# A High-Level Ontology for a Software Development Compliance Framework

**Research** · July 2015

DOI: 10.13140/RG.2.1.2595.1843

Shadi Zarrabi
University of East London
**4** PUBLICATIONS **0** CITATIONS

# A High-Level Scheme for an Ontology-based compliance Framework in Software Development

Ftemeh Zarrabi Jorshari
School of Architecture, Computing And Engineering
University Of East London
London, United Kingdom
Shadi.zr77@gmail.com

Dr Rahman H Tawil
School of Architecture, Computing And Engineering
University Of East London
London, United Kingdom
a.r.Tawil@uel.ac.uk

*Abstract*— **Software development market is currently witnessing an increasing demand for software applications conformance with the international regime of GRC for Governance, Risk and Compliance. In this paper, we propose a compliance requirement analysis method for early stages of software development based on a semantically-rich model, where a mapping can be established from legal and regulatory requirements relevant to system context to software system business goals and contexts. The proposed semantic model consists of a number of ontologies each corresponding to a knowledge component within the developed framework of our approach. Each ontology is a thesaurus of concepts in the compliance and risk assessment domain related to system development along with relationships and rules between concepts that compromise the domain knowledge. The main contribution of the work presented in this paper is a case study that demonstrates how description-logic reasoning techniques can be used to simulate legal reasoning requirements employed by legal professions against the description of each ontology.**

***Keywords-*** ***Ontology, Requirement Engineeering, Compliance, Risk, Data protection, Security, Privacy, Standard***

.

## I. Introduction

Legal Compliance is a term that is generally used for any procedure that organisations take in order to ensure they follow relevant laws, regulations and business rules and standards in their functions and understand and adhere to ethical codes within their profession. Answering such requirements, particularly after the financial crisis of 2007-2008 0 and the resulting likely regulating climate, industries recognised the need to develop new frameworks and clear processes in order to improve the legal compliance and a new regime called Legal Governance, Risk Management and Compliance (LGRC). LGRC is a key issue in Information Technology [5]. Although previous research specifically concentrates on the matter of compliance, more recent research such as [4], [5], and including the current paper, has demonstrated the inseparable nature of concepts of compliance and risk. According to OCEG, compliance has been defined to adhere to legal and policies [5]. However, from a different perspective, Well-defined compliance approaches should also be augmented by an assessment of risk management in order to safeguard the objectives of laws, regulations and policies from aligned risks. In situations where even a few of the elements of GRC are being overlooked or researched in isolation, new research is required in the study of compliance as an integrated concept in the area of software development. In sum, a comprehensive and scientific approach is needed to integrate a number of objectives, and bring together their advantages, in the process of compliance, see Table1. We have chosen the notion of a framework as the optimal model through which to address these issues. A framework is a layered structure consisting of a set of subsystems or components, each performing part of the entire intended process and interrelating components through the output of other components. During the entire framework process, links between the components perform the role of mapping and component integration. Each component also has a number of integrated concepts. In order to provide a platform representing both conceptual and application models of the proposed framework, we needed an approach that could provide both semantic and syntactic aspects of our model along with the relations between elements of the framework. This could all be found in the definition and application of ontology in computer science. Considering the philosophical connotation of the word "ontology" [21], it is being used here to indicate the categories and different components within the universe of the proposed framework, plus sufficient information regarding the concepts and relationships of each component and the components together. Later, the ontology model will be used for a computer application of the framework, which helps users to automatically obtain and retrieve compliance and requirement knowledge from its repository. Furthermore users of the application can retrieve software development and compliance knowledge depending on the state of system development and type of system.

The remainder of this paper is organized as follows: Section 2 introduces an overall picture of the framework, its components, concepts and links and examines the application of the ontology-based approach of the framework using a real case study from e-commerce business. Section 3 evaluates the output by comparing the framework to the elements of OCEG GRC Capability Model [5]. Section 4 discusses the related works to the area of this research and section 5 concludes the paper and introduces future works.

TABLE 1. ADVANTAGES & OBJECTIVES OF COMPLIANCE FRAMEWORK

| Objective | comments |
|---|---|
| Provide a repository of compliance knowledge using Ontology-Semantic web | • Implement a compliance framework as a knowledge repository to automatically retrieve, add or change information on compliance knowledge and system requirements<br>• Categorise and interrelate different components of the framework as well as their concepts and objects<br>• Perform legal reasoning to apply laws, regulations and policies to the scope of the developing system using semantic ontology reasoning infrastructures<br>• Provide awareness, education and ongoing support to users regarding the process of compliance through the communication service of the semantic web site<br>• Being able to easily adhere to changes in laws and legal documents |
| Consider compliance as a critical requirement in Requirement Engineering stage of software development | • Start compliance from early stages of system development<br>• Extract requirements from laws, regulations and policies<br>• Categorize requirements using ontology taxonomy<br>• Check requirement consistency by analysing requirements from different stakeholders using<br>• Trace requirements by identifying requirement dependencies, refining high-level requirements to application level |
| Perform an easy process of Law Analysis | • Resolve the ambiguity of legal language for software developers<br>• Perform a legal reasoning task following similar procedures to legal professions |
| Perform a Compliance process including different elements of compliance | • Apply relevant laws, regulation and internal and external policies to the scope of developing system<br>• Coverage and integration of different resources of compliance such as laws, guidelines and standards and the ability to refine them together in a hierarchical order |
| Perform Risk analysis against legal and security objectives of system | • Address constraint and risk against compliance objectives |
| Address system Design | • Perform early stages of system design using design patterns |

## II. Summarized Layout of the Compliance Framework Ontology

The current stage of the proposed approach has provided a series of successful approximations to the process of compliance in software development. These are discussed in terms of objectives and advantages in the context of the proposed framework, as seen in Table1.

Also Figure 1 depicts a top-level model of the proposed Compliance Framework along with its components and their relationships. Each component of the framework corresponds with one of the objectives from Table 1 and is accompanied by a number of sub-components. Accordingly the components of our compliance framework can be defined separately using separate ontologies. In an ontology, knowledge about a domain is modelled using a knowledge representation language with a reasoning mechanism. The knowledge representation languages such as RDF and OWL are used to create a set of terms as well as to specify classes, properties and relationships between classes and objects in the domain [18]. The basic building block of these languages is triples of *subject-predicate-object* which is called a statement. This is being represented as a relationship between two classes in the knowledge domain *(class-objectProperty-class).*

The general categorization of the framework ontology is based on a primary breakdown of:

1. ontology: framework components and their classes (physical things that remain static with time)

2. Outer-links: mapping between sub-ontologies (logical reasoning that evolves over time)

3. Inner-links: ontological properties (relationships between concepts that change with time)

4. Instances: Ontological individuals (physical things that change with time)

The following sub-sections specify the definitions of each ontology in our framework, along with their concepts, their relationships (Inner-links) and rules (inner or outer links), as the secondary structure of the framework, which is superimposed over the primary model of Figure 1. To summarize, each ontology can be represented as classes and properties implemented in the RDF language.

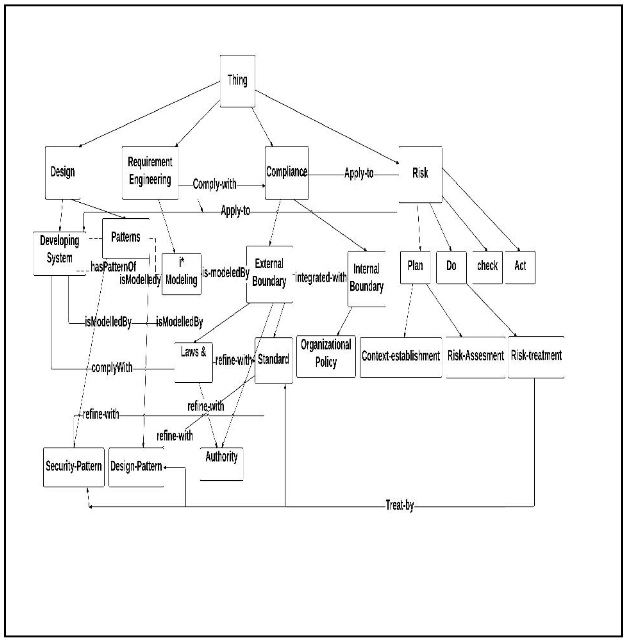
Ontology-System= (Con, Rel, Rules) (1)

Rel: a set of relationships

Con: a set of concepts

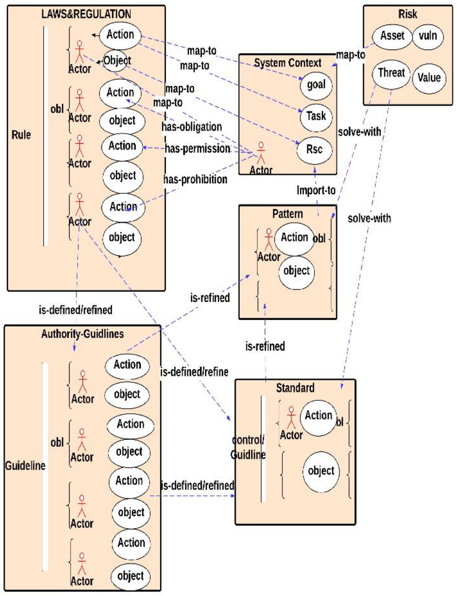
Rules: a set of interface rules

FIG. 1. . COMPLIANCE FRAMEWORK TOP LEVEL TAXONOMY



We are representing the processes involved in our compliance model in Fig2. According to figure 2, there exists a central element in each law or regulation called a rule which is the statement of law. A rule consists of two parts of fact; the condition or circumstances where the law apply, and the right which the rule impose to its stakeholder. Right can be Obligation, Permission or prohibition. Since a rule of law is directly taken from the law's document, facts and rights consist of simple or complex sentences. To analyse complex legal documents a Natural Language processing technique is also used here to parse facts and conclusion to elements of Actor, Action and Object. Based on a similar task of lawyers and legal professions and in order to comply system development with related rule of law, the right of law is applicable where the conditions and circumstances (facts) exist. To simulate this task in our framework, facts of law should be found and mapped to the system context and rights be applied in same context. This is shown in Fig2 by dashed lines labelled map-to The context of system is modelled in our framework using another component called i* modelling language and its concepts Actor, Goal, Task and Resource. I* is a modelling language suitable for early stage of system development and representing social dependency of system stakeholders 0. Parsed elements of fact of law should be found and mapped to mentioned system element and, rights of law to be applied to the system. Legal terms of law are also defined and refined to more detailed requirements by components of compliance such as authority guidelines or by standards. Regarding the textual nature of standards, they also consist of same elements of fact, obligation, permission and prohibition and parsed elements of actor, action and object. In same manner standards and guidelines are refined by application level requirements from another component called patterns. Patterns are solution to software problems repeating over time which can be specified to a special area such as security or web development and etc. as it was discussed, we can see how the compliance task is performed through a hierarchy process based on the abstraction level of the resources of compliance from laws, to standards and guidelines and design level patterns.

FIG 2.  COMPLIANCE FRAMEWORK PROCESS



## A. *i* Ontology*

i* modelling language is an agent-oriented and goal-modelling approach to the early stages of requirement engineering. Social relationships and the strategic interests of agents are modelled in i* in the context of their interdependencies 0. A goal dependency is the highest level of an agent desire. A goal may be soft or hard, depending on whether it indicates a functional or non-functional requirement of the agent. At the refinement stage, an agent may adopt task dependency or resource dependency in order to satisfy its goal or task. Other tasks, goals and resources may also decompose a task. In such a systematic approach that utilizes concepts of Actor, Goal, Task and Resource, the requirement engineer is able to progress through an incremental process of system requirements. Table 2 represents part of the taxonomy of i* as it is developed as a component of our compliance framework in the platform of ontology. They are written in RDF; official language of ontology. The primitives in the category hieratically include *actor*, *goal*, *task, resource* and *system* concepts. The children categories of goal entity as *soft-goal* and *hard-goal* share common characteristics but are otherwise heterogeneous. . Different types of dependencies between i* concepts are drawn as object properties which relates types of classes. Refinement levels of goal and task (means-end, decompose) are also available as properties. In run time situation each of the classes should be instanced by individuals from system context. Regarding no further relationship on mentioned properties, we do not have ontology rules in i* ontology..

TABLE2. i* ONTOLOGY

| CLASS | PROPERTY |
|---|---|
| (1) <rdfs: Class rdf:id= "Actor"><br><rdfs: Subclassof rdf:resource="i*/><br></rdf: Class><br>(2) <rdfs:Class rdf:id= "Goal"><br><rdfs:Subclassof rdf:resource=i*/><br></rdfs:Class><br>(3) <rdfs:Class rdf:id="Soft-goal"><br><rdfs:SubClassOf rdf:resource: "Goal"/><br></rdf:Class><br>(4) <rdf:Class rdf:id="Hard-goal"><br><rdf:SubClassof<br>rdf:resource= "Goal"/><br></rdf:Class> | (5) <rdfs:Property rdf:id="has-<br>GoalDependencyOf"><br><rdfs:domain rdf:resource="Actor"><br><rdfs:range rdf:resource="Goal"><br></rdfs:Property><br>(6) <rdfs:Property rdf:id="has-<br>TaskDependencyOf"><br><rdfs:domain rdf:resource="Actor"><br><rdfs:range rdf:resource="Task"><br></rdfs:Property><br>(7)<rdfs:Property rdf:id="has-ResorceDependencyOf"> |

We are giving scenarios from an e-commerce system to illustrate how i* ontology works. ESilver is a jewelry tailor company aiming to have an e-commerce website in order to sell its products. Having the system context and i* concepts number of ESilver's goals and tasks and resource are modelled in ontology as followings:

- *ESilver has a goal to sell its products* :
  *has-GoalDependencyOf (ESilver-Company, Selling-products)*

- *ESilver client has goal to shop online:*
  *has-GoalDependencyOf ( ESilver-Client , shop-online)*

- *ESilver has task to browse its products:*
  *has-TaskDependencyOf (ESilver-Company , browsing-products*

- *ESilver ecommerce system has type of E-Commerce developing system:*
  *has-TypeOf (ESilver-ecommerce, E-Commerce)*

- *ESilver has the task to collet personal data from clients:*
  *has-TaskDependencyOf (ESilver-Company, collecting-personalData)*

### *B. Developing System Ontology*

This is the ontology and component of our framework representing the categorisation of different types of software systems that a developer may wish to create. Each category and sub-category of system types is represented with classes and sub-classes in the ontology. Having systems in different categorisations makes it easy and economical to find the type of related law to be complied with each system. Also the relationship of systems to pattern ontology makes it easy for developer to find solutions for its requirements or find further requirements provided to the problems in patterns. Following the requirements founded in i* methodology from ESilver scenario, further design and legal knowledge are obtained from Developing system ontology as following. As shown the rules in ontology have lead the development to the consideration of number of User Interface Patterns in order to refine requirements of an ecommerce system, also have found Data Protection Regulation as a related resource of compliance for ecommerce system:

- *has-PatternOf ( E Silver-ecommerce, shopping-Card)*

- *has-PatternOf ( ESilver-ecommerce, item-catalogue)*

- *comply-with (ESilver-ecommerce, Data-Protection -Regulation)*

- *has-PatternOf (ESilver-ecommerce, Form)*

### *C. Laws & Regulation Ontology*

Laws and regulations as a sub-component of *External Boundary,* is being represented here as the other component of the compliance framework in the context of its ontology; the skeleton of our framework. We have employed a technique similar to that used by lawyers to analyse laws, together with an NLP technique to extract legal concepts from legal documents as explained before. This is in order to identify concepts of the legal ontology and their interrelationships and apply laws to the context of the developing system. The ontology has been practiced on the analysis and application of Data Protection Regulation 2012. A number of legal ontology concepts are related to the structure of legal documents in general, including subject of Law, chapters, articles, rules and territory. Others are specified to elements of rules. Categorisation of these elements is based on the lawyers' tasks, in which they divide a rule of law to two parts of:

*Fact:* the criteria where the law applies;
*Conclusion:* the type of right which the law implies to its stakeholder. Right in law may indicate an obligation, permission or prohibition. Fact and Right are each part of a rule text, which in most cases takes the form of a complete sentence; In other words, each is a statement. Statements are ontologically represented in a binary format indicating a relationship between two elements (e.g., *Link(x, y)).* Thus, Fact and Right are discussed in our ontology as a relationship between certain classes. This is NLP technique that identifies the classes of law including *Legal-actor, action and object* and also convert complex sentences such as the one with modifiers to binary format consisting only of the aforementioned atomic elements. Mentioned classes are common classes of Law ontology. The sub-categorisation of each of these classes depends on the type of law. For example sub-classes of class Actor are controller, data-processor, data-subject and others in case of Data Protection Regulation. Table 3 represents number of classes of this ontology and their object-properties in context of RDF language.

To practice the application of Data Protection Regulation to the context of ESilver ecommerce system development, and using the rules and properties in the legal ontology we have the following statements. Individuals and samples from system context which correspond to the facts from Law& Regulatory ontology, and the ontological reasoner conclude number of obligations from legal rule as shown below:

- *collect (ESilver-Company, personal-Data)*

*->is-obligatedTo-ProcessFairly (ESilver-Company, personal-data)*

- *collect (ESilver-Company, personal-Data)*

*->is-obligatedTo-implement (ESilver-Company, Secure-measures)*

TABLE3. LAW & REGULATION ONTOLOGY

| CLASS | PROPERTY |
|---|---|
| (1) <rdfs: Class rdf:id= “Law-By-Subject”><br><rdfs: Subclassof rdf:resource=”Laws&Regulation”/><br></rdfs><br>(2) </rdfs: Class rdf:id= “IT-Law”><br><rdfs: Subclassof rdf:resource=”Law-By-Subject”/><br></rdfs><br>(3) </rdfs: Class rdf:id= “Computer-Law”><br><rdfs: Subclassof rdf:resource=”Laws-By-Subject”/><br>(4) <rdfs: | (5) <rdfs:Property rdf:id=”has-TerritoryOf”><br><rdfs:domain=”Law-By-Subject”><br><rdfs:range=”Territory”><br></rdfs:Property><br>(6) <rdfs:Property rdf:id=”has-ChapterOf”><br><rdfs:domain=”Law-By-Subject”><br><rdfs:range=”Chapter”><br></rdfs:Property><br>(7) <rdfs:Property rdf:id=”has-ArticleOf”><br><rdfs:domain=”Law-By-Subject”><br><rdfs:range=”Territory”><br></rdfs:Property> |

As illustrated above, the fact that Esilver Company collects personal data of its customer, results to its obligation to process the personal data fairly and to implement secure measures. This is based on Article 2 and 30 from Data Protection Regulation as following which each consist of number of classes in Law and regulation ontology:

*2-Personal data must be:*

*(a) processed lawfully, fairly and in a transparent manner in relation to the data subject*;

30- *The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.*

## *D. Authority Guideline Ontology*

The types of relationships defined on our ontology, automatically follow the life cycle of our framework and lead the user to the ontology of Authority Guide-lines strait after Legal ontology. This is done in order to define and refine legal concepts. The specific ontology being used here for Data Protection Regulation is ICO, the Information Commissioner’s Office guidelines for data protection and privacy issues 0. The space and limit of this paper omits us from providing detail of all concepts and relationship of this ontology. In summarize the ontology consist of classes, binary relationships and further rules taken from guidelines documents of ICO. The same NLP technique has been employed here to extract fact and conclusions from guideline texts and the same analysing technique will be used to apply the guidelines to the system context. An implementing example from ESilver Company helps in better understanding of this ontology. As mentioned before, ICO has defined and refined data protection law’s concepts such as *process-fairly*. Based on below rule taken from ICO guidelines, whenever a Data-Processor has the obligation to Process the personal data fairly, he/she also has the obligation to provide a Privacy notice:

- *is-obligatedTo-ProcessFairly (ESilver-Company, personal-data), Process-PersonalDataOf(ESilver-Company, Customer) -> Is-ObligatedTo-providePrivacynotice-To (Esilver-Company, Customer,)*

## *E. Risk Ontology*

In order to correspond to risk element of GRC, risk analysis is considered as a separate component in the framework. Risk analysis may have different purposes, such as Information Security Management System (ISMS), Legal Compliance, Business Plan or Incidence Response Plan. In order to identify risk ontology's concepts and their relationships, we selected the ISO27005 standard as our approach to Risk management. Risk analysis classes of risk ontology, and the relationship between them, are categorised here based on the different stages and activities of risk analysis defined by ISO27005. The top-level components of risk ontology are the four basic phases of risk management in ISO27005: Plan, Do, Check, Act. The second level of concepts is based on the activities in each of the mentioned stages. The main classes of risk ontology belong to *Context Establishment, Risk Analysis* and *Risk Treatment (*FIG 1) activities. The criteria of risk analysis are identified in context establishment activity. Elements of Risk analysis such as assets, threats and vulnerabilities, and their values are recognized and evaluated based on the criteria of risk analysis. Treatment controls are identified in order to fix vulnerabilities. To prioritise and evaluate risks and the related controls, different approaches to risk analysis are available. The elements of risk analysis (asset, threat, vulnerability) and the criteria (financial, regulatory,…) have been engaged as classes of risk ontology and each have number of sub-classes based on their categorisations in ISO27005. The management approaches to risk analysis are implemented in the context of the rules in ontology, and reasoning technique in ontology makes risk-prioritising decisions.

As a starting point in risk analysis ontology, basic criteria of system are recognized and individuals are given from system context. In next stage, assets of system will be identified from modelled system context and their related threats and vulnerabilities are found using property of *has-threatOf(Asset, Threat)* and *has-vulnerabilityOf(Asset, Vulnerability)* or *is-exploidBy(threat, vulnerability).* Based on elements of basic criteria, values are assigned to classes of *assets, threat-likelihood* and *vulnerability-Ease.* At the final stage level of risks are calculated based on some available formulas from ISO 27005. If the risk is not in an accepted level, then treatment controls are taken to fix vulnerabilities and avoid threat by properties of *has-ControlOf(threat, control), has-ControlOf (vulnerability, control).* The latest relationship is a type of outer-link relationship which connects Risk ontology to Standard and pattern ontologies as another solution to fix risks. Risk assessment formulas are performed by number of rules in ontology such as following:

- *Has-quantitativeValueOf(Customer-data,, 4), is-threatenedBy-threatOf(Customer-data, data-corruption), has-vulnerabilityOf(data-corruption, applying-wrongData), has-likelihoodOf(data-corruption, medium), has-EaseOfExploitionOf applying-wrongData,,medium) -> has-RiskValueOf( Customer-data, 5)*

- *Has-threatOf(Customer-Data, Data-Corruption) ->Has-controlOf(Data-Corruption, evaluate-data)*

TABLE 4. RISK ONTOLOGY

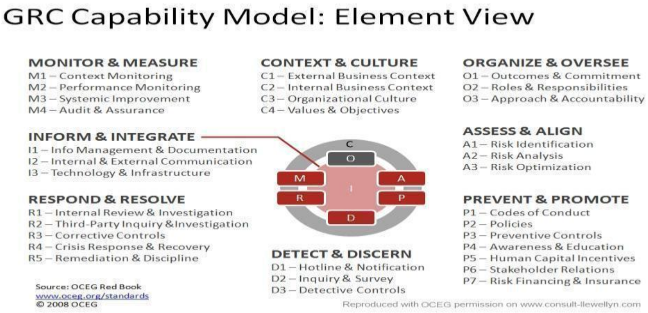
| CLASS | PROPERTY |
|---|---|
| (1) <rdfs:Class rdf:id"Purpose"><br><rdfs:subClassOf<br>rdf:resource="Risk"/><br></rdfs:Class><br><br>(2) <rdfs:Class rdf:about="Legal-Compliance"><br><rdfs:subClassOf<br>rdf:resource="Purpose"/><br></rdfs:Class<br><br>(3) <rdfs:Class<br>rdf:about="Context"><br><rdfs:subClassOf<br>rdf:resource="Risk"/><br></rdfs:Class><br>(4) <rdfs:Class rdf:about="Basic-Criteria"> <rdfs:subClassOf rdf:resource="staffMember"/> </rdfs:Class> | (5) <rdfs:Propertys<br>rdf:about=" has-BasicCriteriaOf"><br><rdfs:domain= Asset<br>rdf:range="Basic-Criteria"/><br></rdfs:Property><br><br>(6) <rdfs:Propertys rdf:about=<br>"has-assetOf>"><br><br><rdfs:domain=”Scope&Boundary”<br>rdf:range="Asset"/><br></rdfs:Property |
| | |

## III. EVALUATION

### A. OCEG Capability Model

We opted to evaluate our proposed compliance framework with the Capability Model from OCEG. The GRC Capability Model from OCEG provides the key components, elements and practices that must be implemented in order to realize a high-performing GRC. Here, we compare the objectives and advantages of our proposed framework from Table 1, along with its components and activities, with eight universal outcomes and eight integrated components of the OCEG model, plus their participant principles, practices, requirements and technology modules. Although not all of the OCEG components will be evaluated here regarding the absent of Governance in our model. Components of our framework that satisfy the outcomes and elements of OCEG referenced capability model are flagged with a sign of each corresponding OCEG outcome and element in Figure 6.2. Figure 6.1, "the GRC Capability Model Elements View" [5], represents the principles and related elements of the model.

Figure6.1. GRC Capability Model: Element View



GRC Capability Model: Element View

MONITOR & MEASURE
M1 – Context Monitoring
M2 – Performance Monitoring
M3 – Systemic Improvement
M4 – Audit & Assurance

CONTEXT & CULTURE
C1 – External Business Context
C2 – Internal Business Context
C3 – Organizational Culture
C4 – Values & Objectives

ORGANIZE & OVERSEE
O1 – Outcomes & Commitment
O2 – Roles & Responsibilities
O3 – Approach & Accountability

INFORM & INTEGRATE
I1 – Info Management & Documentation
I2 – Internal & External Communication
I3 – Technology & Infrastructure

ASSESS & ALIGN
A1 – Risk Identification
A2 – Risk Analysis
A3 – Risk Optimization

RESPOND & RESOLVE
R1 – Internal Review & Investigation
R2 – Third-Party Inquiry &Investigation
R3 – Corrective Controls
R4 – Crisis Response & Recovery
R5 – Remediation & Discipline

PREVENT & PROMOTE
P1 – Codes of Conduct
P2 – Policies
P3 – Preventive Controls
P4 – Awareness & Education
P5 – Human Capital Incentives
P6 – Stakeholder Relations
P7 – Risk Financing & Insurance

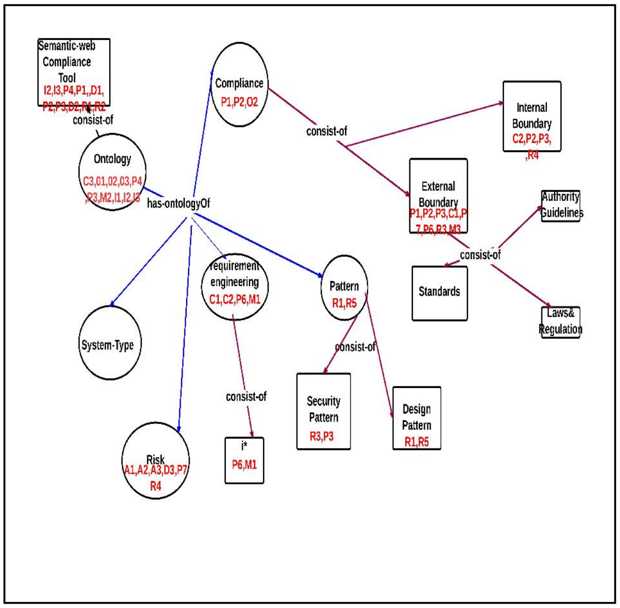
DETECT & DISCERN
D1 – Hotline & Notification
D2 – Inquiry & Survey
D3 – Detective Controls

Source: OCEG Red Book
www.oceg.org/standards
© 2008 OCEG

Reproduced with OCEG permission on www.consult-llewellyn.com

For example, the *Compliance Semantic-web* (the skeleton of our framework) is flagged with the sign of *Awareness & Education* (P4), as it provides knowledge of compliance and educates users through the progress of the proposed compliance process. Other components are flagged in similar process.

Figure6.2. Evaluating the Compliance Framework with OCEG Capability Model



## IV. RELATED WORKS

This section presents related works on compliance in information system development. The literature review is divided into three types of works. First are those that address compliance approaches as a general solution. Second are the works with compliance approaches within the field of information system development. The third type of works is those focusing on ontology techniques within the legal domain. Authors in [4] and [5] provide general solutions for compliance as whole. [2], [3], [8] and [17] give compliance solutions to ISO standards to guarantee the quality assurance of organizations. In recent years, a large body of works have approached compliance as an early requirement of system and, therefore, align requirement engineering with compliance techniques. They mostly used goal-oriented methodologies of requirement engineering, taking law's rights as goal of systems to be satisfied. [7], [10], [12], [13], [15] are sample of these works. Techniques of analysing and extracting rights from legal texts have been also researched by [11]. Using semantic webs and developing ontology of legal concepts is also a well-known approach in the field of artificial intelligence. [16] has delivered a series of works providing legal ontology solutions for legal specialists. They have identified rich legal concepts in their taxonomies. [2], [9], [25], [26] and [8] also propose ontology and semantic web as solution for compliance. We believe that compliance is not an isolated matter and that the GRC regime should be considered as a united and integrated concept. Compliance is strong when it is aligned with elements of risk within a comprehensive framework, also when it covers all possible elements of compliance regarding laws and policies. The aforementioned works also guided us in finding the other components of our framework.

## V. CONCLUSION

This paper has outlined the high level structure of compliance framework ontology. It shows how integration of elements of GRC in ontology platform and the interrelation of their concepts can be used to model a developing system and apply relevant elements of governance to the system context and also perform risk analysis to sys-tem context and compliance. Each component of the compliance framework in con-text of its ontological concepts has been separately discussed with number of its critical and high-level classes and properties. The paper shows how ontological reasoning techniques are used to apply laws to individual instances from modelled sys-tem context, and refine laws by other governance resources and also by corresponding patterns. System resources are risk evaluated against possible vulnerabilities and threats and treat with controls from standards and patterns. Legal reasoning techniques also have been used to model risk assessment approaches. Finally the proposed framework was evaluated with elements and practices of OCEG Capability Model and its consistency and comprehensively has been proved. More works in future can be focused on finding more detailed concepts from other laws and also make compliance between different laws.

## REFERENCES

[1] H.D. Young, D. Gark, L. Jia,. "Experiences in the Logical Specification of the HIPAA and GLBA Privacy Laws." WPES '10 Proceedings of the 9th annual ACM Workshop on Privacy in the Electronic Society

[2] S. Fenz, G. Goluch, A. Ekelhart, B. Riedl,. "Information Security Fortification by Ontological Mapping of ISO/IEC 27001 Standard. Dependable Computing" 2007. PRDC 2007. 13th Pacific Rim International Symposium on

[3]M.S. Saleh,; A. Alrabiah, S.H. Backry. "A STOPE Model for the Investigation of Com-pliance with ISO 17799-2005″, Information Management & Computer Security, Vol. 15 Iss: 4, pp.283 – 294

[4]P. Vicent, M.M. Silva. "A Conceptual Model for Integrated Governance, Risk and Compliance". Advanced Information Systems Engineering.

[5] Open Compliance & Ethics Group (OCEG). "GRC Capability Model "Red Book" *2.0.* OCEG Publication. April 2009.

[6] H. Poor. "An Introduction to Signal Detection and Estimation." New York: Springer-Verlag, 1985, ch. 4.

[7] SH. Islam, H. Mouratidis, S Wagner. "Toward a Framework to Elicit and Manage Security and Privacy Requirements from Laws and Regulations." Journal of Systems and Software Volume 86, Issue 9

[8] H. Susanto, F.B Mulhaya; M.N. Almunawar, Y.C. Tuan, "Refinement of Strategy and Technology Domains, STOPE View on ISO 27001"

[9]A. Gangemi, A Prisco, M.T. Sagri, G. Steve." Some Ontological Tools to Support Legal Regulatory Compliance, with a Case Study" 2003

[10]S. Ghanavati,; D. Amyot, L Peyton. "Toward a Framework for Tracking Legal Compliance in Healthcare." Lecturer Notes in Computer Science Volume4495 2007

[11]TD. Breaux, ,; A. Anton,; E.H. Spafford, "A Distributed Requirement Management Framework for Legal Compliance and Accountability"

[12]SH. Islam,; H. Mouratidis,; I .Jurjense,. "A Framework to Support Alignment of Se-cure System Engineering with Legal Requirements"

[13]T.M. Tyler, "Compliance with Intellectual Property Laws: A Sociological Perspective."

[14]Siena, A; Mylopoulos, J. ; Perini, A. From Laws To Requirements. Requirement Engineering and Law. RELAW. 2008

[15]A. Shamsaei,; D. Amyot,; A. Pourshahid, "A Systematic Review Of Compliance Measurements Based on Goals and Indicators." Lecture Notes in Business Information Processing Volume 83, 2011, pp 228-237

[16]V.R. Benjamin,; P. Casanovas,; J. Breuker, A. Gangemi, "Law and the Semantic Web, an Introduction". Lecture Notes in Computer Science Volume 3369, 2005, pp 1- 17

[17]H. Susanto,; M.N. Almunavar,; Y.CH. Tuan. "Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Redness Level"

[18]E. Yu, P Giorgini,; N. Maider.; P. Mylopoulos. "Social Modeling for Requirement Engineering". Cambridge, MA:MIT Press. 2011

[19]European Commission. PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Brussels, 2012

[20]Kirpatrick, G. The Corporate Governance Lessons from the Financial Crisis. OECD Publication. Vol 2009/1

[21]Gruber, T.R. "Toward Principle for the Design of Ontologies Used for Knowledge Study". Computer. Stud. 43(5-6) [illegible]

[22]E.S. Yu. "Social Modelling and i*. Conceptual Modeling: Foundations and Applications". Lecture Notes in Computer Science Volume 5600, 2009, pp 99-121

[23]E. Yu, P. Giorgini,; N. Maider. P. Mylopoulos. "Social Modeling for Requirement Engineering". Cambridge, MA:MIT Press. 2011

[24]ICO (Information Commissioner Officer). Guide to Data Protection. https://ico.org.uk/for-organisations/guide-to-data-protection/

[25]R. Schmidt, CH.Bartch, R. Oberhauser. "Ontology Based Representation of Compliance Requirements for Service Processes"

[26] J. Brekeur. R. Winkel. "Use and Reuse of Legal Ontologies in knowledge Engineering and Information Management". ICAIL 2003 Workshop on Legal Ontologies & Web Based Legal Information Management