Ontologies for Governance, Risk Management and Policy Compliance[1]

Jorge GONZÁLEZ-CONEJERO [a,2], Albert MEROÑO-PEÑUELA [a] and David FERNÁNDEZ [b]

[a] *Institute of Law and Technology, Universitat Autònoma de Barcelona, Spain*
[b] *S21sec^{TM} , Barcelona, Spain*

Abstract. The Internet and Information Systems evolution have dramatically increased the amount of information hold by companies and public administrations. These data can be very sensitive, specifically regarding personal data, so governments and international organizations promote acts and guidelines in order to ensure privacy and data security. Thus, on the one hand, companies have to consider legal and Information Technology compliance. On the other hand, Governance, Risk Management, and Compliance (GRC) is an emerging discipline which consists of a holistic approach to these three areas of an organization. In this work we introduce the OGRC framework, a software application based on legal and security ontologies that aims at providing organizations with legal compliance support. The main features are: i) the *automation* of some compliance evaluation processes; and ii) *flexibility* to add or modify policies.

Keywords. Governance, Risk Management, Compliance, Ontologies

Introduction

Nowadays, Internet has become the most important channel to share information with the whole world. Most traditional activities including music, film, television, newspapers or books have been reshaped or redefined by the Internet. The Internet has also enabled new forms of human interactions through instant messaging, forums and social networking. In addition, e-commerce and financial services on the Internet have boomed in the recent years. Nevertheless, the use of these services entails providing many personal information to companies and public administrations.

The main issues that arise in this scenario are: i) *privacy*, namely the use that organizations make of these data; and ii) *security*, since sensitive information could be accessed illicitly. Therefore, the most common approaches to face these issues are acts and international standards. On the one hand, governments have developed acts to regulate this scenario. In Spain, the responsible of this area is the Data Protection Agency (AGPD)[3].

[1] This work has been partially supported by the Spanish Ministry of Science and Innovation (Ministerio de Ciencia e Innovación) under Grant IPT-430000-2010-43.

[2] Corresponding Author: Institute of Law and Technology, Universitat Autònoma de Barcelona, B Building, 08193 Bellaterra (Barcelona), Spain; E-mail: jorge.gonzalez.conejero@uab.es

[3] Agencia Española de Protección de Datos `http://www.agpd.es`

AGPD audits organizations to impose a fine when they fail to comply with applicable law. Besides governments, on the other hand, international standard organizations have developed guidelines to ensure the privacy and security of this kind of data.

Governance, Risk Management, and Compliance (GRC) [1] is a holistic approach to these three areas of an organization. GRC is increasingly being integrated in a convergent and more abstract layer, which tries to avoid conflicts, face uncertainty and reduce overlaps and gaps between business processes in order to gain efficiency. In the literature, several approaches that are able to evaluate GRC requirements have been introduced (see [2] and [3]). For instance, Unified Compliance Framework (UCF) [4] is an effort to integrate many compliance policies from the Information Technology department. Modulo Risk Manager [5] implements effective solutions for Compliance based on a wide range of relevant regulations and standards. Finally, Oracle Fusion GRC [6] is a suite of applications designed to work as a complete enterprise GRC solution.

In this work, we introduce the OGRC project, which states for Ontologies for Governance, Risk Management and Compliance. This project will provide organizations with an integrated software solution intended to monitor processes, assets, risks and requirements. Moreover, the OGRC framework is supported by semantic data models aimed to promote desirable features as *automation* and *flexibility*.

The work is organized as follows: section 1 describes the OGRC project. Specifically, acts and standards considered in the OGRC framework are presented in section 1.1, the most important tools operated are described in section 1.2 and the architecture is depicted in section 1.3. Finally section 2 points out some conclusions.

1. Ontologies for Governance, Risk Management and Compliance

Currently, compliance of legal and international standards is verified mostly by experts, usually auditors or consultants, and it is still a manual task. This compliance assessment process can be extraordinarily expensive. The OGRC project aims at providing organizations with legal and automatic compliance support through Bitacora^{TM} [7] and ontologies. Bitacora^{TM} is a S21sec's^{TM} SIEM that collects information from IT systems, applications, users and external intelligence data feeds into a centralized data warehouse. The OGRC framework joins features from Bitacora^{TM} and ontologies to provide organizations with a tool suitable for: i) automatically evaluate compliance for many policies –automation–; and ii) providing a flexible platform for monitoring business processes, were policies can be added or modified accordingly –flexibility–.

1.1. Acts and Standards

The first step is to set the policies that organizations consider as the most useful, in order to integrate them in the OGRC framework. At this point, the consultancy services from S21sec^{TM} pointed out three different policies. The first one is a Spanish act: the Spanish Data Protection Act (LOPD). The LOPD[4] aims at protecting sensible and personal data from citizens. It is specifically devised to guarantee two main issues: i) honor; and ii) personal and family privacy. The scope includes mediums where this sensible data is

[4] Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD)

managed. The act also involves both citizen's rights and obligations of those persons or/and companies responsible of managing this kind of data.

The second one is also a Spanish act: the National Security Scheme or ENS[5]. The ENS states the principles and requirements of a security policy regarding the use of electronic tools, ensuring an adequate protection for information. Besides scoping systems, services and security measures that are present in most real scenarios, the ENS is intended to increase security of services and information provided by systems held by public administrations, as well as protecting communications between citizens and these systems. It does so identifying sensible assets, setting security dimensions and its levels, deciding categories for systems and selecting suitable security measures. This process generates a number of documents whose compliance must be certified.

The third policy is an International Security Standard: the Payment Card Industry Data Security Standard (PCI DSS)[6]. The PCI DSS was developed to enhance cardholder data security. The keystone is the PCI DSS, which offers robust and comprehensive standards and supporting materials to enhance and facilitate the broad adoption of consistent data security measures globally. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS applies to all entities involved in payment card processing such as merchants, acquirers, service providers, etc.

1.2. Tools

In the OGRC framework, ontologies are designed to represent the extracted knowledge from policies presented in section 1.1 in a machine-readable format. In addition, its XML Schema allows the execution of a reasoner algorithm against the ontology structure to determine the compliance status of sensible assets.

1.2.1. Ontologies

An ontology describes the concepts and relationships that are important in a particular domain, providing a vocabulary for that domain as well as a computerized specification of the meaning of terms used in the vocabulary. Gruber defined an ontology as a formal, explicit specification of a shared conceptualization [8]. It is an abstract model of some phenomenon in the world that identifies the relevant concepts of that phenomenon. The main features that make ontologies suitable to our GRC platform are: i) ability to share common information; ii) enable the reuse of knowledge; iii) resilience to changes in the acquired knowledge; and iv) reasoning to determine the compliance. Ontologies have generally been associated with logical inferencing and have begun to be applied to the Semantic Web [9]. Ontologies also provide specific tools to organize and provide a useful description of heterogeneous content.

1.2.2. Protégé and Pellet

Protégé[7] is a suite of tools for ontology development and use, and it is the main framework used in our projects to implement ontologies. It was introduced in [10] and devel-

[5] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad

[6] PCI DSS Home page `http://www.pcisecuritystandards.org`

[7] Protégé Team `http://protege.stanford.edu`

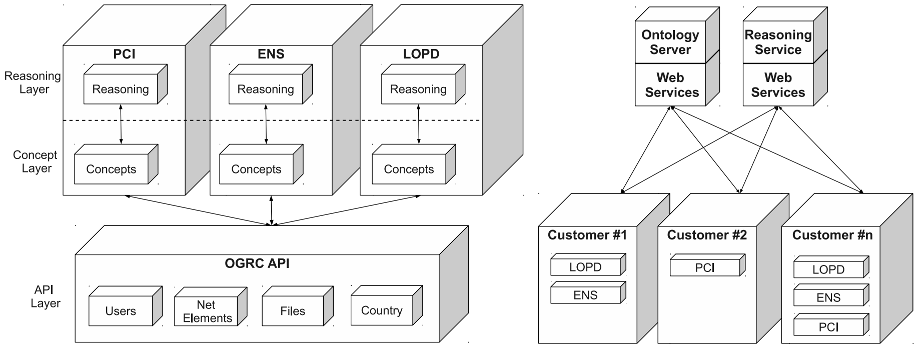

Figure 1. *Left*: Ontologies for each regulation divided in three different layers: API, Concept and Reasoning. *Right*: Architecture falling in a client/server paradigm, including ontology and reasoning modules.

oped by the Stanford Center for Biomedical Informatics Research[8] at the Stanford University School of Medicine[9]. Its main features are: 1) it is a free, open source platform that provides a suite of tools to construct domain models and knowledge-based applications with ontologies; 2) it also implements a rich set of knowledge-modeling structures and actions that support the creation, visualization, and manipulation of ontologies in various representation formats; 3) the framework supports two main ways of modeling ontologies via the Frames and OWL editors; and 4) ontologies can be exported into a variety of formats including RDF(S), OWL, and XML Schema.

Many applications developed for the Semantic Web require some kind of reasoning capability. Providing complete reasoning services is essential for many of these applications to function properly. Pellet [11] has a number of features either driven by OWL requirements or Semantic Web issues.

1.3. Architecture

In this section we focus on the designed architecture concerning two main issues of the OGRC framework: the development of ontologies and the updating process for the customers' software. Ontologies design method fall on a three-layer paradigm. Fig. 1 *Left* depicts the structure. From bottom to top, the first layer is an Application Programming Interface (API) composed by common elements, which are shared between specifically modeled policies. Next layer provides the acquired knowledge from each policy modeled independently. The last layer joins acquired knowledge in the previous layer and suitable elements to obtain reasoning capabilities. In this architecture, changes are propagated from lower layers to upper layers and the modular structure eases the inclusion of new policies. Both benefits provide flexibility feature to the OGRC framework. In addition, the reasoning capabilities obtained from the third layer also favor the automation feature.

The architecture of the OGRC framework is specifically designed to manage ontologies and reasoning algorithm executions through a client/server architecture. Fig. 1 *Right* depicts this. The main idea is to create a structure where users –client side– are able to

[8] Stanford Center for Biomedical Informatics Research `http://bmir.stanford.edu`
[9] Stanford University School of Medicine `http://med.stanford.edu`

update and download new policies from the server. In addition, a reasoning machine is enabled to release the user machine from the reasoning process.

2. Conclusions

Over the last years, sensitive information that organizations manage from citizens has increased exponentially. Therefore, governments and international organizations have developed regulations to ensure privacy and security of sensitive data. In this work we introduce the OGRC framework, which implements semantic data models in the form of ontologies. Ontologies provide two main features: i) *automation* of assets compliance evaluation; and ii) *flexibility* to incorporate modifications and new policies.

Currently, semantic models for two Spanish acts and one international standard are included in the OGRC framework. The ontology architecture falls on a three-layer paradigm. From bottom to top, the first layer is aimed to share common knowledge. Then, the second layer is specifically designed for acquisition of knowledge from each developed policy. The last layer provides elements needed in order to run a reasoning algorithm to determine the assets compliance. Finally, the OGRC framework features a client/server architecture with an ontology repository in the server side, which allows users to connect to the server to update or download new policies.

Acknowledgments

This work was conducted using the Protégé resource, which is supported by grant LM007885 from the United States National Library of Medicine.

References

[1] A. Tarantino, *Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and Int'l Guidance and Best Practices*, Business & Economics, John Wiley and Sons, Hoboken, NJ, 2008.

[2] N. Racz, E. Weippl and R. Bonazzi, *IT Governance, Risk & Compliance (GRC) Status Quo and Integration: An Explorative Industry Case Study*, IEEE World Congress on Services (SERVICES), IEEE Proceedings, (2011), 429–436.

[3] N. Racz, E. Weippl and A. Seufert, *Governance, Risk & Compliance (GRC) Software – An Exploratory Study of Software Vendor and Market Research Perspectives*, 44th International Conference on System Sciences (HICSS), IEEE Proceedings, (2011), 1–10.

[4] Network Frontiers, *Unified Compliance Framework (UCF)*, (2011), available on-line at: http://www.unifiedcompliance.com.

[5] MODULO Solution for GRC: Comprehensive Solutions for Governance, Risk and Compliance Management, *Modulo Risk Manager*, (2011), available on-line at: http://www.modulo.com/risk-manager.

[6] Oracle, *Oracle Fusion GRC: The New Standard for Risk Management and Compliance*, (2011), available on-line at: http://www.oracle.com/us/solutions/corporate-governance/index.html.

[7] S21sec, *Bitacora v5*, available on-line at: http://www.s21sec.com/productos.aspx.

[8] T.A. Gruber, *A translation approach to portable ontology specifications*, Knowledge Acquisition **5**(2), (1993), 199–220.

[9] T. Berners-Lee, J. Hendler, O. Lassila, *The Semantic Web*, Scientific American.

[10] D. Rubin, N. Noy, M. Musen, *Protege: A tool for managing and using terminology in radiology applications*, Journal of Digital Imaging, **0**(0), (2007), 1–13.

[11] E. Sirin, B. Parsiaa, B.C. Graua, A. Kalyanpura, Y. Katza, *Pellet: A practical OWL-DL reasoner*, Web Semantics: Science, Services and Agents on the World Wide Web, **5**(2), (2007), 51–53.