On the Design of Compliance Governance Dashboards for Effective Compliance and Audit Management

Patrícia Silveira[1], Carlos Rodríguez[1], Fabio Casati[1], Florian Daniel[1], Vincenzo D'Andrea[1], Claire Worledge[2], and Zouhair Taheri[3]

[1] University of Trento, Italy
{silveira,crodriguez,casati,daniel,dandrea}@disi.unitn.it
[2] Deloitte Conseil, Paris, France
cworledge@deloitte.fr
[3] PricewaterhouseCoopers Accountants, Rotterdam, Netherlands
zouhair.taheri@nl.pwc.com

Abstract. Assessing whether a company's business practices conform to laws and regulations and follow standards, i.e., compliance governance, is a complex and costly task. Few software tools aiding compliance governance exist; however, they typically do not address the needs of who is in charge of assessing and controlling compliance, that is, compliance experts and auditors. We advocate the use of compliance governance dashboards, whose design and implementation is however challenging for these reasons: (i) it is fundamental to identify the right level of abstraction for the information to be shown; (ii) it is not trivial to visualize distinct analysis perspectives; and (iii) it is difficult to manage the large amount of involved concepts, instruments, and data. This paper shows how to address these issues, which concepts and models underlie the problem, and, how IT can effectively support compliance analysis in SOAs.

1 Introduction

Compliance is a term generally used to refer to the conformance to a set of laws, regulations, policies, or best practices. *Compliance governance* refers to the set of procedures, methodologies, and technologies put in place by a corporation to carry out, monitor, and manage compliance.

Compliance governance is an important, expensive, and complex problem to deal with: It is *important* because there is increasing regulatory pressure on companies to meet a variety of policies and laws (e.g., Basel II, SOX). This increase has been to a large extent fueled by high-profile bankruptcy cases (Parmalat, WorldCom, the recent crisis) or safety mishaps (the April 2009 earthquake in Italy has already led to stricter rules and procedures for construction companies). Failing to meet these regulations means safety risks, hefty penalties, loss of reputation, or even bankruptcy [9].

Managing and auditing/certifying compliance is a very *expensive* endeavor. A report by AMR Research [5] estimates that companies will spend US$32B only on governance, compliance, and risk in 2008 and more than US$33B in 2009. Audits are themselves expensive and invasive activities, costly not only in terms of auditors' salaries but also in terms of internal costs for preparing for and assisting the audit – not to mention the cost of non-compliance in terms of penalties and reputation.

A. Dan, F. Gittler, and F. Toumani (Eds.): ICSOC/ServiceWave 2009, LNCS 6275, pp. 208–217, 2010.

Finally, the problem is *complex* because each corporation has to face a large set of compliance requirements in the various business segments, from how internal IT is managed to how personnel is trained, how product safety is ensured, or how (and how promptly) information is provided to shareholders. As a result, compliance governance requires understanding/interpreting requirements and implementing and managing a large number of control actions on a variety of procedures across the business units of a company. Each compliance regulation and procedure may require its own control mechanism and its own set of indicators to assess the compliance status of the procedure [1]. Today, compliance is to a large extent managed by the various business units in rather ad-hoc ways (each unit, line of business, or even each business process has its own methodology, policy, controls, and technology for managing compliance). Hence, it is very hard for any CFO or CIO to answer questions such as [16]: *Which rules does my company have to comply with? Which processes are following regulations? Where do violations occur? Which processes do we have under control?* Even more, it is hard to do so from a perspective that not only satisfies the company but also the company's *auditors,* since they are the ones that certify compliance.

This paper presents a conceptual model for compliance and for *compliance governance dashboards* (CGDs), along with a dashboard architecture and a prototype implementation. The aim of our CGD is to report on compliance, to create an awareness of possible problems/ violations, and to facilitate the identification of root-causes for non-compliant situations. The dashboard is targeted at several classes of users: chief officers of a company, line of business managers, internal auditors, and external auditors (certification agencies). Typically, the two latter focus on a narrow set of processes and historical data to verify non-compliant situations and how they have been dealt with. Via the CGD, they also have *access to key compliance indicators* (KCIs). Managers are interested in a much broader set of compliance regulations and at quasi-real time compliance information that allows them to detect problems (unsatisfactory KCIs) as they happen and identify the causes (drill-down to the root of the problem), so that they can take decisions before they become (significant) violations. They have access and navigate through the entire set of regulations, business processes, and business units and also observe the overall compliance status (through KCIs).

Technically, building a dashboard that shows a bunch of indicators and allows drill-downs is easy. Indeed, the main challenges are *conceptual* more than technological [15] and constitute the contributions of this paper as follows:

1. Provide a *conceptual model for compliance and for compliance dashboards* that covers a broad class of compliance issues. It is important to identify the key abstractions and their relationships; otherwise the dashboard loses its value of single entry point for compliance assessment.
2. Combine the above *broadness with simplicity and effectiveness*. The challenge here is to derive a model that, despite being broad, remains simple and useful. If the abstractions are not carefully crafted and kept to a minimum, the dashboard will be too complex and remain unused. As we have experienced, this problem may seem easy but is instead rather complex, up to the point that discussions on the conceptual model in the projects took well over a year. There is no clarity in this area, and this is demonstrated by the fact that while everybody talks about compliance, there are no generic but simple compliance models available.

3. Define a *user interaction and navigation model* that captures the way the different kinds of users need to interact with the dashboard, to minimize the time to accesses spent in getting the information users need and to make sure that key problems do not remain unnoticed.
4. Derive a model aligned with the *criteria and approach that auditors have* to verify compliance. In this paper, this latter is achieved "by design", in that the model is derived via a joint effort of two of the major auditing companies and reflects the desired method of understanding of and navigation among compliance concerns.

2 The Problem of Compliance Management

Despite the increasing awareness of compliance issues in companies and the recognition that part of the compliance auditing task can be automated, i.e., assisted by software tools [9][12][13], there is still a lot of confusion around. This is especially true for the IT community, which would actually be in charge of aiding compliance governance with dedicated software. To help thinking in terms of auditing, in the following we aim to abstract a wide class of compliance problems into a few key concepts that are also the ones understood by auditors. The resulting model (see Fig. 1) does not cover all possible compliance problems, but our goal is to strike a balance between coverage and simplicity. So far, we didn't find any such model in literature.

At the top-left corner: The *Regulation* entity generalizes all documents that provide guidelines for the good conduct of business in a given domain. Examples of regulations are legislations (e.g., MiFID, The Electronic Commerce Directive), laws (e.g., SOX, HIPAA), standards (e.g., CoBIT, ISO-9001), and SLAs. Typically, a regulation defines a set of rules in natural language, which constrain or guide the way business is conducted. *Complying* with a regulation means satisfying its rules. The selection of the pertaining ones represents the *requirements* for compliance management, usually expressed in terms of control objectives and activities. A regulation expresses multiple requirements, and a requirement might relate to one or more regulations.

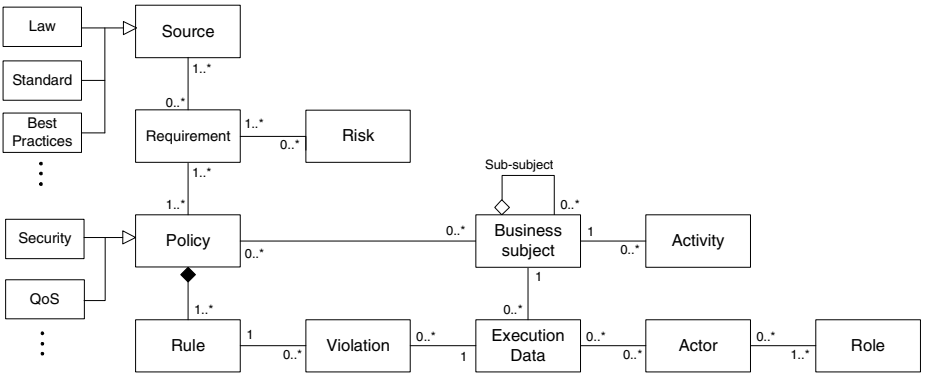


Fig. 1. Conceptual model of the compliance management problem

Assessing compliance demands for an interpretation and translation of the requirements provided in natural language in an actionable rule description (especially in the case of principle-based regulations) [7][8]. This is modeled by the *Rule* entity, which represents actionable rules expressed either in natural language (using the company's terminology and telling exactly how to perform work) or, as desirable in a formalism that facilitates its automated processing (e.g., Boolean expressions over events generated during business execution). Rules are then grouped into *policies*, which are the company-internal documents that operatively describe how the company intends achieving compliance with the selected requirements. Typically, policies group requirements into topics, e.g., security policies, QoS policies, and similar.

At a strategic level, compliance is related to the concept of risk. Non-compliant situations expose a company to risks that might be mitigated (e.g., a non-encrypted message that is sent through the network might violate a security compliance rule, which might put at risk sensitive information). Risk mitigation is the actual driver for internal compliance auditing. The *Risk* entity represents the risks a company wants to monitor; risks are associated with compliance requirements. For the evaluation of whether business execution is compliant, we must know which rules must be evaluated in which business context. We therefore assume that we can associate policies with specific *business processes*. Processes are composed of *activities*, which represent the atomic work items in a process.

The actual evaluation of compliance rules is not performed on business processes (that is, on their models) but on their concrete executions (their instances). Executing a business process means performing activities, invoking services, and produced business data (captured by the *Execution data* entity). In addition, e.g., separation of duties, it is necessary to track the *actors* and *roles* of execution of activities. When evaluation of a rule for a process/activity instance is negative, it corresponds to *violations*, which are the core for assessing compliance level and computing KCIs.

The model in Fig. 1 puts into context the most important concepts auditors are interested in when auditing a company. Indeed, the typical auditing process looks at a the company decides which regulations are pertaining, how it implements its business processes, how it checks for violations, and so on. In short, the auditing process is embedded in a so-called compliance management life cycle [18].

3 Designing Compliance Governance Dashboards (CGDs)

To aid the internal evaluation and to help a company pass external audits, a concise and intuitive visualization of its compliance state is paramount. To report on compliance, we advocate the use of a web-based CGD, whose good design is not trivial [4][14]. It is important to understand how: i) the information auditors expect to find look like; ii) large amounts of data can be visualized in an effective manner, and how data can be meaningfully grouped and summarized; and iii) to structure the available information into multiple pages, that is, how to intuitively guide the user through the wealth of information. Each page of the dashboard should be concise and intuitive, yet complete and expressive. It is important that users are immediately able to identify the key information in a page, but that there are also facilities to drill-down to details.

Designing a CGD requires mastering some new concepts in addition to those discussed above. Then, the new concepts must be equipped with a well-thought navigation structure to effectively convey the necessary information. Here, we do not focus on how data are stored and how rules are evaluated; several proposals and approaches have been conceived so far for that (see Section 4), and we build on top of them.

3.1 A Conceptual Model for CGDs

In Fig. 2 we extend the conceptual model (Fig. 1) to capture the necessary constructs for the development of a CGD (bold lines represent new entities and their respective interrelations). The extensions aim at (i) providing different *analysis perspectives,* (ii) *summarizing* data at different levels of abstraction, and (iii) enabling drill-down/roll-up features (from aggregated data to detailed data, and vice versa).

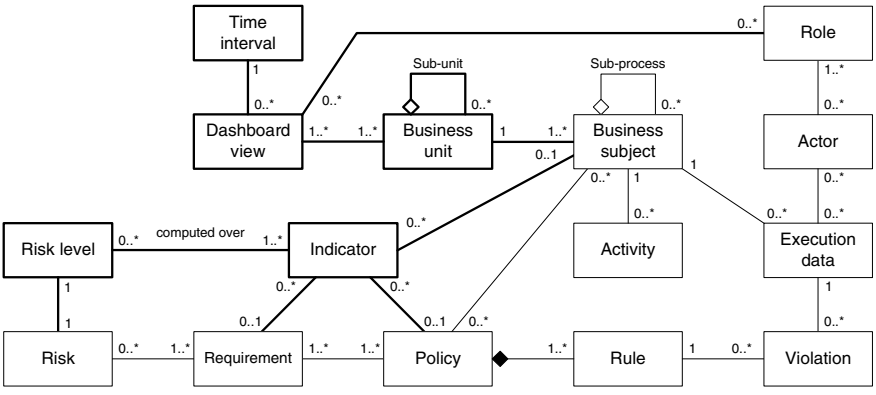


Fig. 2. Conceptual model for CGDs (dashboard-specific constructs are in bold)

The *Dashboard view* entity represents individual views over the compliance status of the company. A view is characterized by the user role that accesses it, e.g., IT specialists, compliance experts, or managers. Each of these roles has different needs and rights. For instance, managers are more interested in aggregated data, risk levels, and long time horizons (to take decisions); IT personnel are interested in instance-level data and short time spans (to fix violations). A view is further characterized by the *time interval* considered for showing data (e.g., day or year), also providing for the historical analysis (e.g., last year) and supporting different reporting purposes (operative, tactical, strategic). Finally, a view might be restricted to some of the company's *business units*, based on the role of the user. In summary, views support distinct summarization levels of the available data, ranging over multiple granularity levels.

Effective summarization of data is one of the most challenging aspects in the design of a CGD instrumented with indicators [11]. An *indicator* is a quantitative summarization of a particular aspect of interest in the business, i.e., a metric of how well an objective is being reached. Typically, KPIs (key performance indicators), are used to summarize the level at which business objectives are reached. In our context, we speak about KCIs, referring to the achievement of the stated compliance objectives (e.g., the number of unauthorized accesses to our payroll data).

In general, indicators are computed out of a variety of data and functions; in the context of compliance assessment, however, indicators can typically be related to the ratio of encountered violations vs. compliant instances of a process or activity. As an abstraction of indicator values, we can define taxonomies (e.g., low, medium, high) and use colors (e.g., red, yellow, green) for their intuitive visualization.

3.2 Navigation Design

After discussing the *static* aspects of the design of CGDs, we now focus on the *dynamic* aspect, i.e., on how to structure the interaction of users with the dashboard, and on how users can explore the data underlying the dashboard application. Specifically, on top of the conceptual model for CGDs we now describe how complex data can be organized into hypertext pages and which navigation paths are important.

For this purpose, we adopt the Web Modeling Language (WebML [2]), a conceptual modeling notation and methodology for the development of data-intensive web applications. We use the language for the purpose of illustration only (we show a simplified, not executable WebML schema) and intuitively introduce all the necessary constructs along with the description of the actual CGD navigation structure.

The WebML hypertext schema (Fig. 3) describes the organization of our ideal CGD. It consists of five *pages* (the boxes with the name labels in the upper left corner), Compliance Home being the home page. Each page contains a number of *content units*, which represent the publication of contents from the data schema in Fig. 2 (the *selector* condition below the units indicates the source data entity). Usually, there are many *hyperlinks* (the arrows) in a hypertext schema, representing the navigations a user might perform, but, for simplicity, we limit our explanation to only those links that represent the main navigation flow. Links carry *parameters*, which represent the selection done by the user when activating a link (e.g., the selection of a process from a list). For the purpose of reporting on compliance, we define a new content unit (not part of WebML), the *compliance drill-down* unit, which allows us to show compliance data in a table-like structure (see the screenshots in Fig. 4).

Let's examine the CGD's structure (Fig. 3): The home page of the CGD provides insight into the compliance state of the company at a glance. It shows the set of most important indicators (Main indicators *multidata* unit) and a set of indicators grouped by policy (IndByPolicy *hierarchical index* unit). Then, we show the (BUnits/Regul.) unit that allows the user to drill-down from business units to processes and from regulations to policies. A click on one of: i) the processes leads the user to the Regulations by Activity page; ii) regulations leads her to the Rules by BusinessUnits page; and iii) the cell of the table leads her to the Rules by Activity page. After the selection of a process, in the Regulations by Activity page the user can inspect the compliance state of each activity of the selected process with the given regulations and policies (RegByActivity), a set of related indicators (BPIndicators unit; the unit consumes the Process parameter), and the details of the selected process (Process *data* unit). Similar details are shown for policies in the Rules by BusinessUnits page, which allows the user to inspect the satisfaction of individual compliance rules at business unit or process level (RulesByBU). A further selection in the compliance drill-down units in these last two pages or the selection of a cell in the BUnits/Regul. unit in the home page

leads the user to the Rules by Activity page, which provides the user with the lowest level of aggregated information. It visualizes the satisfaction of the compliance rules of the chosen policy by the individual activities of the chosen process (RulesByActivity), along with the details of the chosen policy and process and their respective indicators. A further selection in this page leads the user to the Compliance violations page, which shows the details of the violations related to the chosen process/policy combination at an instance level in the Violations *index* unit.

The navigation structure in Fig. 3 shows one of the possible views over the data in Fig. 2, e.g., the one of the internal compliance expert. Other views can easily be added by restraining access to data and defining alternative navigation structures. Each page provides a distinct summarization level from high-level information to low-level details. The time interval for the visualization can be chosen in each of the pages.

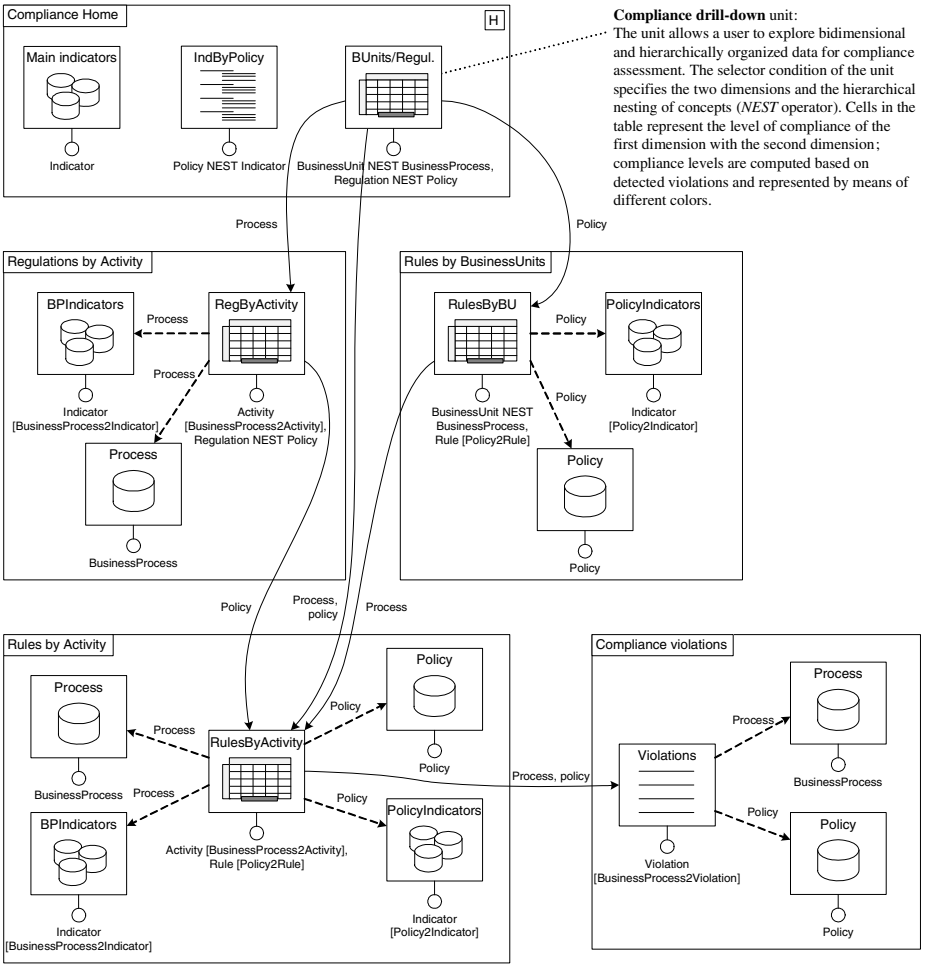
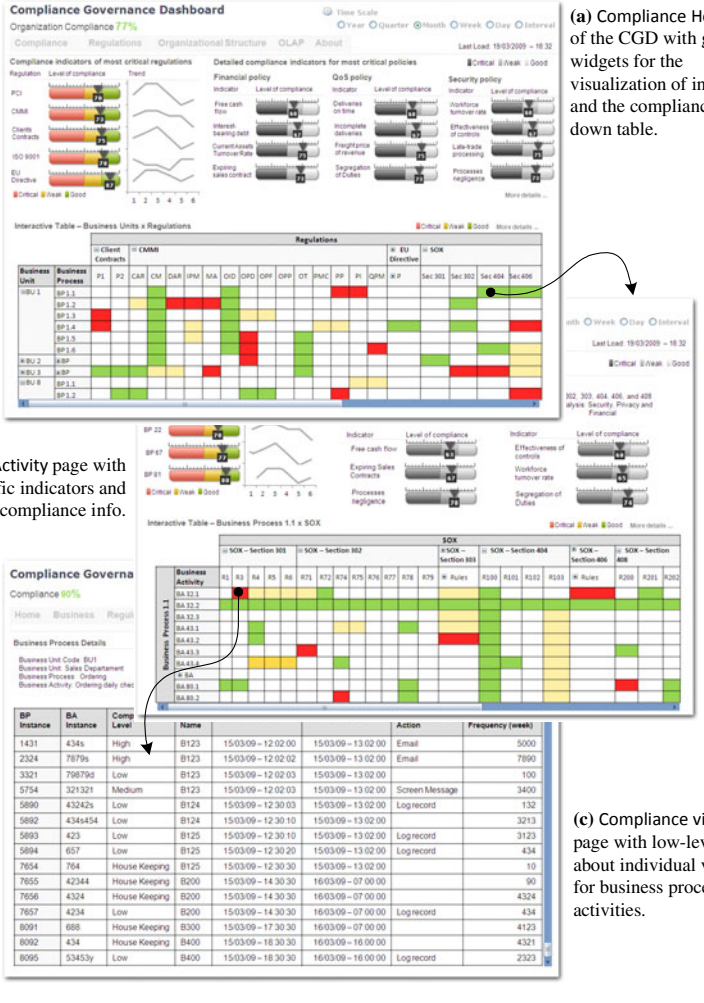


Fig. 3. WebML hypertext schema structuring the navigation of CGD concepts and data

3.3 CGDs in Practice

In Fig. 4 we illustrate some screenshots from our prototype CGD, in order to illustrate its look and feel. The screenshots show views that consistently present our ideal CGD. Fig. 4(a) shows the Compliance Home page, Fig. 4(b) the Rules by Activity page, and Fig. 4(c) the Compliance violations page.

Compliance Home concentrates on the most important information at a glance, condensed into just one page. The five colored indicators (top left) are the most relevant, showing the most critical non-compliant regulations. The gray indicators (right) report on the compliance with the three main policies. In the bottom, there is the interactive compliance drill-down table containing the compliance performance of business units and processes (rows) in relation to regulations and policies (columns).



(a) Compliance Home page of the CGD with graphical widgets for the visualization of indicators and the compliance drill-down table.

(b) Rules by Activity page with process-specific indicators and activity-level compliance info.

(c) Compliance violations page with low-level details about individual violations for business processes and activities.

Fig. 4. Example CGD screenshots of our prototype implementation

The user can easily reach lower levels of granularity by drilling down on the table. For instance, the Rules by Activity page condenses lower level information concerning a combination of Business Process 1.1 and the company's SOX policy. The colors of the cells represent the compliance performance of each combination (e.g., the Business activity 32.1 presents a critical situation regarding Rule 3 of SOX - Section 301 (red cell) and weak performance regarding Rule 5, and Rule 6 (yellow cells)).

A drill-down on the red cell, for instance, leads us to the Compliance violations page, which provides the lowest level of abstraction in form of a table of event violations of the selected rule. The page illustrates the main information that must be reported to assist internal and external auditors. The data in the particular page reports all violations of one activity in Business Process 1.1 of Business Unit 1, detected considering Rule 3 of SOX - Section 301. Each row of the table represents a distinct violation and the columns contain the typical information required by auditors, e.g., responsible of activity, timestamps, mitigation action, cause of violation.

The amount and position of the graphical widgets for indicators, tables, summaries, and so on are chosen in accordance with our short-term memory and the convention of most western languages that are read from left to right and from top to bottom [4].

4 Related Work

To the best of our knowledge, there are only few works that deal with the problem we address in this paper. For example, [1] studies the problem of designing visualizations (i.e., the representation of data through visual languages) for risk and compliance management. Such study focuses on capturing the information required by users and on providing visual metaphors for satisfying those requirements. In [3], the performance reporting is provided in a model-driven fashion. The framework provides four models: data, navigation, report template, and access control, which jointly help designing a business performance dashboard.

Business Activity Monitoring (BAM) has gained attention in the last decade, and many tools support it. BAM aims at providing aggregated information suitable for performing analysis on data obtained from the execution of business activities. For example, tools such as Oracle BAM, Nimbus and IBM Tivoli aim at providing its users with real-time visual information and alerts based on business events in a SOA. The information provided to users comes in the form of dashboards for reporting on KPIs and SLA violations. The compliance management part of these tools (if any) comes in the form of monitoring of SLA violations, which need the SLA formal specifications as one of its inputs. In our work, we take a more general view on compliance (beyond SLAs, which are a special case to us) and cover the whole lifecycle of compliance governance, including a suitable CGD for reporting purposes.

5 Conclusions and Future Work

In this paper we discussed a relevant aspect in modern business software systems, i.e., compliance governance. Increasingly, industry and academia are investing money and efforts into the development of compliance governance solutions. Yet, we believe CGDs in particular, probably the most effective means for visualizing and reporting on compliance, have mostly been neglected so far. It is important to implement sophisticated solutions to check compliance, but it is at least as important (if not even

more) to effectively convey the results of the compliance checks to a variety of different actors, ranging from IT specialists to senior managers.

Our contribution is a conceptualization of the issues involved in the design of CGDs in service- and process-centric systems, the definition of a navigation structure that supports drill-down/roll-up features at adequate levels of detail and complexity, and a set of examples that demonstrate the concepts at work. Our aim was to devise a solution with in mind the real needs of auditors and – more importantly – with the help of people who are indeed involved every day in the auditing.

References

1. Bellamy, R., Erickson, T., Fuller, B., Kellogg, W., Rosenbaum, R., Thomas, J., Vetting Wolf, T.: Seeing is believing: Designing visualizations for managing risk and compliance. IBM Systems Journal 46(2), 205–218 (2007)
2. Ceri, S., Fraternali, P., Bongio, A., Brambilla, M., Comai, S., Matera, M.: Designing Data-Intensive Web Applications. Morgan Kaufmann Publishers Inc., USA (2002)
3. Chowdhary, P., Palpanas, T., Pinel, F., Chen, S.-K., Wu, F.Y.: Model-driven Dashboards for Business Performance Reporting. In: Proceedings of the 10th IEEE EDOC, pp. 374–386 (2006)
4. Few, S.: Information Dashboard Design: The Effective Visual Communication of Data, p. 223. O'Reilly Media, Inc., Sebastopol (2006)
5. Hagerty, J., Hackbush, J., Gaughan, D., Jacobson, S.: The Governance, Risk Management, and Compliance Spending Report, 2008-2009: Inside the $32B GRC Market. AMR Research (2008)
6. Saqid, S., Governatori, G., Naimiri, K.: Modeling Control Objectives for Business Process Compliance. In: Alonso, G., Dadam, P., Rosemann, M. (eds.) BPM 2007. LNCS, vol. 4714, pp. 149–164. Springer, Heidelberg (2007)
7. Giblin, C., Müller, S., Pfitzmann, B.: From Regulatory Policies to Event Monitoring Rules: Towards Model-Driven Compliance Automation. IBM Research Report (October 2006)
8. Namiri, K., Stojanovic, N.: A Semantic-based Approach for Compliance Management of Internal Controls in Business Processes. In: CAiSE 2007, pp. 61–64 (2007)
9. Trent, H.: Products for Managing Governance, Risk, and Compliance: Market Fluff or Relevant Stuff? In-Depth Research Report, Burton Group (2008)
10. Lam, J.: Operational Risk Management – Beyond Compliance to Value Creation. White Paper, Open Pages (2007)
11. Imrey, L.: CIO Dashboards: Flying by Instrumentation. Journal of Information Technology Management 19(4), 31–35 (2006)
12. Evans, G., Benton, S.: The BT Risk Cockpit – a visual approach to ORM. BT Technology Journal 25(1) (2007)
13. Papazoglou, M.P.: Compliance Requirements for Business-process-driven SOAs. E-Gov. Ict Professionalism and Competences Service Science 280, 183–194 (2008)
14. Read, A., Tarrel, A., Fruhling, A.: Exploring User Preference for the Dashboard Menu Design. In: Proceedings of the 42nd Hawaii Intern. Conf. on System Sciences, pp. 1–10 (2009)
15. Allman, E.: Complying with Compliance. ACM Queue 4(7), 18–21 (2006)
16. Cannon, J., Byers, M.: Compliance deconstructed. ACM Queue 4(7), 30–37 (2006)
17. Oberortner, E., Zdun, U., Dustdar, S.: Tailoring a Model-Driven Quality-of-Service DSL for Various Stakeholders. In: Workshop on Modeling in Software Engineering, MiSE (2009)
18. Daniel, F., Casati, F., D'Andrea, V., Strauch, S., Schumm, D., Leymann, F., Mulo, E., Zdun, U., Dustdar, S., Sebahi, S., de Marchi, F., Hacid, M.: Business Compliance Governance in Service-Oriented Architectures. In: Proceedings of AINA 2009. IEEE Press, Los Alamitos (May 2009)