as well as the identification of additional concepts of relevance. Furthermore, some of the relationships between concepts were also refined based on the eight case studies, resulting now in a set of 7, rather than the initial 10, core concepts. In the following paragraphs we provide examples

Table 11 Perceived ease of use (PEOU) responses

Statements	P1	P2	P3	P4	P5	P6	Mean
PEOU1. Background knowledge in ontology usage is essential to effectively use this ontology.	3	3	3	5	6	2	3.7
PEOU2. Compliance management experts would understand this ontology with little effort.	6	5	5	6	7	7	6.0
PEOU3. I can easily master the use of this ontology.	6	6	5	7	6	6	6.0
PEOU4. I find it is easy to use the ontology to describe compliance management in my organisation.	6	5	6	7	6	6	6.0
PEOU5. I find the ontology is flexible to apply.	5	6	6	6	5	6	5.7
PEOU6. Learning to use the compliance management ontology is easy for me.	6	6	5	6	5	6	5.7
PEOU7. The ontology is difficult to use.	2	2	6	1	2	2	2.5
PEOU8. The ontology is presented in a way that allows me to easily locate/identify a concept to instantiate.	4	5	2	6	6	5	4.7
PEOU9. The ontology is unnecessarily complex.	3	2	6	2	2	3	3.0
PEOU10. This ontology is cumbersome to understand.	3	2	6	2	2	2	2.8

Table 12 Perceived usefulness responses

Statements	P1	P2	P3	P4	P5	P6	Mean
PU1. I find this ontology useful for representing my organisation's compliance management situation.	6	7	4	6	5	5	5.5
PU2. I needed to ask a lot of questions before I could start using this ontology.	3	2	5	2	2	2	2.7
PU3. I find the ontology useful for my job.	5	6	3	6	6	6	5.3

of how and why ontology refinements were made. We do so by way of three excerpts from the refinement stage that depict the refinement of Requirement, Regulatee and Cost concepts (due to the length of the paper we are unable to include all refinement details).

The Requirement concept received low scores for Clarity, Accuracy and Comprehensiveness (when compared to Interpretability). These scores hinted at the need to improve the definition and the scope of the Requirement concept. The need for improvement was also supported by participant feedback. For example, participants indicated: "obligations is a better term to be used to replace 'requirement' term", "the concept must include mandatory and voluntary obligations" and "the concept must include code of practice as its sub-concept", and "the lack of comprehensiveness due restricting the definition to only mandated requirements". Thus, the Requirement concept was renamed to Obligation. The definition for this concept was also revised to include mandatory and voluntary compliance obligations, while Code of Practice was added as a sub-concept of Voluntary Obligations. Figure 4 shows the refined concept (Obligation) and the earlier (Requirement) version.

The Regulatee concept received average scores, however participant feedback indicated lack of need for it. For example, participants stated: "This concept may not necessarily be required as this would mean the organisation itself." and "I have never heard of this term". Considering the need for ontology parsimony, the Regulatee concept was removed from CoMOn.

Lower scores for the Cost concept particularly on Accuracy (4.6) and Comprehensiveness (4.5) indicated a need for refinement. In addition, participants indicated that the "cost concepts need to incorporate more than monetary value" and "to include resources as part of non-compliance cost e.g. due to extra time allocated to persuade people to comply". Hence, as indicated in Fig. 5, the Cost concept was renamed to Resource, which includes monetary and non-monetary costs (both sub-concepts of Resource). The definition of the Resource concept and the definition of its associated sub-concepts were also revised in accordance with the participant feedback.

This process resulted in a new version of the ontology, which contains 81 ontological constructs, with 7 core constructs, structured into four main tiers, representing different levels of detail derived through progressive decomposition of

higher tier constructs. For example, as per Fig. 6, the program concept can be split into constructs of obligation identification and assessment, competency and training, controls & monitoring, record keeping & reporting, review, and structure in tier 2, and so on. each concept is equipped with a definition, attributes, and relationships where Applicabl*e*. **error**! **Reference source not found.**6 shows overall CoMOn concepts including its first, second, and third tier concepts after the evaluation and refinement phases.

Overall, comon concepts are led by seven core concepts namely business process management, culture management, obligations, program, resources, risk management, and solutions. Table 9 lists the definition of the core constructs for CoMOn. A summary of all 81 constructs is provided in Appendix B[6].

5 Ontology usability evaluation

Once the ontology was developed and then refined through validation with eight participants, we aimed to study the usability of the ontology in practice. Given our aim to develop an industry-relevant ontology that will be accepted in practice, understanding quality alone is insufficient because while an ontology might be of high quality it may not necessarily be cognitively accessible to the target users. Feedback received from the usability evaluation (conducted with experts, as outlined in section 3) is thus vital to determine users' perceptions on CoMOn in their own compliance management context, and for providing insight into future use of the ontology.

Table 10 summarizes the overall usability feedback of CoMOn. The feedback received from the participants indicates that, overall, CoMOn scores favourably in all constructs involved in the usability evaluation. This favourable perception is evidenced by the 5.6 mean score each for Perception of External Control and Job Relevance, and the 5.4 mean score for each of Perceived Ease of Use, Perceived Usefulness, Ontology Anxiety, and Behavioural Intention. All constructs were measured on a 7-point Likert scale through multiple questions in the usability survey (see tables below).

In addition to exploring the mean rating for each participant per usability construct, we also explore the median score per usability construct, across all accumulated construct

---

[6] Full details of all 81 constructs are available by request.

Table 13 Perception of external control responses

Statements	P1	P2	P3	P4	P5	P6	Mean
PEC1. I have the knowledge necessary to use the ontology.	6	7	4	6	6	6	5.8
PEC2. I have the resources necessary to use the ontology.	4	7	4	5	6	6	5.3

responses. In particular, we find that based on the 60 responses for PEOU construct (which was measured with 10 questions, as outlined in Table 10, each answered by 6 respondents) the median for overall PEOU is 6. This score supports the high agreement received on PEOU, as represented in its overall mean score of 5.4. This finding indicates that the participants agreed that CoMOn is easy to use. Further exploration of the evaluation of PEOU of the ontology shows that statements PEOU2, PEOU3 and PEOU4 received the highest mean scores i.e. 6.0 (see Table 11). These scores highlight the participants' agreement that "Compliance management experts would understand CoMOn with very little effort" (PEOU2), "The participants can easily master the use of CoMOn" (PEOU3), and "The participants find it easy to use CoMOn to describe compliance management in their organisation" (PEOU4). PEOU5 and PEOU6 received a mean score of 5.7 and thus indicate the participants' agreement on the flexibility of CoMOn (PEOU5) and their ability to easily learn CoMOn concepts (PEOU6). The participants are also in agreement that "CoMOn is presented in a way that allows them to easily locate or identify a concept to instantiate", with a mean scores of 4.7 for PEOU8. The respondents rated all reverse scale questions with low scores, further indicating agreement on the ease of use of CoMOn. Among all PEOU related statements, statements PEOU1, PEOU7, PEOU9 and PEOU10 were reverse scale questions. The low scores for these questions indicate that the respondents do not consider background knowledge in ontology usage is essential to effectively use this ontology (PEOU1), nor the ontology to be difficult to use (PEOU7), nor cumbersome to understand (PEOU10), nor unnecessarily complex (PEOU9).

Three statements were used to measure the Perceived Usefulness (PU) TAM construct, as shown in Table 12. Further investigation of participants' feedback for PU suggests that CoMOn is useful for representing participants' compliance management situation. This finding is supported by the high mean scores for PU1 and PU3 with 5.4 and 5.3, respectively. Considering all accumulated feedback, the PU construct received a median score of 6, which evidences the overall agreement on usefulness of CoMOn as perceived by

the industry participants. The participants' opinion on ontology usefulness is also supported by their shared disagreement on PU2, which indicates the level of interaction required to learn the ontology ("I needed to ask a lot of statements before I could start using this ontology"), which received a mean score of 2.7, which shows higher tendency towards accepting CoMOn.

Perception of External Control was measured through two questions, PEC1 and PEC2 shown in Table 13. Our findings indicate that participants agree on readily possessing all required resources and knowledge to apply the ontology. In particular, the participants agree that they have the knowledge necessary to use the ontology (PEC1 mean of 5.8) and, to a lesser but acceptable extent, the resources necessary to use the ontology (PEC2 mean of 5.3). PEC has a median score that equals that of PEOU and PU, thus the median scores so far represent a very consistent level of agreement for PEOU, PU, and PEC.

Job Relevance of the ontology to the context of the participant was measured through three statements, REL1, REL2 and REL3 as shown in Table 14. For REL construct, high scores were received for REL1 and REL2. Participants agreed that the hierarchy (the progressive specialisation of concepts) in the ontology is helpful (REL1), as indicated by the mean score of 5.3. Likewise, REL2 recorded a slightly higher mean score of 5.7. This score indicates that agreement achieved by the participants with respect to the ontology being able to capture the participants' organisation's compliance management structure (i.e. "The ontology is able to capture the compliance management structure in their organisation"). Similarly, the response to the reverse scale question REL3 (i.e. "The ontology is not compatible with current compliance management practices in my organisation"), indicates that the respondents agree that the ontology is compatible with compliance management practice in their organisation.

The Ontology Anxiety construct allows us to determine the level of discomfort or lack of confidence with the ontology. The ANX construct is measured through five questions viz. ANX1, ANX2, ANX3, ANX4, and ANX5, as shown in Table 15. ANX3, which scores the participant's confidence with their understanding of the ontology, received a mean score 6.0,

Table 14 Job relevance responses

Statements	P1	P2	P3	P4	P5	P6	Mean
REL1. The hierarchy (progressive refinement of concepts) in the ontology is helpful.	5	6	3	6	6	6	5.3
REL2. The ontology is able to capture the compliance management structure in my organisation.	6	6	5	6	6	5	5.7
REL3. The ontology is not compatible with current compliance management practices in my organisation.	3	1	3	2	2	2	2.2

Table 15 Ontology anxiety responses

Statements	P1	P2	P3	P4	P5	P6	Mean
ANX1. It scares me to think that I could end up with a lot more problems after using this ontology to describe compliance management in my organisation.	5	1	2	2	2	6	3.0
ANX2. Further theoretical knowledge on ontology design is needed to enable understanding of this ontology.	3	1	2	3	3	3	2.5
ANX3. I am confident that I understand the design of the ontology.	6	7	5	6	6	6	6.0
ANX4. I feel apprehensive about using the ontology.	4	1	5	2	2	3	2.8
ANX5. The ontology is somewhat intimidating to me.	5	1	3	2	2	2	2.5

indicating high participant agreement The low mean scores received for questions ANX1 (3.0), ANX2 (2.5), ANX4 (2.8) and ANX5 (2.5) are in agreement with ANX3 given the reverse scale nature of the questions. Thus, ANX1 shows that participants somewhat disagree on "It scares me to think that I could end up with a lot more problems after using this ontology to describe compliance management in my organisation" statement. Similarly, ANX2, ANX4, and ANX5 mean scores show that the participants either disagree or somewhat disagree that further theoretical knowledge is required to use the ontology (ANX2), that they are apprehensive about the ontology (ANX4) or intimidated by it (ANX5).

Finally, Behavioural Intention is measured through five questions, BI1, BI2, BI3, BI4, and BI5 as depicted in Table 16. The highest mean score of 5.8, received for BI1, indicates agreement on participants' belief that it would be a good idea to use CoMOn for compliance management in their organisation. BI2 and BI4 received mean scores of 5.5, indicating that the participants have an overall favourable attitude to the use of CoMOn. The participants also agreed or strongly agreed that they intend to use the ontology in their own organisational setting (BI3 of 5.3), however, they were less sure in regards to the frequency with which they would refer to the ontology once in use (BI5 mean score of 4.8). Overall, a median score of 6 was recorded from the Behavioural Intention assessment, evidencing a high level of agreement among the participants with respect to the BI construct.

6 Concluding discussion

In this paper, we presented a Compliance Management Ontology (CoMOn) – developed to address an evident need

within the compliance management professional and research communities for a shared understanding of the various concepts that define the compliance management landscape. CoMOn is the result of a study that has spanned across the various phases of ontology development, refinement and evaluation. In particular, the rigorous development process, with multiple cycles, expert and practitioner feedback, refinement, and the usability evaluation, has positioned CoMOn as an ontology that provides a basis for shared conceptualisation for the Compliance Management domain. The professional community has indicated that they consider the ontology as a foundation on which to assess the thoroughness of their compliance regimens and identify aspects of their compliance initiatives and programs that may be missing or lacking. For example, participants of the usability evaluation stated "*CoMOn can be used to validate the current models that we used in current compliance management practice. I see CoMOn as a smart tool to start off with where you can benchmark it. I can look at the diagram and see where I can incorporate any of the items (concepts) and if there is an area where I cannot incorporate it well then I will know I have got a problem.*" and "*CoMOn can also show the level of maturity to see gap. We should be able to bring this to the board and say based on this (CoMOn), this is where we believe the compliance maturity is sitting in our organisation and in two years' time we want to get there. So, we need investment in items A, B and C (for example).*" In addition, unsolicited feedback from the compliance management community has also demonstrated the potential of this ontology – for example, "*I like the terminology here. I found it is very sanitised in terms that it is not industry specific so that's quite a good strength.*" and "*Seeing it set out like this, if you were starting out and doing like year first compliance for the first time, I think this is a nice little map for want of a better*

Table 16 Behavioural intention responses

Statements	P1	P2	P3	P4	P5	P6	Mean
BI1. I believe it would be a good idea to use this ontology for compliance management in my organisation.	5	7	3	7	6	7	5.8
BI2. I have generally favourable attitude toward using this ontology.	5	6	4	6	6	6	5.5
BI3. I intend to use this ontology for my compliance management needs.	5	7	2	6	6	6	5.3
BI4. I like the idea of using this ontology.	5	7	3	6	6	6	5.5
BI5. I will refer to this ontology often.	4	6	2	6	6	5	4.8

term." Further, the professional community indicated that CoMOn is suitable to be realised as a tool for organisations compliance management learning and training.
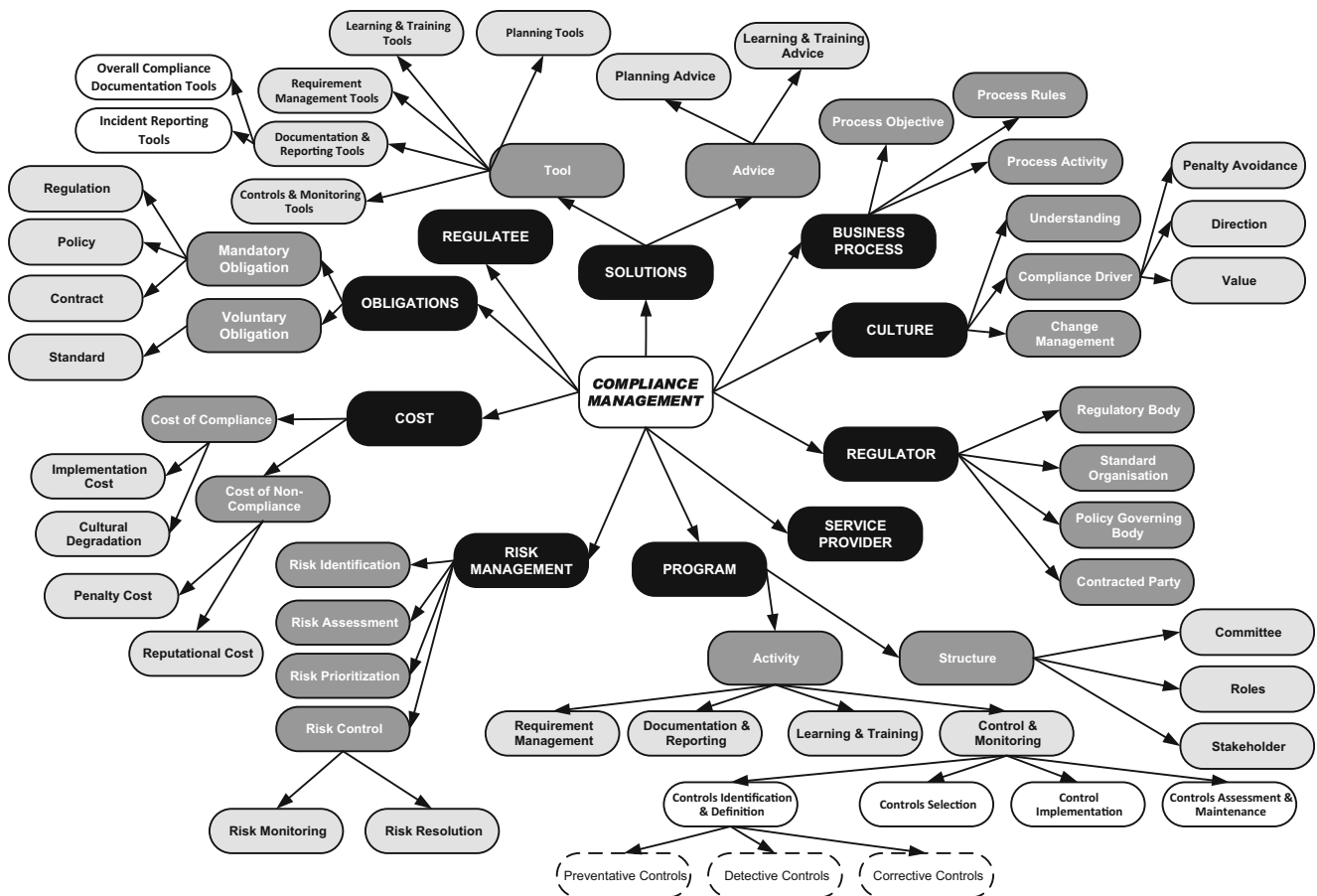
In addition to our ontological contribution to the compliance management domain, our work also denotes a methodological contribution. A review of existing ontology development methodologies highlighted gaps in the body of knowledge in relation to the process of rigorous identification of ontology concepts, determining the concepts' industry relevance, as well as overall evaluation of the ontology. Accordingly, we extended a well-known ontology development methodology - ENTERPRISE - to include a rigorous and iterative process of concept coding based on a variety of data sources. In addition, we extended the methodology to incorporate a validation step within the ontology building phase - an additional quality check that facilitates the refinement of the ontology based on the input of its target user group, prior to final evaluation. Finally, we also provided a detailed approach for ontology usability evaluation based on the Technology Acceptance Model.

In our future work, we will focus on the identification of further relationships between ontological sub-constructs belonging to different tiers of CoMOn constructs. The main limitation of the ontology in its current form is the limitation in the scope of relationships between detailed ontological constructs to those belonging to the same core ontological construct. A further empirical study has begun to identify all relationships that exist between the eighty-one ontological constructs. Once this study is completed, a larger scale quality and usability study will be conducted, also incorporating the currently excluded dimensions from the semiotics framework. In addition, work is currently under way to develop a web portal through which the ontology can be provided to practitioners and researchers for research, reference and training purposes.

Appendix A

Overview of the structure and content of CoMOn (used for Ontology Validation)

Appendix B

Table 17   List of constructs and definitions

Concepts	Definitions
Business process management	A holistic management approach focused on aligning all aspects of an organization with the wants and needs of clients. It promotes business effectiveness and efficiency while striving for innovation, flexibility, and integration with technology.
Business process	A set of coordinated activities designed to accomplish a particular business objective.
Process objective	Measurable result or state a particular process is intended/required to attain.
Process activity	A single logical step in a business process.
Process rules	Constraints and conditions imposed on a particular process.
Process monitoring	Continual checking, supervising, critically observing or determining the status of the process in order to identify the occurrence of changes, errors, irregularities, inefficiencies and bottlenecks.
Process improvement	A systematic approach to help an organization optimize its underlying processes to achieve more efficient business outcomes.
Culture management	The way the organization cultivates compliance culture.
Compliance culture	The values, ethics and beliefs that exist throughout an organization and interact with the organization's structures and control systems to produce behavioural norms those are conducive to compliance outcomes.
Formal culture	The visible segment of the organizational culture, such as policies and procedures, mission statement, and dress codes.
Informal culture	Organizational characteristics and relationships that are not part of the formal structure but that influence how the organization accomplishes its goals.
Organizational commitment	Commitment by the organization and top management towards effective compliance that permeates through the whole organization. Organizational commitment includes change management, setting up compliance drivers, putting resources towards compliance programs, and strengthening compliance understanding.
Change management	A well-structured approach to infuse compliance behavior in a particular organization.
Compliance driver	A condition, offering, or value that promotes compliance behavior.
Direction	The strategic focus of an organization toward a particular end or goal that influences its compliance activities. This may include, but not limited to, strategic decision, risk appetite, or organizational aspiration.
Value	Advantage/benefit gained as a result of compliant behaviour.
Penalty avoidance	A condition where a regulated organization/individual may be influenced to be compliant in order to avoid non-compliant associated penalty.
Compliance awareness	The ability to connect compliance with business operations.
Culture measurement	Assessment of the degree of compliance culture cultivation among individuals and within an organization.
Obligation	The prescribed and/or agreed set of norms that are mandated or voluntarily adopted by an organization or individual.
Mandatory obligation	The obligations that are mandated to a particular individual, organization or industry due to endorsement of a particular regulation/legislation, policy, or contractual agreement.
Regulation	Rule or law designed based on, and intended to carry out, a specific piece of legislation in governing and controlling conduct of a regulate.
Policy	Set of basic principles and associated guidelines, formulated and enforced by the governing body or a particular organisation, to direct and limit its actions in pursuit of intended goals.
Internal policy	Set of basic principles and associated guidelines, formulated and enforced by a particular organisation to direct and limit its actions in pursuit of intended goals.
External policy	Set of basic principles and associated guidelines, formulated and enforced by the governing body to direct and limit the organisational actions in pursuit of intended goals.
Contract	The visible segment of the organizational culture, such as policies and procedures, mission statement, and dress codes.

Table 17 (continued)

Concepts	Definitions
Voluntary obligation	The obligations, either in form of a standard or a code of practice, that are voluntarily adopted or accepted by a particular organization or industry.
Standard	Documented codes of ethics, codes of conduct, good practices and charters that an organization has adopted for its operations.
Code of practice	A statement of recommended practice developed internally by an organization or by an international, national or industry body or other organization.
Program	A series of activities that, when combined, are intended to achieve the desired level of compliance.
Obligation identification & assessment	The systematic way of identifying organizational compliance obligations and the way in which they impact on its activities, products and services. This includes the maintenance and prioritization of compliance obligations.
Competency & training	Activities planned to ensure that all employees are competent to fulfil their job role in a manner that is consistent with the organization's compliance culture and its commitment to compliance.
Control & monitoring	The observation mechanisms set up and performed by an organization to observe their particular business operations and to reduce/prevent the likelihood of non-compliance (risk).
Control identification & definition	Activities created to address and resolve compliance related risks.
Preventative control	Mechanisms designed to avoid the likelihood of non-compliance.
Detective control	Mechanisms designed to observe a particular business activity and detect any compliance violation.
Corrective control	Provide remediation to a particular non-compliance that has been detected.
Control selection	An activity that is performed to choose the appropriate controls to be employed for a particular business operation. This includes choosing the type of control that will be implemented which could be preventative, detective, or corrective in nature.
Control implementation	Putting the selected controls for particular business operation in place.
Control assessment & maintenance	Activity that corresponds to review of current controls in place. Accordingly, the decision from the review will prompt the organization to add new controls; or to replace, update, or drop a particular control.
Record keeping & reporting	The preparation and maintenance of documents, records and reports that are associated with organizational compliance activities to assist monitoring and review processes and demonstrate conformity with the compliance program. This includes full and frank reporting to keep governing body, organization and compliance manager well informed on all relevant compliance incidents.
Review	Continuous assessment of compliance program to ensure its continued suitability, adequacy and effectiveness.
Structure	The visible segment of the organizational culture, such as policies and procedures, mission statement, and dress codes.
Committee	Specification of how compliance related responsibilities are delegated, controlled, and coordinated within a compliance program.
Role	Specification of how compliance related responsibilities are delegated, controlled, and coordinated within a compliance program.
Stakeholder	Specification of how compliance related responsibilities are delegated, controlled, and coordinated within a compliance program.
Resource	Monetary and non-monetary resources allocated to meet compliance obligations.
Monetary resource	The amount of money or loss that an organization needs to pay to have their compliance management initiatives in place. This may include implementation cost, remediation cost, and penalty associated cost or loss.
Implementation cost	A monetary value allocated by an organisation to support the implementation of compliance management activities. This includes, but is not limited to, staff and training cost, legal and governance cost, insurance cost, auditing cost, consulting cost, software and it services cost, and record management cost.
Penalty cost	A cost that need to be paid as a result of compliance violation. This may include exemplary fine, damage cost, and cost of redevelopment.

Table 17 (continued)

Concepts	Definitions
Remediation cost	Cost that deals with removal or corrective actions taken onto the source or cause of non-compliance.
Non-monetary resources	The use or loss of non-monetary sources by an organization in exchange to have their compliance management initiatives in place. This may include reputational cost and resistance management cost.
Reputational cost	A cost associated with the reputational damage that is incurred by an organisation as a result of non-compliance. This includes cost as a result of decreased market influence, loss of competitive advantage, and loss of customers to another competitor.
Resistance management cost	Organisational loss due to unfavourable reaction towards compliance management initiatives. This may include, but not limited to, losing employees, interruption in business activities, and staff resistance.
Risk management	Coordinated activities to direct and control an organization with regard to risk.
Risk management principle	A specific basis of conduct for managing risk.
Risk management framework	Set of components that provide the foundation and organizational arrangements (i.e. Policies, procedures and practices) for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
Risk management process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.
Context establishment	Defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk identification	Process of finding, recognizing and describing risks.
Risk analysis	Process of comprehending the nature of risk and to determine the level of risk.
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.
Risk treatment	Process of modifying risk. Risk treatment can involve avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk, taking or increasing risk in order to pursue an opportunity, removing the risk source, changing the likelihood, changing the consequences, sharing the risk with another party or parties (including contracts and risk financing) and retaining the risk by informed decision.
Communication & consultation	Continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk.
Monitor & review	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected. This may also include activity undertaken to determine the suitability, adequacy and effectiveness of the risk management framework, risk management process risk or control to achieve established objectives.
Solution	A particular method, tool or service that provides assistance to the regulated organization in meeting their compliance obligations.
Tool	Instruments (manual or automated) used by an organization as means to accomplish their compliance related activities. Tools include obligation management tool, competency & training tool, control & monitoring tool, record keeping & reporting tool, and review tool.
Obligation management tool	Instruments used by the organization to facilitate managing and communicating of compliance obligations.
Control & monitoring tool	Instruments used by the organization to facilitate monitoring of their compliance state and performing the designated controls.
Competency & training tool	Instruments used by the organization to facilitate employee training and develop employees' competency to fulfill their job role in a manner that is consistent with the organization's compliance culture and its commitment to compliance.
Record keeping & reporting tool	Instruments used by the organization to facilitate the preparation and maintenance of documents, records and reports that are associated with organizational compliance activities.
Review tool	Instruments used by the organization to facilitate continuous assessment of compliance program.

Table 17 (continued)

Concepts	Definitions
Service	Services refer to assistance provided to the regulated organisation either internally or externally in ensuring the organizational fulfill their compliance obligations. Services include compliance related services namely audit, assurance and advisory.
Audit	Services undertaken to assess a regulated organisation's adherence to its compliance obligations.
Internal audit	Services undertaken by organisational auditors to assess a regulated organisation's adherence to its compliance obligations.
External audit	Services undertaken by third party or independent auditors to assess a regulated organisation's adherence to its compliance obligations.
Advisory	Guidance provided to facilitate an entity in deciding and implementing a compliance program (initiative). Advisory services may come from the organization (internally acquired) or may be provided by advisory service providers (externally acquired).
Planning	Sets of guidelines and support provided by compliance experts in conducting proper learning and training for a compliance program.
Training	Sets of guidelines and support provided by compliance experts to ease and facilitate the planning of a compliance program.
Assurance	Assistance provided to the regulated organisation to ensure that the provisions of its compliance obligations are being met.

References

Anon, J.,. L., Filowitz, H., & Kovatch, J. M. (2007). Integrating sarbanes-oxley controls into an investment firm governance framework. *The Journal of Investment Compliance*, 8(1), 40–43.

Bace, J., & Rozwell, C. (2006). Understanding the Components of Compliance. *Gartner Research*: Gartner Research, Inc.

Bace, J., Rozwell, C., Feiman, J., & Kirwin, B. (2006). Understanding the Costs of Compliance. *Gartner Research*: Gartner, Inc.

Berente, N., Ivanov, D., & Vandenbosch, B. (2010). Process gatekeepers and compliance with enterprise processes. *Business Process Management Journal*, 16(3), 394–419.

Boella, G., Janssen, M., Hulstijn, J., Humphreys, L., & Torre, L. v. d. (2013). Managing legal interpretation in regulatory compliance. Paper presented at the Proceedings of the Fourteenth International Conference on Artificial Intelligence and Law, Rome, Italy,

Bonner, E., J., O.'. R., & Curran, K. (2011). Implementing the payment card industry (PCI) data security standard (DSS). *Telkomnika*, 9(2), 365–376.

Booch, G., Rumbaugh, J., & Jacobson, I. (2005). *Unified modeling language user guide (2nd ed*. Addison-Wesley Object Technology Series): Addison-Wesley Professional.

Brank, J., Grobelnik, M., & Mladenić, D. (2005) A Survey of Ontology Evaluation Techniques. In *Proceedings of the Conference on Data Mining and Data Warehouses* (*SiKDD 2005*.

Brewster, C., Alani, H., Dasmahapatra, S., & Wilks, Y. (2004) Data Driven Ontology Evaluation. In *Proceedings of International Conference on Language Resources and Evaluation*

Brusa, G., Caliusco, M. L., & Chiotti, O. (2006). *A process for building a domain ontology: An experience in developing a government budgetary ontology*. Hobart, Australia: Paper presented at the Proceedings of the Second Australasian Workshop on Advances in Ontologies.

Burton-Jones, A., Storey, V. C., Sugumaran, V., & Ahluwalia, P. (2005). A semiotic metrics suite for assessing the quality of ontologies. *Data & Knowledge Engineering*, 55(1), 84–102. doi:10.1016/j.datak.2004.11.010.

Butler, T., & McGovern, D. (2012). A conceptual model and IS framework for the design and adoption of environmental compliance management systems. *Information Systems Frontiers*, 14(2), 221–235. doi:10.1007/s10796-009-9197-5.

Buttigieg, P. L., Morrison, N., Smith, B., Mungall, C. J., Lewis, S. E., &, t. E. C. (2013). The environment ontology: contextualising biological and biomedical entities. *Journal of Biomedical Semantics*, 4(43), 1–9.

Caldwell, F. (2008). The enterprise governance, risk and compliance platform defined. *Gartner Research:* Gartner, Inc.

Caldwell, F., & Eid, T. (2008). Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms. *Gartner Research*: Gartner, Inc.

Caldwell, F., & Mogull, R. (2006). Risk management and business performance are compatible. *Gartner Research:* Gartner, Inc.

Casellas, N. (2009). Ontology Evaluation through Usability Measures. In R. Meersman, P. Herrero, & T. Dillon (Eds.), *On the Move to Meaningful Internet Systems*: OTM 2009 Workshops (Vol. 5872, pp. 594–603, Lecture Notes in Computer Science): Springer Berlin/Heidelberg.

Clayton Utz. (2013). *Governance*. Risk and Compliance: Managing Legal Risks in An Integrated Governance, Risk and Compliance Framework.

Coates, J. C. (2007). The goals and promise of the sarbanes-oxley act. *The Journal of Economic Perspectives*, 21, 91–116.

Cohen, J. (1960). A Coefficient of Agreement for Nominal Scales. *Educational and Psychological Measurement*, 20(1), 37–46, doi:10.1177/001316446002000104.

Corcho, O., Fernández-López, M., & Gómez-Pérez, A. (2003). Methodologies, tools and languages for building ontologies. Where is their meeting point? *Data & Knowledge Engineering*, 46(1), 41–64. doi:10.1016/S0169-023X(02)00195-7.

Cozens, J. (2009). Anti-money laundering - practical tips and lessons to be learned. *Keeping Good Companies*, 61(8), 452–453.

Cuaresma, J. C. (2002). The gramm-leach-bliley act. *Berkeley Technology Law Journal*, 17, 497.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. doi:10.2307/249008.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, 35(8), 982–1003. doi:10.1287/mnsc.35.8.982.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1992). Extrinsic and intrinsic motivation to use computers in the Workplace. *Journal of Applied Social Psychology*, *22*(14), 1111–1132. doi:10.1111/j.1559-1816.1992.tb00945.x.

Deloitte (2013). *Enterprise compliance: The risk intelligent approach.* USA: Deloitte Development LLC..

Dividino, R., & Sonntag, D. (2008). *Controlled Ontology Evolution through Semiotic-based Ontology Evaluation.* Paper presented at the Proceedings of the International Workshop on Ontology Dynamics (IWOD), in collaboration with the 7th International Semantic Web Conference (ISWC)},

Dreyfuss, C. (2008). Use IT governance to leverage business objectives and to support compliance requirements. Gartner Research.

Eessaar, E. (2013). On Using a Semiotic Quality Framework to Evaluate the Quality of Conceptual Database Schemas. In T. Sobh, & K. Elleithy (Eds.), *Emerging Trends in Computing, Informatics, Systems Sciences, and Engineering* (Vol. 151, pp. 103–115, Lecture Notes in Electrical Engineering): Springer New York.

EMC (2010). Enterprise governance risk and compliance: a new paradigm to meet new demands. EMC Perspective

Esteban, A. (2009). *Integrated governance, risk and compliance: Enabling transparency, accountability and integrity.* Australia: SAI GLobal Limited.

Fensel, D. (2001). Ontologies. In *Ontologies* (pp. 11–18): Springer Berlin Heidelberg.

Fernández-López, M., & Gómez-Pérez, A. (2002). Overview and analysis of methodologies for building ontologies. *The Knowledge Engineering Review*, *17*(2), 129–156. doi:10.1017/s0269888902000462.

Fernández, M., Gómez-Pérez, A., & Juristo, N. (1997) METHONTOLOGY: From Ontological Art towards Ontological Engineering. In *AAAI97 Spring Symposium Series, Menlo Park, California*, (pp. 33–40)

Frimpong, J. A., & Rivers, P. A. (2006). Health insurance portability and accountability act: blessing or curse? *Journal of Health Care Finance*, *33*(1), 31–39.

Ghanavati, S., Amyot, D., & Peyton, L. (2007). Towards a Framework for Tracking Legal Compliance in Healthcare. In J. Krogstie, A. Opdahl, & G. Sindre (Eds.), *Advanced Information Systems Engineering* (Vol. 4495, pp. 218–232, Lecture Notes in Computer Science): Springer Berlin Heidelberg.

Gómez-Pérez, A., Fernández-López, M., & Corcho, O. (2004). Methodologies and Methods for Building Ontologies. In *Ontological Engineering* (pp. 107–197, Advanced Information and Knowledge Processing): Springer London.

Grimes, G. A. (2007). Compliance with the CAN-SPAM act of 2003. *Communications of the ACM*, *50*(2), 56–62.

Gruber, T. (2009). Ontology. In L. Liu, & M. T. Özsu (Eds.), *Encyclopedia of database systems*. Springer: US.

Grüninger, M., & Fox, M. S. (1995). *Methodology for the Design and Evaluation of Ontologies.* Paper presented at the Workshop on Basic Ontological Issues in Knowledge Sharing: International Joint Conference on Artificial Inteligence (IJCAI95),, Montreal, Canada,

Grüninger, M., & Lee, J. (2002). Ontology application and design: introduction. *Communications of the ACM*, *45*(2), 39–41.

Guarino, N., & Welty, C. A. (2009). An Overview of OntoClean. In S. Staab, & D. Rudi Studer (Eds.), *Handbook on Ontologies* (pp. 201–220, International Handbooks on Information Systems): Springer Berlin Heidelberg.

Guo, T., Schwartz, D. G., Burstein, F., & Linger, H. (2009). Codifying collaborative knowledge: using wikipedia as a basis for automated ontology learning. *Knowledge Management Research and Practice*, *7*(3), 206–217.

Gupta, P. P. (2008). Management's evaluation of internal controls under section 404(a) using the COSO 1992 control framework: evidence

from practice. *International Journal of Disclosure and Governance*, *5*(1), 48–68.

Haghighi, P. D., Burstein, F., Zaslavsky, A., & Arbon, P. (2013). Development and evaluation of ontology for intelligent decision support in medical emergency management for mass gatherings. *Decision Support Systems*, *54*(2), 1192–1204. doi:10.1016/j.dss.2012.11.013.

Hasan, & Stiller, B. (2007). AURIC: A Scalable and Highly Reusable SLA Compliance Auditing Framework. In A. Clemm, L. Granville, & R. Stadler (Eds.), *Managing Virtualization of Networks and Services* (Vol. 4785, pp. 203–215, Lecture Notes in Computer Science): Springer Berlin Heidelberg.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105.

Hoffmann, J., Weber, I., & Governatori, G. (2012). On compliance checking for clausal constraints in annotated process models. *Information Systems Frontiers*, *14*(2), 155–177. doi:10.1007/s10796-009-9179-7.

Horrocks, I., & Patel-Schneider, P. (2011). KR and Reasoning on the Semantic Web: OWL. In J. Domingue, D. Fensel, & J. Hendler (Eds.), *Handbook of Semantic Web Technologies* (pp. 365–398): Springer Berlin Heidelberg.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 54–60. doi:10.1145/1953122.1953142.

Jones, D. M., Bench-Capon, T. J. M., & Visser, P. R. S. (1998) Methodologies for Ontology Development. In *ITi and KNOWS Conference of the 15th IFIP World Computer Congress, Chapman-Hall*, (pp. 62–75)

Kim, H. M., Fox, M. S., & Sengupta, A. (2007). How to Build Enterprise Data Models to Achieve Compliance to Standards or Regulatory Requirements (and share data). *Journal of the Association for Information Systems*, *8*(2), 105–128.

Knight, K., & Luk, S. K. (1994). *Building a Large-Scale Knowledge Base for Machine Translation.* Paper presented at the Proceedings of the Twelfth National Conference on Artificial Intelligence (vol. 1), Seattle, Washington, United States.

KPMG (2005a). The compliance journey: Balancing risk and controls with business improvement. KPMG Advisory.

KPMG (2005b). The compliance journey:Making compliance sustainable. KPMG International.

KPMG (2006). The compliance journey: Leveraging information technology to reduce costs and improve responsiveness. KPMG International.

KPMG (2007). Compliance framework. KPMG International.

KPMG (2008). Understanding and articulating risk appetite. KPMG International.

Lahti, C., Lanza, S., & Peterson, R. (2005). *Sarbanes-oxley IT compliance using COBIT and open source tools*: Syngress publishing.

Leukel, J., & Sugumaran, V. (2009). Towards a semiotic metrics suite for product ontology evaluation. *Intelligent Information Technologies*, *5*(4), 1–15. doi:10.4018/jiit.2009080701.

Lim, S. C. J., Liu, Y., & Lee, W. B. (2011). A methodology for building a semantically annotated multi-faceted ontology for product family modelling. *Advanced Engineering Informatics*, *25*(2), 147–161. doi:10.1016/j.aei.2010.07.005.

Lu, R., Sadiq, S., & Governatori, G. (2008). Measurement of compliance distance in business work practice. *Information Systems Management*, *25*(4), 344–355.

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research*, *2*(3), 173–191. doi:10.1287/isre.2.3.173.

McClure, D., Caldwell, F., & Bittinger, S. (2009). An Overall Risk and Compliance Management Framework for Government Agencies. *Gartner Industry Research* (31 March 2009 ed.): Gartner, Inc.

McCorkell, P. L. (1998). EU data protection directive. *Credit World*, *86*, 5–6.

Mellouli, S., Bouslama, F., & Akande, A. (2010). An ontology for representing financial headline news. *Web Semantic*, *8*(2–3), 203–208. doi:10.1016/j.websem.2010.02.001.

Mitchell, S. L., & Switzer, C. S. (2009). *GRC Capability Model "Red Book" 2.0*: Open Compliance & Ethics Group (OCEG).

Mont, M. C., & Thyne, R. (2008). Privacy policy enforcement in enterprises with identity management solutions. *Journal of Computer Security*, *16*, 133–163. doi:10.1145/1501434.1501465.

Mount, S. (1993). The privacy act 1993. *Auckland University Law Review*, *7*, 408.

Nawoj, A., & Goniak, M. (2004, Ontology development challenges and applications using DARPA agent markup language (DAML). IAnewsletter

Noy, N. F., & McGuinness, D. L. (2001). Ontology Development 101: A Guide to Creating Your First Ontology. *Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880*. Stanford: Stanford University.

OCEG (2011). GRC Technology Solutions Guide Version 2.1. OCEG.

Opdahl, A. L., & Henderson-Sellers, B. (2002). Ontological evaluation of the UML using the bunge–wand–weber model. *Software and Systems Modeling*, *1*(1), 43–67. doi:10.1007/s10270-002-0003-9.

Pacini, C., & Barker, K. (2010). The fair credit reporting act. *The CPA Journal*, *80*, 60–63.

Paredes-Moreno, A., Martínez-López, F. J., & Schwartz, D. G. (2010). A methodology for the semi-automatic creation of data-driven detailed business ontologies. *Information Systems*, *35*(7), 758–773. doi:10.1016/j.is.2010.03.002.

Pershkow, B. I. (2003). Sarbanes-oxley: investment company compliance. *The Journal of Investment Compliance*, *3*(4), 16–30.

Pinto, H. S., Gómez-Pérez, A., & Martins, J. P. (1999). Some Issues on Ontology Integration. In *Proceedings of the IJCAI-99 Workshop on Ontologies and Problem-Solving Methods*

Pinto, H. S., & Martins, J. P. (2001). *A Methodology for Ontology Integration*. Paper presented at the Proceedings of the 1st International Conference on Knowledge Capture, Victoria, British Columbia, Canada,

Pinto, H. S., & Martins, J. P. (2004). Ontologies: how can they be built? *Knowledge and Information Systems*, *6*(4), 441–464. doi:10.1007/s10115-003-0138-1.

Porzel, R., & Malaka, R. (2004) A Task-based Approach for Ontology Evaluation. In *ECAI Workshop on Ontology Learning and Population*, (pp. 7–12)

Protiviti (2013). *Growing with governance, risk and compliance (GRC) solutions: Avoiding common pitfalls to maximize GRC solutions*. United States: Protiviti Inc..

Pulido, J. R. G., Ruiz, M. A. G., Herrera, R., Cabello, E., Legrand, S., & Elliman, D. (2006). Ontology languages for the semantic web: a never completely updated review. *Knowledge-Based Systems*, *19*(7), 489–497. doi:10.1016/j.knosys.2006.04.013.

Recker, J., Indulska, M., Rosemann, M., & Green, P. (2005) Do Process Modelling Techniques Get Better? A Comparative Ontological Analysis of BPMN. In B. Campbell, J. Underwood, & D. Bunker (Eds.), *16th Australasian Conference on Information Systems*, *Sydney, Australia, November 30 - December 2, 2005*

S. Smith, D. Bunker, V. Pang. (2006) Does Agency Size affect IS Security Compliance for E-government? In *The Tenth Pacific Asia Conference on Information Systems* (*PACIS 2006*)

Sadiq, S., Governatori, G., & Naimiri, K. (2007). Modeling Control Objectives for Business Process Compliance. In *5th International Conference on Business Process Management, Brisbane, Australia, Sept 2007 2007*: Springer-Verlag

Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices: how are the fortune 500 handling online privacy disclosures? *Information Management*, *43*, 805–820.

Sekaran, U., & Bougie, R. (2010). *Research methods for business*: *A skill building approach*: John Wiley & sons.

Shanks, G., Tansley, E., Nuredini, J., Tobin, D., & Weber, R. (2008). Representing part-whole relations in conceptual modeling: an empirical evaluation. *MIS Quarterly*, *32*(3), 553–573.

Smith, B., Williams, J., & Steffen, S. K. (2003). The Ontology of the Gene Ontology. In *AMIA Annual Symposium Proceedings*, *2003* (Vol. 2003, pp. 609)

Smith, H. A., & McKeen, J. D. (2006). Developments in practice XXI: IT in the new world of corporate governance reforms. *Communications of the Association FOR Information Systems, Volume 17*, 714-727.

Standards Australia. (2006). *AS 3806:2006 compliance programs. (pp. 25)*. Sydney, Australia: Standards Australia.

Sure, Y., Staab, S., & Studer, R. (2009). Ontology Engineering Methodology. In S. Staab, & D. Rudi Studer (Eds.), *Handbook on Ontologies* (pp. 135–152, International Handbooks on Information Systems): Springer Berlin Heidelberg.

Syed Abdullah, N., Indulska, M., & Sadiq, S. (2009). *A Study of Compliance Management in Information Systems Research*. Paper presented at the The 17th European Conference on Information Systems (ECIS2009), Verona, Italy, 8–10 June

Syed Abdullah, N., Sadiq, S., & Indulska, M. (2010b). Emerging Challenges in Information Systems Research for Regulatory Compliance Management. In B. Pernici (Ed.), *Advanced Information Systems Engineering* (Vol. 6051, pp. 251–265, Lecture Notes in Computer Science): Springer Berlin/Heidelberg.

Syed Abdullah, N., Sadiq, S., & Indulska, M. (2010b). *Information Systems Research*: *Aligning to Industry Challenges in Management of Regulatory Compliance*. Paper presented at the Proceedings of the Pacific Asia Conference on Information Systems Engineering (PACIS 2010a), Taipei, Taiwan,

Syed Abdullah, N., Sadiq, S., & Indulska, M. (2011). *A Framework for Industry-Relevant Ontology Development*. Paper presented at the Proceedings of the 22nd Australasian Conference on Information Systems (ACIS 2011), Sydney, Australia, 29 November - 2 December 2011

Tan, Y.-H., & Thoen, W. (2000). INCAS: a legal expert system for contract terms in electronic commerce. *Decision Support Systems*, *29*(4), 389–411. doi:10.1016/S0167-9236(00)00085-3.

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: a test of competing models. *Information Systems Research*, *6*(2), 144–176. doi:10.1287/isre.6.2.144.

Uschold, M. (1996). Building Ontologies: Towards a Unified Methodology. In *16th Annual Conf. of the British Computer Society Specialist Group on Expert Systems*, *1996 1996*. doi: citeulike-article-id:1244396.

Uschold, M., & King, M. (1995). *Towards a Methodology for Building Ontologies*. Paper presented at the Workshop on Basic Ontological Issues in Knowledge Sharing, held in conduction with IJCAI-95, Montreal, Canada,

Velardi, P., Missikoff, M., & Basili, R. (2001). *Identification of relevant terms to support the construction of domain ontologies*. Toulouse, France: Paper presented at the Proceedings of the Workshop on Human Language Technology and Knowledge Management.

Venkatesh, V. (2000). Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research*, *11*(4), 342–365. doi:10.1287/isre.11.4.342.11872.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*, 273–315. doi:10.1111/j.1540-5915.2008.00192.x.

Viera, A. J., & Garrett, J. M. (2005). Understanding interobserver agreement: the kappa statistic. *Family Medicine*, *37*(5), 360–363.

Volonino, L. (2003). Electronic evidence and computer forensics. *Communications of the Association for Information Systems*, *12*, 457–468.

W3C OWL Working Group (2009). OWL 2 Web Ontology Language - Document Overview. (Recommendation REC-owl2-overview-20091027 ed.): World Wide Web Consortium.

Wand, Y., & Weber, R. (1995). On the deep structure of information systems. *Information Systems Journal, 5*(3), 203–223. doi:10.1111/j.1365-2575.1995.tb00108.x.

Weber, R. (1997). *Ontological foundations of information systems*. Melbourne, Australia: Coopers & Lybrand and the Accounting Association of Australia and New Zealand.

WenJun, W., CunXiang, D., & Peng, Y. (2009). *Ontology Modeling of Emergency Plan Systems.* Paper presented at the Proceedings of the 6th International Conference on Fuzzy Systems and Knowledge Discovery - Volume 2, Tianjin, China.

Wenk, M. S. (2005). Interrelationships between BS 7750 and the EMAS Program. In *The European Union's Eco-Management and Audit Scheme* (*EMAS*) (Vol. 16, pp. 5–8, Eco-Efficiency in Industry and Science): Springer Netherlands.

Williams, B. J., & King, M. S. (2004). Implementing Voting Systems: The Georgia Method. *Communications of the ACM, 47*(10), 39–42.

Wood, J. M. (2007). Understanding and computing Cohen's kappa: a tutorial. WebPsychEmpiricist

Yang, D., Miao, R., Wu, H., & Zhou, Y. (2009). Product configuration knowledge modeling using Ontology Web Language. *Expert Systems with Applications, 36*(3, Part 1), 4399–4411. doi:10.1016/j.eswa.2008.05.026.

Yin, R. K. (2009). *Case study research: Design and methods.* (Fourth ed.,). California: SAGE Publications.

Zeshan, F., & Mohamad, R. (2012). Medical ontology in the dynamic healthcare environment. Procedia Computer Science, 10(0), 340–348, doi:10.1016/j.procs.2012.06.045.

Norris Syed Abdullah is a Senior Lecturer in Information Systems at Faculty of Computing, Universiti Teknologi Malaysia. He received his PhD in Information Systems from the University of Queensland. His research interests include governance risk and compliance, ontology engineering, business intelligence, and information systems planning. He has published his works on reputable Information Systems conferences such as Australasian Conference on Information Systems (ACIS), European Conference on Information Systems (ECIS), Pacific Asia Conference on Information Systems (PACIS), and Conference on Advanced Information Systems Engineering (CAiSE).

Marta Indulska is an Associate Professor and Head of the Business Information Systems group at the UQ Business School, The University of Queensland, Australia. Her research interests include conceptual modelling, business process management, compliance and innovation. She has published over 60 fully refereed articles in internationally recognised journals and conferences, with her work appearing in journals such as MIS Quarterly, European Journal of Information Systems, Journal of the Association for Information Systems, Decision Support Systems, Information Systems, among others. Her work has also been published in numerous conferences, including ICIS, BPM, ER and CAiSE.

Shazia Sadiq is Professor of Computer Science at the School of Information Technology and Electrical Engineering, The University of Queensland, Brisbane, Australia. Her main research interests include business process management, risk and compliance modeling, and information quality and use. She has published over 100 peer-reviewed publications in journals such Information Systems Journal, VLDBJ, TKDE, as well as major conferences such as SIGMOD, ICDE, ER, BPM, ICIS and CAiSE.