TOWARDS A COMPLIANCE SUPPORT FRAMEWORK FOR GLOBAL SOFTWARE COMPANIES

AbdelKrim Hamou-Lhadj[1] Abdelwahab Hamou-Lhadj[2]
[1] Cognos Inc.
3755 Riverside Drive, Ottawa, ON K1G4K9
Canada
abdelkrim.hamou-lhadj@cognos.com
[2] Department of Electrical and Computer Engineering, Concordia University
1455 de Maisonneuve West, Montreal, QC H3G1M8
Canada
abdelw@ece.concordia.ca

ABSTRACT
Regulated companies are required to comply with the laws and regulations that apply to their industries. An important aspect of these authoritative rules is directly related to the way by which software systems, used by the regulated companies, are built, tested, and maintained. As a result, many regulated companies have turned to their software vendors to request their support in the compliance efforts. For most global software vendors, this new situation represents a significant challenge. From the technological standpoint, the complexity and sheer volume of typical authoritative rules poses a serious obstacle to implementing effective compliance support strategies. From the organizational perspective, the delivery of compliance support activities requires efficient business processes, skilled and valued employees, and a strong governance model with commitment at all management levels. To address these issues, we present a compliance support framework that aims to facilitate the linkage between compliance requirements, software development practices, and business process management. We believe that, if implemented properly, this framework can significantly improve the way software companies handle the increasing customer demand for compliance support. It can turn compliance support into a revenue-generating activity, and possibly a competitive advantage.

KEY WORDS
Software project management, software standards, software compliance, regulatory compliance, software process

1. Introduction

For most industries in the global economy, regulations, standards, and guidelines have become an integral part of the business landscape. More than ever before, regulated companies are required to abide by stringent regulations, and diligently follow the standards and guidelines that are relevant to their industries. Failure to comply may result in customer dissatisfaction, loss of business, and even legal actions. A few examples of these regulations, standards, and guidelines include Sarbanes-Oxley act (SOX), Health Insurance Portability and Accountability act (HIPAA), Quality Management Systems standard (ISO 9001:2000), Analysis of LAN Security guidelines (FIPS 191), etc.

The process by which regulated companies address compliance requirements is commonly known as *Compliance Management*. According to a study conducted by AMR Research[*], the total spending on global compliance management (including governance and risk management) is expected to attain $29.9 billion by the end of 2007, up by 8.5% from 2006.

Like any other organizations, regulated companies expect from their software vendors to deliver products and services that can help them streamline their business processes, improve their operational efficiency, and produce better quality products. However, as the necessity to comply with existing regulations has become inevitable, regulated companies have now a greater expectation from their software partners: To support them in their compliance management efforts.

For example, a North-American pharmaceutical company that acquires a software product for the management of its clinical trial records must ensure that the use of this software meet FDA (Food and Drug Administration) regulations; in particular, the compliance requirements of 21 CFR Part 11 (Electronic Records; Electronic Signatures). Compliance requirements of 21 CFR Part 11 specify the approach by which documents, electronic data and digital signatures must be managed. These requirements apply, for example, to all clinical trial

[*] http://www.amrresearch.com/Content/view.asp?pmillid=20232

electronic records that are created, edited, maintained, archived, retrieved or transmitted. The objective of 21 CFR Part 11 requirements is to ensure integrity, authenticity, confidentiality, and continuity of data, as well as integrity of systems and authenticity of signatures. This is a typical situation where the pharmaceutical company will turn to its software vendor in order to help validate the software product against the 21 CFR Part 11 compliance requirements, and other related FDA regulations.

Cascading the compliance goal to software companies, technology builders are now required to develop software products that are compliance-friendly (i.e., anticipate potential compliance issues) while delivering innovative and high quality product, and reducing the cost of development and maintenance.

For most global software companies, providing such compliance-friendly solutions represents a significant challenge. First, there are just too many regulations, standards, and guidelines that need to be considered [1]. This is further complicated by the fact that compliance requirements vary significantly from one industry sector to another, as well as from one country to another, making it hard to reuse tools and expertise [1]. Second, there is no mandated centralized organization responsible for mapping regulatory compliance requirements at the international level, which renders the task of global software companies to support compliance efforts on the international scene virtually impossible. Third, the compliance problem is new to most global software companies, which hinders effective delivery of end-to-end solutions due to a lack of a clear mission, skilled employees in the area of compliance management, and efficient processes.

Research in the area of compliance management is still in its infancy. The focus has been on investigating techniques to help organizations cope with the large amount of information contained in typical regulatory documents [2, 3, 4, 5, 6, 7]. However, these techniques address the compliance problem only from the technological aspect, placing less attention on organizational issues that global software companies face when dealing with compliance support.

In this paper, we present a compliance support framework that facilitates the linkage between compliance requirements, software development practices, and business process management. The objective is to help software companies cope with the increasing customer demand to support their compliance efforts.

The remaining parts of this paper are as follows. In the next section, we briefly introduce the background needed for this paper. We present the compliance support framework in Section 3. In Section 4, we discuss related work. We finally conclude the paper in Section 5.

2. Compliance Management

Cougias et al. define compliance as the activity of "ensuring that the requirements of laws, regulations, industry codes, and organizational doctrines are met" [1]. There are different types of compliance requirements ranging from local, state, and federal laws and regulations to company policies and procedures, developed for performance management purposes.

In practice, compliance can be viewed as the process by which specific requirements (imposed by enforced regulations, agreed-on standards, or recommended guidelines) are being fulfilled, or the degree to which this fulfillment has been formally verified.

Therefore, compliance management can be seen as the management discipline within which the process of compliance is executed and managed in order to achieve a specific and verifiable compliance level.

One of the key issues in setting up an effective compliance management program is dealing with the complexity level of the relevant regulations, standards, and guidelines. From the quantitative perspective, the number of these authoritative rules might be quite significant for a global company. In addition, this number is continuously increasing to support international trade agreements and new technologies. From the qualitative perspective, many of these authoritative rules tend to overlap in their intents and requirements while many other ones conflict [1].

For example, on the one hand, there is an overlap in the area of data privacy between the following national regulations: Canada Personal Information Protection and Electronic Documents Act (PIPEDA), European Union Data Protection Directive (Directive 95/46/EC), and California Security Breach Information Act (SB-1386). On the other hand, there is a conflict in the area of International Data Privacy Rules in Cyberspace.

There is unfortunately very little work being done to map these authoritative rules in order to provide a high level view of the similarities and the differences.

Global software vendors are expected to support their customers in their compliance efforts. Consequently, they are required to be aware of the key authoritative rules that are important to their customers, and integrate in their business practices (including software development and maintenance) activities that are geared towards making the software product compliance-friendly. These activities can be grouped into three categories:

- Enhancing a specific functionality of the software product (e.g., in order to meet FDA 21 CFR Part 11 compliance requirements).
- Adding a specific task to the software process in use for the development of the software product (e.g., in

order to meet requirements of ISO/IEC 12207 Software Life Cycle Processes).

- Improving a specific organizational practice of the organizational function/division that develops or maintains the software product (e.g., in order to meet ISO 9001:2000 requirements).

Currently, most of the global software vendors seem to deal with compliance support in an ad-hoc manner. They are continuously in a reactive mode; they deal with compliance requirements once these become a serious issue from the business standpoint (i.e., a deal-breaker). Being proactive about compliance support, integrating compliance support in strategic management decisions, and using it as a competitive advantage is a very new scenario for global software vendors.

3. A Compliance Support Framework

Figure 1 illustrates the components of the Compliance Support Framework presented in this paper. The framework is based on the well-known PPT (People, Process, and Technology) model frequently used in project management [8]. We have enhanced the PPT model by adding a governance component to enable strategic thinking and management related to compliance support initiatives. The specifics of each component and how it could be applied to compliance support is presented in the subsequent sections.

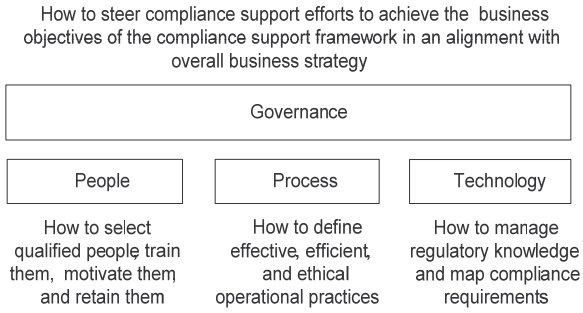

Figure 1. Components of a Compliance Support Framework

3.1 Governance Component

The mission of the governance component in the compliance support framework is to provide the strategic directions in order to fulfill on its compliance support objectives. This component embodies a set of performance objectives, execution policies, management internal controls, and strategic alignment mechanisms.

In fact, the governance component is the way by which the software company would steer the compliance support framework to engage in a successful and unified approach to compliance support, to integrate compliance support activities with software development and maintenance activities at both the process level and the project level, and to generate effective products and services to regulated customers so as to support them in their compliance efforts. In what follows, we present key success factors for an effective governance component.

To start with, software companies must recognize compliance support as an emerging need in the marketplace, and allocate the necessary resources to it. This will allow them to transform compliance support from a mere support activity to a revenue-generating business activity with the ultimate objective being to deliver compliance related products and services.

In addition, software companies should adopt a proactive approach to ensure effective monitoring of key authoritative rules. Doing so, the software company will be able to anticipate regulatory changes, and even influence some of them, through active participation in their development or through knowledge transfer from partnering organizations.

Another key success factor for governance is to establish a clear accountable role for the management of the compliance support framework. This role will ensure that the system is effectively governed and efficiently functioning towards the achievement of its compliance support objectives. It is recommended to have this management role at the senior management level in the software company.

Finally, the governance component will also require a set of management processes in place to ensure proper planning, execution, and monitoring of compliance support activities. These processes should be integrated with existing business processes, including those of software development and maintenance.

3.2 People Component

The objective of the people component is to set up the right conditions in order to enable the selection, the motivation, the training, and the retention of qualified human talents who will operate the compliance support framework and deliver on its business objectives.

Software projects involving compliance requirements necessitate specific interdisciplinary skills in various areas including regulatory and quality framework analysis (e.g., FDA regulations, ISO quality standards), software engineering processes and standards, and quality management. While educational institutions provide good training and qualifications with respect to the technical side of software development, basic knowledge about compliance challenges, issues, and solutions associated to the development and maintenance of software products is almost inexistent from their curriculum. This knowledge is necessary in order to design, verify, and validate software products that meet compliance requirements.

3.3 Process Component

The focus of the process component is to define the operational activities that need to take place for the

development and delivery of compliance support products and services.

From the product standpoint, examples of compliance support activities include having an audit trail function in the software product, providing the functional specifications document of a specific software capability, and sharing the description of the quality control process followed to test the software product. From the service standpoint, examples of activities include documenting how to validate the most risky software functions, developing a validation plan for a regulated customer, and providing test scripts.

The delivery of compliance support activities should include the following activities:

- Defining compliance requirements for a software development project.
- Integrating required compliance support activities within software development activities.
- Using relevant software quality assurance activities for compliance support verification.

The processes underlying these delivery activities should aim to be effective, efficient, and ethical.

3.4 Technology Component

The objective of the technology component is to provide tool support to compliance analysts, working on large, possibly overlapping or conflicting, compliance documents.

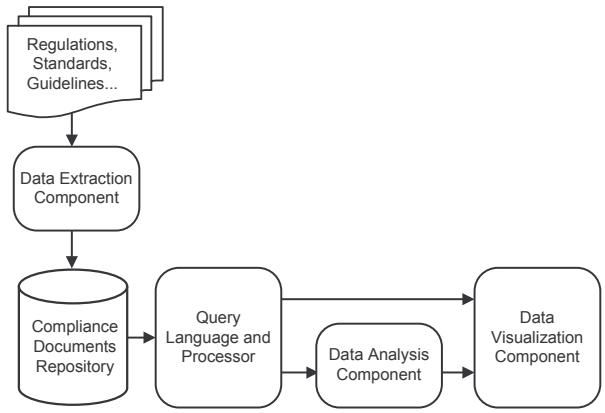

Figure 2. Architecture of a compliance management tool

A typical compliance management tool should have the following components (see Figure 2): A data repository, a data extraction component, a query language and processor, a data analysis component, and a data visualization component. These components are discussed in more detail in what follows.

A compliance documents repository:

The key component of a compliance management tool is a data repository that optimizes storage, retrieval and processing of very large compliance documents. These documents should, however, be modeled according to a well-defined schema, designed to express a full spectrum of compliance documents semantics (e.g., provisions, rules, etc.). In [2], the authors propose an XML-based schema for representing specific United States (U.S.) regulations. We believe that this schema can be easily extended to support other types of regulatory documents.

In addition, we need to work towards having a *standard* schema for representing compliance documents. There are many advantages of having a standard schema:

- It enables interoperability between different compliance management tools, by eliminating the need to create converters between various formats.
- It allows users to experiment with different tools, without having to worry about how the data is represented.
- It makes it possible to easily add new regulations (or any changes made to existing ones).
- It provides a powerful mechanism for comparing and mapping various regulatory documents.

It should be noted, however, that the adoption of a standard schema by tool builders will greatly depend on its ability to scale up to support large documents, and the degree to which it can be easily extended to express new types of compliance requirements.

A data extraction component:

The role of the data extraction module is to parse compliance documents, extract information from them, and populate the compliance documents repository. Existing natural language parsers can be easily adapted to achieve this purpose.

A query language and processor:

A specialized query language is needed to facilitate the retrieval of information from the compliance documents repository. The language should contain built-in functions that compliance analysts can readily work with when searching for specific parts of a regulatory document, comparing different sections of a range of compliance documents, etc.

It is not required to create the query language from the scratch. We can simply reuse existing languages such as SQL [9], XQuery [9], etc. For example, if the compliance documents repository is implemented using relational databases then the built-in functions can be made of SQL statements. Similarly, XQuery can be used if the repository consists of XML-based files.

A data analysis component:

A compliance management tool should support a large range of analyses, among which the most needed are:

- Content analysis: The objective here is to enable users to browse long documents, navigate across documents, search for keywords, etc. One of the key features that should be provided is the ability to express complex search queries by allowing users to combine various search criteria in a single search query. In addition, the tool should be able to return similar, but not necessarily identical, results, since the same concept may be represented by many different terms, while the same term may have different meanings in different places.
- Relatedness analysis: The objective of relatedness analysis is to compare different compliance documents in order to detect common rules and patterns. It can also be used to identify similar compliance documents and perhaps group them into clusters. In [5, 6], the authors present an approach for relatedness analysis by combining several techniques, namely information retrieval, feature matching, and document structure analysis.
- Abstractness analysis: Compliance documents tend to contain a large amount of information that some users, typically experts, might wish to skip in order to focus on important content. In such cases, a compliance management tool should automatically (or semi-automatically) hide unnecessary details and exhibit most relevant content. Existing information retrieval techniques (e.g., [10, 11]) can be adapted to achieve this goal.
- Compliance checking: A compliance management tool should support the ability to detect violations to specific compliance requirements. Although, we anticipate that it would be difficult to automate this process, a compliance checker can be designed to provide clues on possible discrepancies between the user's specifications and the compliance requirements that need to be satisfied.

A data visualization component:

The information derived from the previous steps needs to be displayed in a usable user interface in order to be easily explored and analyzed. Textual browsers can be used to display the content of particular parts of a compliance document. Hyperlinked pages can help navigate across the various sections of the document. Graphical visualizers are recommended if complex relationships between various compliance documents are to be displayed. For this purpose, visualization techniques such as color-coding, use of icons, highlighting, etc. can be utilized. There is a need to conduct usability studies in order to understand the best way to represent compliance documents in an effective user interface.

4. Related Work

We are not aware of any work that addresses compliance management from the perspective of global software companies.

Most existing studies focus on investigating techniques to manage the sheer size of compliance documents. Therefore, we can only compare them with the techniques presented in the technology component of the proposed framework.

In April of 2005, the Object Management Group (OMG) launched a new initiative to address the increasing number of regulatory documents and their impact on organizations [12]. This has led to the creation of the Governance, Risk Management and Compliance Roundtable (GRC-RT). Led by Adrian Bowles, a worldwide expert in compliance management, the GRC-RT group has initiated many programs that address compliance issues, among which the most related to this paper is the creation of a Global Rules Information Database (GRC-GRID), an open resource for GRC professionals. The global database is similar to the compliance documents repository presented in this paper. The work of the GRC-RT is still ongoing and the details regarding the global database such as the schema, the query language, etc. have not been released.

Perhaps, one of the most comprehensive research projects that addresses the sheer volume of compliance documents is the REGNET project. Led by members of the Engineering Informatics Group from Stanford University, the project aims to create an information infrastructure that supports U.S. federal and state regulations. The main outcomes of the project include an XML-based repository to represent specific government regulations [2], an approach for locating and comparing related regulations based on information retrieval techniques, feature matching, etc. [5, 6], and a compliance assistance system that facilitates the analysis of the compliance documents in question [4]. Most of these techniques can be adapted to support some aspects of the technology component presented in this paper such as the compliance documents repository and the data analysis component.

In [3], the authors present an approach for compliance validation to help health information custodians improve their business processes in order to comply with the Personal Health Information Protection act (PHIPA). Their approach is based on using the User Requirement Notation (URN) [13] to model the business processes specific to the access of confidential information. Another model is created to model the PHIPA privacy legislation requirements. The two models are then analyzed using a requirement engineering tool that supports URN, and the discrepancies between the hospital business practices and the PHIPA regulations have been identified. Although this technique requires an extensive human effort, it can serve as a starting point for the development of an

efficient approach for compliance validation and checking.

Finally, Viswanathan et al. present an overall research methodology for the development of knowledge-based compliance systems [7]. However, their methodology is too abstract and focuses more on the requirements for a good research methodology in the area of compliance management rather than specific techniques on how to deal with the large volume of compliance documents.

5. Conclusion

In this paper, we presented a unique and innovative compliance support framework to help global software companies cope with the increasing customer demand for compliance support. The proposed framework is composed of four main components: Governance, People, Process, and Technology.

The aim of the governance component is to provide the strategic direction that will steer the overall framework towards an effective delivery of end-to-end compliance support activities. This steering role is also responsible for ensuring the proposed direction is fully aligned with company's business objectives and value system.

The people component presents the key activities for the selection, motivation, and retention of the human talents who will operate the framework. A point of interest is to involve personnel in training programs that cover compliance challenges, issues, and solutions. These topics are generally not covered in educational institutions.

The process component defines the operational approach by which the delivery of compliance support activities will take place in the framework. This approach must be based on a set of effective, efficient, and ethical practices that will allow the framework to achieve its support objectives through an optimal performance.

Finally, the technology component emphasizes on the proper tools and techniques that should be made available in order to automate the delivery of compliance support activities. These tools must be built so as to overcome the sheer size of typical compliance documents. In this paper, we architected a compliance support tool that can facilitate the exploration and analysis of, possibly overlapping or conflicting, large compliance documents.

Disclaimer

The opinions expressed in this paper are exclusively of the authors and do not necessarily reflect official support or endorsement by Cognos Incorporated.

References

[1] D.J. Cougias, M. Halpern, R. Herold, *Say what you do: Building a framework of IT controls, policies, standards, and procedures* (Shaser-Vartan, 2007).

[2] G.T. Lau, S. Kerrigan, H. Wang, K.H. Law and G. Wiederhold, An information infrastructure for government regulation analysis and compliance assistance, *Proc. 5th Conf. on Digital Government Research*, Seattle, WA, USA, 2004, 1-2.

[3] S. Ghanavati, D. Amyot, and L. Peyton, Towards a framework for tracking legal compliance in healthcare, *Proc. 19th Conf. on Advanced Information Systems Engineering*, Trondheim, Norway, 2007, 218-232.

[4] S.L. Kerrigan and K.H. Law, A regulation-centric, logic-based compliance assistance framework, *International Journal of Computing in Civil Engineering, 19*(1), 2005, 1-15.

[5] G.T. Lau, H. Wang, and K.H. Law, Locating related regulations using a comparative analysis approach, *Proc. 7th Conf. on Digital Government Research*, San Diego, CA, USA, 2006, 229 - 238.

[6] G.T. Lau, K.H. Law, and G. Wiederhold, A relatedness analysis of government regulations using domain knowledge and structural organization, *International Journal of Information Retrieval 9*(6), 2006, 657 – 680.

[7] M. Viswanathan, Y.K. Yang, T.k. Whangbo, N.B. Kim, B. Garner, Knowledge-based compliance management systems - methodology and implementation, *Proc. 4th IEEE/ACIS Conf. on Computer and Information Science*, Jeju Island, South Korea 2005, 25-29.

[8] S. Berkun, *The art of project management* (O'Reilly Media, 2005).

[9] J. Melton, S. Buxton, *Querying XML, XQuery, XPath, and SQL/XML in context* (Morgan Kaufmann, 2006).

[10] M. Kan, K.R. McKeown, and J.L. Klavans, Applying natural language generation to indicative summarization, *Proc. 8th European Workshop on Natural Language Generation*, Toulouse, France, 2001, 1-9.

[11] G.C. Stein, A. Bagga, G.B. Wise, Multi-document summarization: Methodologies and evaluations, *Proc. 7th Conf. on Automatic Natural Language Processing,* Lausanne, Switzerland, 2000, 337-346.

[12] A. Bowles, The global rules information database: An open IP project, *White paper, URL: http://www.grcroundtable.org/presentations-papers.htm.*

[13] M. Weiss, D. Amyot, Business process modeling with URN, *International Journal of E-Business Research 1*(3), 2005, 63–90.