A Roadmap for Research in Business Process Compliance

Shazia Sadiq

School of Information Technology and Electrical Engineering,
The University of Queensland,
St. Lucia, QLD 4067,
Brisbane, Australia
shazia@itee.uq.edu.au

Abstract. We stipulate that for researchers interested in the computational and organizational aspects of research in compliance and risk management, there are two key aspects to be considered. Firstly, research should aim towards a sustainable methodology for compliance management. Secondly, research in this highly multi-disciplinary area must be aligned with industry demands in order to maximize potential for impact and relevance. We have presented a snapshot recommendation for the two aspects, namely a compliance by design methodology that has a fundamentally preventative focus, and an industry driven research agenda that is derived through expert opinion and practitioner feedback. We hope that this will assist researchers to better position their future research endeavors in the area of risk and compliance management.

1 Introduction

Developing strategies to manage inevitable regulatory shifts emerging from government and global reactions to the financial crisis is high on corporate agendas and will continue to be in the coming years. Finding resources to ensure compliance with regulations and managing compliance obligations in a cost effective way are key issues that organisations currently face. Regulatory pressures can be found across all industry sectors and affect all sizes of organization. In addition, pervasiveness of the globalised economy means that compliance may span across geographical boundaries. In these times, more than ever before, organisations seek tools, techniques and methods that allow them to design and implement an effective and efficient compliance regimen. In this project, we will address a particular aspect of this large and complex problem, which is to assist organisations in measuring the adequacy of their control portfolios against particular regulations.

Compliance essentially means ensuring business processes, operations and practice are in accordance with a prescribed and/or agreed set of norms. Compliance requirements may stem from legislature and regulatory bodies (e.g. Sarbanes-Oxley, Basel II, HIPAA), standards and codes of practice (e.g. SCOR, ISO9000) and also business partner contracts. Compliance directives can be complex, vague and often require interpretation. Business will typically deal with a number of regulations/standards at one time, which may have overlapping and even conflicting requirements.

W. Abramowicz, L. Maciaszek, K. Węcel (Eds.): BIS 2011 Workshops, LNBIP 97, pp. 1–4, 2011.

In general, a compliance regimen must include three interrelated but distinct perspectives on compliance, *viz.* corrective, detective and preventative perspective. *Corrective* measures can be undertaken due to a number of reasons, but, when undertaken in a proactive manner, position the organisationfavourably with regulators or other control authorities. *Detective* measures are typically based on reporting and traditional audits conducted 'after-the-fact'. A shortcoming of the above two approaches (in varying degrees of impact) is lack of sustainability. Even with an automated detection facility, the hard coded check repositories can quickly grow out of control, making it difficult to evolve and maintain them for changing legislatures and compliance requirements.

A sustainable approach for achieving compliance should fundamentally have a *preventative* focus, thus achieving 'compliance by design' (Sadiq et al. 2007). That is, compliance should be embedded into the business practice, rather than seen as a distinct activity. Intuitively, the role of business process platforms seem instrumental to this end, as they have the potential to contribute to all three perspectives, namely preventative (through compliance aware process design (Lu et al. 2007)), detective (through business process monitoring tools (van der Aalst et al. 2003) and corrective (through model-driven execution of business transactions (Giblin et al. 2007). However, the disparate life cycles, ownership and governance mechanisms of the business and compliance functions within organisations indicates that driving compliance through business processes management is not trivial. In (Sadiq et al. 2010), a methodological framework is presented to align business processes with regulatory compliance obligations.

The framework is based on six key interrelated tasks, namely: (1) Controls directory management in order to provide requisite content management functionality which may span several business functions within the organization as well as several regulations that impact on them; (2) Ontological (or conceptual) alignment between the controls, risk and business processes that are related; (3) Modeling of the controls in order to provide conceptually faithful and machine interpretable specifications for compliance obligations; (4) Tools, techniques and methods for process model enrichment, which may include various checking, annotation and enhancement approaches; (5) assistance with compliance enforcement through targeted tools and technologies such as control automation, simulation for enriched process models etc. and lastly (6) compliance monitoring to ensure continued surveillance where in technologies such as data mining, business intelligence etc. are instrumental.

The various tasks of the above framework hold a number of research challenges. In (Syed Abdullah et al. 2009) we embarked upon a large review of existing information systems research literature to identify contributions that may help fulfill the challenges of such a framework as well as to gain an understanding of the current research landscape.

Furthermore we conducted an empirical study that contrasts the review of literature with industry input derived from expert professionals in the Australian compliance industry. The study has uncovered insights into problematic areas within the compliance management domain and the results show a glaring gap with current research efforts. Below is a summary of the identified research agenda, which we hope can direct ICT and Information System researchers towards industry relevant research questions:

First and foremost, there is an urgent need for proper **benchmarking studies** to help address the challenge of high cost. Particularly for SMEs, there is high cost and great difficulty in **measuring the adequacy of controls** for principles based regulations where the onus is on the organization to design an appropriate compliance regimen. Benchmarking and best practice studies will allow improvement of controls effectiveness, a reduction of costs, and an improved potential to deal with resistance to change through demonstrating methods used by others. Such additional knowledge can further help alleviate the perception of legislation weaknessesin principles based regulations and consequently promote regulation acceptance.

There is also a need for investigation of **process reference models** relating to various regulations. A focus on the development of such reference models and the study of the impact of the use of such models in organizations (i.e. impact on compliance management spending, frequency of breaches, etc) is largely missing in Information Systems research. The development of proven reference models, however, may significantly lessen the cost of compliance management in organizations.

The culture of compliance is ingrained in the daily rituals of each of the firm's employees, including senior management, who must learn to lead by example. There is a clear lack of Information Systems research on **organisationalbehavior**in the context of compliance management. In particular we see a need for investigation of how IT and IS tools can be used to incentivize employees to 'do the right thing' and adapt their practices. There is also a need for the development of relevant IT and IS tools that can help facilitate employee training for compliance management, promote communication among staff and increase organizational capacity to manage its compliance knowledge base.

How the compliance (and risk) factor interrelates with the operations of business units is understudied, with only a small number of researchers working on the **conceptualisation of compliance and risk** requirements per se let alone their inter-relationships with business processes and business activities. A comprehensive and well-grounded conceptual model for compliance and risk is needed.

Further to the point above, tools and methods are needed to **annotate, enhance, analyse and simulate business models** with compliance and risk modeling elements. This will facilitate better coordination between an organization's compliance and business functions and help employees understand compliance value and business relevance.

Although reporting and monitoring tools of high sophistication are available, there is little development towards tools that provide **specialized solutions in monitoring and analysing** compliance related data (partly due the absence of any generic conceptual models for GRC), thus causing big problems for organisations required to create evidence of compliance. Accordingly, we see a need for affordable IT and IS tools that facilitate compliance management self-audits and compliance monitoring activities in general. Furthermore, there is also a clear need for tools that facilitate the identification of non-compliance processes with respect to a given regulation.

Lastly, although frequency of change, as well as inconsistency and overlaps in regulations is beyond the realm of IS research, studies to understand the **impact of regulation changes** (inconsistencies and overlaps) can promote better understanding of the cost of compliance and allow business to lobby for regulatory reform where needed. Multi disciplinary research is warranted in order to cover legal, business and IT aspects. From an Information Systems perspective, there is a need for solutions that can filter out updates that are not relevant to a given organization or industry sector, thus reducing the amount of information that the organization has to process in order to update or assess their compliance management initiatives.

In summary, we stipulate that for researchers interested in the computational and organizational aspects of research in compliance and risk management, there are two key aspects to be considered. Firstly, research should aim towards a sustainable methodology for compliance management. Secondly, research in this highly multi-disciplinary area must be aligned with industry demands in order to maximize potential for impact and relevance. Above, we have presented a snapshot recommendation for the two aspects with the hope that it will assist researchers to better position their future research endeavors.

Acknowledgements. I would like to acknowledge the following colleagues for their contributions to various aspects of this work: Syed Norris Abdullah, The University of Queensland; Guido Governatori, NICTA, Australia; Marta Indulska, The University of Queensland; Ruopeng Lu, SAP Australia; ZoranMilosovic, deontik.com; Ingo Weber, University of NSW; Michael zurMuehlen, Stevens Institute of Technology.

References

Giblin, C., Müller, S., Pfitzmann, B.: From Regulatory Policies to Event Monitoring Rules: Towards Model-Driven Compliance Automation. IBM Research Report RZ3662 (2006)

Lu, R., Sadiq, S., Governatori, G.: Compliance Aware Business Process Design. In: 3rd International Workshop on Business Process Design (BPD 2007) In Conjunction with the 5th International Conference on Business Process Management. LNCS. Springer, Heidelberg (2007)

Sadiq, S., Governatori, G.: A Methodological Framework for Aligning Business Processes and Regulatory Compliance. In: Brocke, J., Rosemann, M. (eds.) Handbook of Business Process Management. Introduction, Methods and Information Systems Series: International Handbooks on Information Systems. Springer, Heidelberg (2010)

Sadiq, 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)

Syed Abdullah, N., Indulska, M., Sadiq, S.: A Study of Compliance Management in Information Systems Research. In: The 17th European Conference on Information Systems (ECIS 2009), Verona, Italy (2009)

Syed Abdullah, N., Sadiq, S., Indulska, M.: Emerging Challenges in Information Systems Research for Regulatory Compliance Management. In: Pernici, B. (ed.) CAiSE 2010. LNCS, vol. 6051, pp. 251–265. Springer, Heidelberg (2010)

van der Aalst, W.M.P., van Dongen, B.F., Herbst, J., Maruster, L., Schimm, G., Weijters, A.J.M.M.: Workflow Mining: A Survey of Issues and Approaches. Data & Knowledge Engineering 47(2), 237–267 (2003)