

Indicator-based Policy Compliance of Business Processes

Azalia Shamsaei

SITE, University of Ottawa, 800 King Edward, Ottawa, ON, K1N 6N5, Canada
asham092@uottawa.ca

Abstract. Business process compliance management has recently grabbed a lot of attention in both business and academia as it helps organizations not only to control and monitor their business processes from a legal point of view but also to avoid financial penalties and undesirable consequences to their reputation. Balancing compliance obligations with business objectives remains however a difficult challenge. We believe goal-oriented compliance management using Key Performance Indicators (KPIs) to measure the compliance level of organizations is an area that can be further developed to tackle this challenge. Goal-oriented compliance management concepts have been explored before. However, there is little research on how to measure and improve the compliance level of organizations using KPIs while considering the impact of candidate adjustments on business goals. We discuss a proposal toward a framework to address the aforementioned problems.

Keywords: Business Process, Goal Modeling, Legal Compliance, Key Performance Indicator.

1 Introduction to Research Questions

Compliance with various levels of regulations is a critical activity in any organization. Every year, organizations invest time and money to ensure their business processes are compliant with different regulations. Regulations may vary depending on an organization's sector of activity. In addition, different legislative bodies and regulators create these regulations. Therefore, they may conflict or overlap with each other.

Compliance management becomes complex partly due to an overwhelming number of laws, policies, standards, and other types of regulations introduced or modified each year. With so many rules to follow, large organizations have a difficult time keeping track of business process compliance levels and evaluating the impact on the organization goals when making these processes compliant. Different stakeholders in an organization have different and perhaps conflicting goals, which makes the situation even more complicated. Furthermore, it is next to impossible to comply with all imposed regulations given limited resources (e.g., human and financial) and conflicting rules. Hence, organizations have to pick and choose the compliance areas they want to address considering different factors. Finally, many organizations use a reactive approach to compliance and only address issues after failures in audits as opposed to taking a proactive approach to prevent such failures in the first place.

In this context, it is necessary to develop a framework that would allow organizations to address the above issues. Such a framework should help organizations answer the following questions: How can we establish simple traceability between policies, laws, regulations in general, business processes, and organization goals? How can organizations constantly monitor the level of compliance of business processes to avoid audit failures? How does making a process compliant with a particular regulation impact organizations goals including goals of different stakeholders? What is the overall compliance level of the organization with respect to one or multiple regulations? What if modifications to a process improve compliance with a regulation while degrading compliance with other regulations? How can organizations select the most important compliance issues to address given their limited resources?

2 Analysis of Related Work

In recent years, much work has been done to improve business process compliance management and measure business process compliance levels. We only describe the most significant research in this section. However, we have conducted a systematic literature review in this area [10].

Lu *et al.* [4] propose a method for measuring business process compliance against control rules defined using control objectives from different sources (e.g., regulations or partner contracts) and modeled using FCL (Formal Contract Language). They define concepts of ideal semantics for control rules in order to categorize various degrees of compliance between processes and rules. They categorize them into four groups including ideal, sub-ideal, irrelevant, and non-compliant situations. They calculate both ideal and sub-ideal compliance degrees of businesses processes against control rules to evaluate how well the process model supports control rules. The end result of this method can be utilized by process designers to improve the compliance degree, but the complexity of the method may be an impediment for regular business users.

Silveira *et al.* [8] suggest a compliance governance dashboard (CGD), with key compliance indicators (KCI) used to measure the compliance level of processes. Their CGD consists of different levels of abstraction. The top-level view shows the most critical regulatory and policy indicators, the compliance level of the main processes, as well as an overall compliance level for the organization. One can drill down to see more details and analyze the compliance of individual process atomic units in various business units. Furthermore, one can view compliance violation reports consisting of all the information reported to internal and external auditors. However, their framework does not identify the impact of regulations on organizations goals.

Rifaut and Dubois [7] propose a method to combine and model the regulations and business requirements for processes. They combine tabular requirements with *i** goal models, where they model purposes, and decompose them all the way down to indicators used to assess and measure the success of processes. This framework can be used prior to the design and implementation of a process, as well as later on for monitoring and controlling the compliance of processes. However, the proposed framework does

not identify how KPI values are measured and does not suggest a method for measuring the overall compliance level of the organization

Morrison *et al.* [5] define a method for measuring the degree of compliance of processes with respect to both crisp and imprecise compliance requirements. Their method relies on creating a compliance scale model that allows measurement of both qualitative and quantitative values for a particular process instance. Although this method can assess the level of compliance of a process, it requires a lot of preparatory work to determine the compliance scales.

Much work related to compliance audits of business process instances has been done. However, modeling the intents and objectives of regulations, organization goals, and key performance indicators for measuring compliance level of regulations as an integrated framework has not been explored yet. A goal view with associated compliance KPIs integrated with a process view allow for reasoning about what to do next as well as about the impact of candidate improvements on organization goals, hence providing a holistic view.

Our proposed framework is based on the User Requirements Notation (URN), the first international standard to combine goal modeling (Goal-oriented Requirement Language — GRL) with scenario modeling (Use Case Map notation — UCM) [2]. URN was created for modeling telecommunication services and reactive systems, but it was shown to be a competitive language for business process modeling [11]. jUCMNav [3], a free Eclipse-based tool, is used to analyze and manage URN models.

3 Sketch of Proposed Solution

To address the problems mentioned in Section 1, we propose a goal-oriented model-based framework for measuring the level of business process compliance with respect to regulations, laws, standards, and policies. This framework consists of the elements illustrated in Fig. 1. We model regulations, starting at high-level (i.e., policy). Then, we decompose the policies down to operational/control rules level. These rules control the processes meant to be compliant with the policies and regulations. We define a set of KPIs for each rule that measure the level of compliance for the rules by comparing the desired target value with the current value of each KPI. Furthermore, we also model organization goals and business processes, hence providing a more holistic view. Rules are associated with related organization business processes through URN traceability links. A set of KPIs is defined to help analyze the impact on the organization goals of changes made to business processes for improving the compliance level.

The first step of the framework is modeling all the aforementioned elements required by the framework. This step helps us to simplify traceability between policies, regulations, business processes, and organization goals.

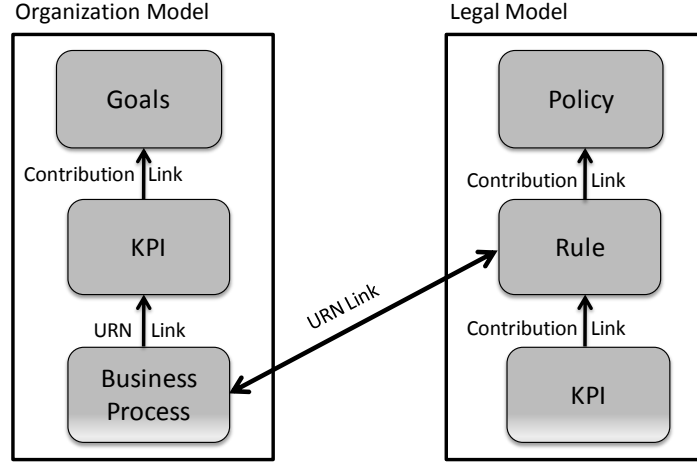


Fig. 1 Elements of the framework

Organization goals, policies, and rules are modeled using the GRL notation while business processes are modeled using the UCM notation. The KPIs are, however, modeled using an extension of URN introduced in [6]. Finally, we associate the business processes in the organization model to related business goals and KPIs using URN links. We use the same method to associate the control rules in the regulation model with corresponding business processes in the organization model.

In the next step we evaluate the model to find the overall compliance level of the organization with respect to one or multiple regulations. We perform this assessment using the designed model and GRL *strategies*, usually used to initialize the leaf elements of GRL models in order to compute the satisfaction level of the higher level nodes using a bottom-up propagation algorithm [1]. In our application, GRL strategies initialize the KPI value sets (i.e., target value, threshold value, worst value, evaluation value). An evaluation value is the actual value of a KPI at the time of the evaluation. The evaluation values can be entered manually like other value sets (which is useful for the analysis of what-if situations) or automatically obtained from various data sources such as a Business Intelligence (BI) systems. A GRL KPI maps the evaluation value to a satisfaction level (on a scale from -100 to 100, by linear interpolation considering the target, threshold, and worst values) that can then be propagated to other elements (rules, policies) in the goal model according to the goal evaluation algorithms presented in [1].

In order to find out how organizations can select the most important compliance issues to address given their limited resources, we define the importance values of the high-level business goals that will be propagated using a top-down importance algorithm to business processes and associated policies/rules through the URN links.

In the improvement step, we illustrate the rules on a quadrant diagram based on their compliance level (satisfaction level) and importance value. We then highlight the critical rules with low satisfaction levels and high importance value and track down the associated processes for improvement.

Finally, in the last step, we monitor the business processes to observe not only the expected changes on the modified process but also to detect potential side effects on organization goals and compliance levels of other control rules in the organization.

This framework already addresses some of the problems mentioned in section 1 [9]. In the next phase of our research, we plan to extend the framework in order to find solutions for the following problems as well.

In the suggested approach, it could be challenging to determine appropriate targets required for KPI values to make the high-level business goals and compliance objectives reach a desired satisfaction level. The current GRL evaluation algorithms are all bottom-up, and hence can only be used to assess an explicit strategy. In order to be able to solve the mentioned problem, a top-down algorithm (i.e., a search algorithm) should be designed to suggest appropriate KPI target values given the satisfaction values required for the high-level goal in the model. Coming up with an algorithm to find the answers for the small model can be done using approaches like game theory or constraint solving. However, coming up with a scalable algorithm that can be used in complex situations (e.g., large organizations with hundreds of processes and many policies and regulations) could quickly become very challenging.

Moreover, we will improve the precision of models by defining appropriate stereotypes (e.g., policies and rules) and by adding constraints to the metamodel elements of the framework. These constraints can help the modelers deal with common complexities in large models. The constraints will be formalized with UML's Object Constraint Language (OCL) and checked against the model. For instance, these rules will check that "policies cannot have KPIs" or that "rules can only influence policies". User-defined OCL rules can already be verified on URN models with jUCMNav.

Moreover, we also plan to further analyze the impact of making a process compliant with regulations on organization goals, including goals of different stakeholders. We believe the current framework already supports this to some extent using the KPIs in the organization model. However, we have not validated the use of these KPIs in a case study and we think there is more work to be done on that front.

In addition, we plan to further develop our approach for selecting the most important compliance issues. The current proposed algorithm needs improvement in order to support importance values for business goals and policies/regulations. Furthermore, implementing the proposed quadrant-based visualization and bringing it to the business users can help with the validation of this approach.

Finally, the constant monitoring of the changes in compliance levels and observing the positive and negative impacts of the changes made to the processes on the business context are other areas of interest.

4 Contributions

While doing research on the proposed framework, several papers have been published [9, 10] and the following contributions have been done:

- Modeled legal requirement and policies/rules using URN.
- Measured the level of business process compliance for one or multiple regulations or policies (in a Human Resource example).

- Calculated the importance level of processes and rules considering high-level business goals.
- Discovered the business processes that violate the rules derived from regulations and policies.
- Systematically reviewed compliance measurement approaches based on goals and indicators (with 32 publications selected from four search engines and the study of specialized conferences).

We plan to work toward the following contributions:

- Determining the impact of compliance-related process modifications on business goals, including conflicting goals between stakeholders, and on conflicting rules.
- Determining the target value of selected KPIs given the desired satisfaction value of high-level organization and compliance goals.
- Using the importance level of processes and compliance level to come up with a prioritized list of improvements required for business processes.
- Using Business Intelligence tools as the infrastructure for extracting the KPI values.
- Validating the framework with case studies related to human resources and airport security policies and business processes.

5 Progress and Evaluation

The groundwork for this framework has been already established. We have published a paper on business process compliance tracking using KPIs [9] as well as a systematic literature review on compliance measurement based on goals and indicators [10]. In [9], we used a case study related to human resource policies to explore the benefits and shortcomings of the framework. In the future, we are going to further expand and analyze the human resource policies to have a better enterprise-level scenario for validation purposes. The expanded model will allow us to broaden the validation of the framework by examining some of the future work suggested in section 4. We will then address the inadequacies of the suggested framework according to the initial results and feedback on the human resource scenario. Finally, we will use a second case study on airport security policies and business processes in collaboration with Transport Canada (the national regulator) to complete the validation of the improved framework by using it in a realistic and different context.

References

1. Amyot, D., Ghanavati, S., Horkoff, J., Mussbacher, G., Peyton, L., Yu, E.: Evaluating Goal Models within the Goal-oriented Requirement Language. *International Journal of Intelligent Systems*, Vol. 25, Issue 8, pp. 841–877. Wiley (2010)
2. International Telecommunication Union: Recommendation Z.151 (11/08), User Requirements Notation (URN) – Language definition, <http://www.itu.int/rec/T-REC-Z.151/en>.
3. jUCMNav, Version 4.2.1, University of Ottawa (2010)
<http://softwareengineering.ca/jucmnav>
4. Lu, R., Sadiq, S., and Governatori, G.: Measurement of Compliance Distance in Business Processes. In: *Info. Sys. Management*, vol. 25, pp. 344–355. Taylor & Francis, USA (2008)
5. Morrison, E., Ghose, A., and Koliadis, G.: Dealing With Imprecise Compliance Requirements. In: *EDOCW*, pp. 6–14. IEEE CS, New Zealand (2009)
6. Pourshahid, A., Chen, P., Amyot, D., Forster, A.J., Ghanavati, S., Peyton, L., Weiss, M.: Business Process Management with the User Requirements Notation. *Electronic Commerce Research*, 9(4), pp. 269–316. Springer (2009)
7. Rifaut, A. and Dubois, E.: Using Goal-Oriented Requirements Engineering for Improving the Quality of ISO/IEC 15504 based Compliance Assessment Frameworks. In: *RE'08*, IEEE, pp. 33–42. Barcelona, Catalunya, Spain (2008)
8. Silveira, P., Rodriguez, C., Casati, F., Daniel, F., D'Andrea, V., Worledge, C and Taheri, Z.: On the Design of Compliance Governance Dashboards for Effective Compliance and Audit Management. In: *ICSOC-ServiceWave 2009*, Stockholm, Sweden. LNCS, vol. 5900, pp. 208–217. Springer (2009)
9. Shamsaei, A., Pourshahid, A., and Amyot, D.: Business Process Compliance Tracking Using Key Performance Indicators. *BPD 2010*, Hoboken, USA. *BPM 2010 Workshops. LNBIP*, vol. 66, pp. 73–84. Springer (2010)
10. Shamsaei, A., Amyot, D., and Pourshahid, A.: A Systematic Review of Compliance Measurement Based on Goals and Indicators. In: *GRCIS 2011*, London, UK. *CAiSE 2011 Workshops, LNBIP*, vol. 83, pp. 228–237. Springer (2011)
11. Weiss, M., Amyot, D.: Business process modeling with URN. *International Journal of E-Business Research* 1(3), pp. 63–90. IGI Global, Hershey (2005)