Toward a Holistic Method for Regulatory Change Management

Sagar Sunkle and Vinay Kulkarni
Tata Consultancy Services Research, 54B Hadapsar Industrial Estate, Pune 411028, India
{*sagar.sunkle,vinay.vkulkarni@tcs.com*}

Keywords: Regulatory Change Management, GRC, Formal Compliance Checking, Norm Change, Business Process Change Propagation, Risk Modeling.

Abstract: Complexity of regulatory compliance is heightened for modern enterprises due their global footprints and multiple regulations they are subjected to across varied domains and geographies and continual changes therein. This necessitates a method for compliance management that is capable of establishing compliance to both regulations and changes to regulations from a holistic perspective of governance, risk, and compliance (GRC). We propose such a method using a conceptual model of integrated GRC whereby formal compliance checking and norm change techniques for regulations represented as formal rules are coupled with business process change propagation and risk modeling. The method also considers legal and business goals of regulators and regulatees respectively in enacting compliance to regulation and changes therein. The method is substantiated with a brief example of a real world banking regulation.

1 INTRODUCTION

Modern enterprises need to comply with multiple domain- and geography-specific regulations. Non-compliance results not only in putting the hard earned reputation of enterprises at stake, but may also lead to personal liability and risk for board directors and top management (Alberth et al., 2012). The compliance problem is acerbated by continual changes to regulations (French Caldwell, 2013; English and Hammond, 2014). Enterprises not only have to be compliant with multiple regulations but also *remain compliant as these regulations change*. Regulatory change management therefore assumes a very important role in any regulatory compliance framework and practices. Proper regulatory change management requires adoption of right attitude at the top management level and machinery to enact compliance to both regulations and changes to regulations.

Interestingly, both industrial governance, risk, and compliance (GRC) solutions and formal compliance checking techniques address the problem of compliance to regulations and regulatory changes in such a way that a compliance solution that is better than both can be obtained by combining the best features from both. Industrial GRC solutions mostly provide informal, content management-based, document-driven, and expert-dependent ways of solving the compliance problem (French Caldwell, 2013), but at the same time support an integrated view of G, R, and C tools and practices, which is a desirable feature since changes in regulations affect aspects of governance and risk as much as they affect already compliant processes (Racz et al., 2011). An integrated GRC solution can help in managing and evaluating assumptions in the current business model and assessing the effectiveness of strategies for new business models (Switzer et al., 2013). Formal compliance checking techniques, in comparison to industry GRC solutions, provide formal guarantees of compliance and several formal compliance analysis possibilities (Becker et al., 2012). But research in formal compliance checking, although extensive, has focused on segments of topics such as compliance checking of business process, changes to legal norms, business process change, and risk modeling without providing techniques from an integrated GRC perspective (Neiger et al., 2006; Schäfer et al., 2011).

In this position paper, we propose to relate formal norm change techniques based on formal compliance checking techniques with business process change propagation and risk modeling based on an integrated GRC perspective. To elaborate our approach, we use elements from a conceptual model for integrated GRC (Vicente and da Silva, 2011). Starting with key elements, we show how G, R, C concerns are treated separately as far as formal compliance checking techniques are considered and eventually we arrive at a

Sunkle S. and Kulkarni V.
Toward a Holistic Method for Regulatory Change Management.
DOI: 10.5220/0005887402180223
In *Proceedings of the Fifth International Symposium on Business Modeling and Software Design (BMSD 2015)*, pages 218-223
ISBN: 978-989-758-111-3

method which ensures that all three concerns are addressed while using these techniques. We believe that this method has the potential to provide formal guarantees and analysis benefits along with holistic treatment of G, R, and C concerns.

The paper is arranged as follows. In Section 2, we begin with a conceptual model of GRC and motivate why G, R, C concerns need to be addressed together, and how the current formal research techniques treat these in a divided manner. In Section 3, first we review norm change techniques, business process change propagation in connection with norm change, and risk modeling techniques in that sequence. We then put forth a method for a formal treatment of regulatory changes on top of integrated GRC model. In Section 4 present a very brief example of how this method may be applied to a Know Your Customer (KYC) regulation of Reserve Bank of India (RBI). We discuss some pertinent pointers with regards using integrated GRC perspective for cost-effective enterprise decision making in Section 5 and Section 6 concludes the paper.

2 THREE DIMENSIONS OF REGULATORY CHANGE

GRC is an integrated, holistic approach to organization-wide governance, risk and compliance (Racz et al., 2010). Taking the stance that different enterprises would define GRC in their own way, (Vicente and da Silva, 2011) came up with a conceptual model to define the domain of of integrated GRC. We illustrate an adapted version of this model in Figure 1.

Note that Figure 1 deliberately includes elements common to G, R, and C, namely Key Objectives, Policies, Internal Controls, Processes, and Risks. Additionally it contains elements specific to C, namely Regulations and Standards, and elements specific to R, namely Inquires/Surveys, Risk Appetite, Issues, and Heat Maps. *Governance* is responsible for *risk* and *compliance* oversight, as well as evaluating performance against enterprise's Key Objectives. Compliant enterprises need an effective approach to verify that they are in conformity with rules set from external Regulations and Standards and internal Policies which are eventually related to and are exercised in terms of Internal Controls. Enterprise's Key Objectives are achieved by Processes which have an associated set of Risks. Internal Controls should be implemented on top of Processes such that they are able to *track, prevent, detect, and correct* Risks associated with Processes and thereby *fulfill* Key Objectives of

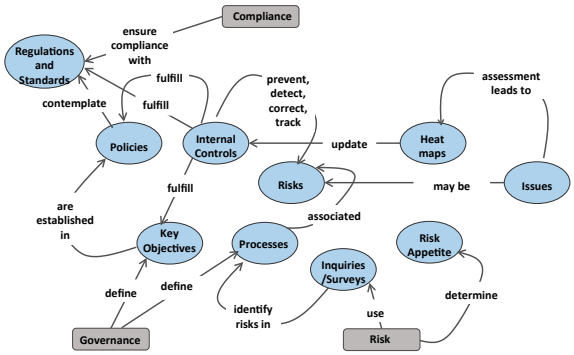

Figure 1: Integrated GRC conceptual model adapted from (Vicente and da Silva, 2011).

the enterprise.

Figure 1 represents integrated GRC without differentiating between compliance to Regulations and Standards and compliance to *changes in* Regulations and Standards. The elements related to R not covered in the reading above indicate essentially the industrial GRC way of risk-adjusted decision making in compliance to both regulations and changes to regulations. Based on predetermined Risk Appetite, Risks associated with Processes are identified by expert Inquiries/Surveys. Certain issues with Internal Controls may also be treated as Risks. Based on Inquiries/Surveys, risk Heat Maps are created pointing to specific Processes and business functions and Internal Controls are updated based on evaluation of Heat Maps.

In contrast to industry GRC solutions, formal compliance checking approaches help in reducing the burden on experts by using formal models of regulations and business processes. An extensive research exists in formal compliance checking of regulations where methods to check formalized models of business processes against models of regulations are explicated (Sadiq et al., 2007; Liu et al., 2007; Ly et al., 2010). Additionally, some of these approaches even enable formal proofs of (non-)compliance by utilizing diagnostic information about process activities (Antoniou et al., 2008; Governatori et al., 2009). But research on formal compliance checking of *changes* in regulations is not yet coordinated. This is illustrated in Figure 2.

Figure 2 adds *changes* to key elements of Figure 1 and positions research in formal methods of norm change, business process change propagation and risks associated with changes on top of these elements. It can be seen that links between the common elements of GRC, namely Processes, Internal Controls, and Risks do not hold as illustrated by relations between elements drawn in red. Some relations are

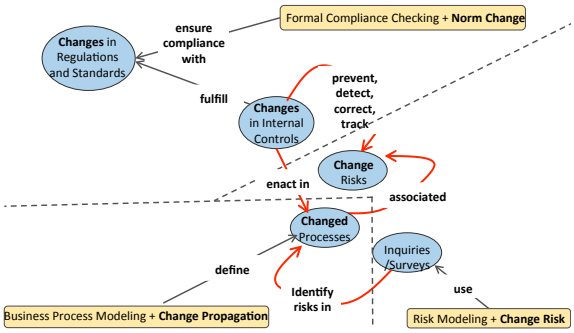

Figure 2: Research on changes in norms, business process, and risks.

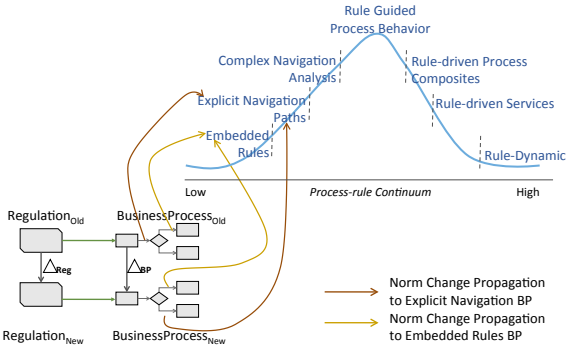

Figure 3: Propagating norm changes to processes.

different from Figure 1, because they depict the way *formal* techniques solve individual problems of norm change, business process change, and change risks. For an effective and efficient regulatory change management, elements in the three dimensions of norm change, business process change, and change risks need to be coordinated. They can be coordinated precisely by focusing on relations drawn in red. We elaborate this in the next section by reviewing existing work in each of these dimensions and then proposing a method for coordination.

3 TOWARD A METHOD FOR REGULATORY CHANGE

Norm Change Norm change research focuses on different ways in which contraction, expansion, and revision of legal theories can be achieved. Several interesting aspects have to be taken into consideration to formally model norm changes as enumerated below:

1. Distinction between *legal* (obligations, prohibitions and permissions) and *counts-as* rules
2. Distinction between norms and their legal effects and the notion of *defeasiblity*
3. Distinction between *Ex Tunc* and *Ex Nunc* norms
4. Ways in which expansion and contraction of legal effects is achieved
5. *Interpretation* mechanism for balancing goals of norms and legal effects

Each aspect above is elaborated further below.

While legal rules specify the ideal behavior and can be changed by the legislative system such as a regulatory body, the *counts-as* rules provide definitions of institutional concepts. The applicability conditions of legal rules refer to these institutional concepts, rather than to the so called brute facts (Boella et al., 2009).

Considerable research in norm change uses extensions of defeasible logic (Governatori and Rotolo, 2008a; Governatori and Rotolo, 2008b; Boella et al., 2009) and is based on formal compliance checking techniques using the same extensions of defeasible logic (Antoniou et al., 2008) with at least two implementations, namely Formal Contract Language (Sadiq et al., 2007) and DR-Prolog (Antoniou et al., 2008). The notion of *defeasibility* helps in terms of revising legal effects without necessarily revising norms. In other words, obligations can change with normative system being the same, as for instance, due to change in the world, new obligations can be attached or old obligations can be detached from the legal norms. The norms themselves can be distinguished as *Ex Tunc* or *Ex Nunc* based on how the legal effects are realized.

Ex Tunc norm is a norm that retroactively changes the legal effects of actions committed prior to the existence of the norm, whereas an *Ex Nunc* norm affects only actions committed after the existence of the norm.

Based on the notions of *Ex Tunc* and *Ex Nunc* norms expansion can be prospective and retroactive promulgation (Gómez-Sebastià et al., 2012) and contraction can be annulment or abrogation respectively. Since regulations are represented as rules in the implementation, different ways have been suggested to expand and contract legal effects such as adding or removing rules, adding exception via defeaters, i.e., rules that can be used for defeating conclusions[1], or changing rule superiority.

Finally, the *interpretation* mechanism enables adapting norms after their creation to the unforeseen situations in order to achieve the social goals they have been planned for (Boella et al., 2009).

The research in norm change does not propose how to propagate changes with regards legal effects realized as modified rule base to processes. We re-

[1]For the formal specification of defeasible logic, its extensions, and proof theory, reader is requested to refer to (Antoniou et al., 2008; Boella et al., 2009).

view the research in business process change propagation in order to suggest a way to do so.

Business Process Change Propagation We focus on the fact that industry GRC solutions as well various formal compliance checking techniques enact regulations in processes in terms of rules. The way rules are integrated into business processes may depend on where the default level of rule and process integration in given enterprise lies along what is called as *process-rule continuum* (Sinur, 2009; Koehler, 2011). This is illustrated in Figure 3 top right.

Seven scenarios with regards how rules are integrated with processes were described in (Sinur, 2009) and later elaborated by (Koehler, 2011). Processes with *embedded rules* encode all process paths into the process without explicit rules and denote processes that do not change frequently. In processes with *explicit navigation rules* explicit rules manage and direct the process routes for each process instance. At the end of the continuum with *fully rule-dynamic* processes, rules dynamically configure processes and rules themselves may change.

On the bottom left of Figure 3, we depict the regulation change scenario. Here, original regulations Regulation_{Old} with which original business process $\text{BusinessProcess}_{old}$ was compliant with, is changed to Regulation_{New}. The new regulations need to be propagated to the original business process in a compliant manner to yield $\text{BusinessProcess}_{New}$. Δ_{Reg} captures the change operations in terms of rule addition/removal, defeater addition/removal and rule superiority assertions. Δ_{BP} is a change sensitive function of Δ_{Reg} meaning that instead of reapplying new rules from scratch, only changes in rules are reflected into business processes.

For *embedded rules* type of process, the change propagation is most costly since the process has to be redesigned by first finding how rules are implicitly embedded into the processes. The change propagation becomes easier along the continuum, such as for processes of an enterprise that fall between the types of *explicit navigation rules* processes and *complex navigation and analysis*. In processes with *explicit navigation rules*, processes contain business rule tasks that determine when a rule component is executed. This is the most common scenario in enterprises (Koehler, 2011). Variation of this type is where rules are annotated to a task. In that case, to propagate changes in regulations, the changed set of rules may be directly annotated to the original task. Next, we quickly review change risk modeling.

Change Risk Modeling As illustrated earlier in Figure 2, a standard process of Inquiries/Surveys of Changed Processes may be carried out to ascertain risks resulting from regulation changes that are now propagated to the business processes. The basic formulation for risk estimation is the probability of the identified event evaluated by its consequence. We believe that by incorporating the computation of goals related with norms and legal effects (Boella et al., 2009) into risk modeling, consequences of events (i.e., legal effects) can be computed with more reliability.

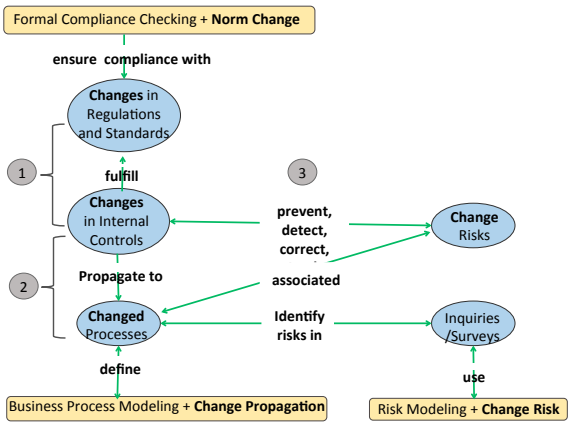

Figure 4: Steps for holistic regulatory change management.

Method for Regulatory Change Using formal models of norm change (step 1), changes in regulations can be propagated to business process based on the level of rule integration (step 2) and finally risk can be computed for these changes (step 3). This method is illustrated in Figure 4 by rearranging Figure 2. A possible application of method illustrated in Figure 4 for Know Your Customer (KYC) regulations for Indian banks by Reserve Bank of India (RBI) is briefly described next.

4 CASE STUDY

The key goal of KYC regulations is curbing money laundering, and it is achieved by a basic due diligence activity of admitting customers of given type with related set of identity and address documents as specified in several annexes of KYC. Depending on customer types, there may be other due diligence activities that a bank may be obligated to carry out, such as for instance, in case of politically exposed persons or foreign policy investors[2]. In accordance with aspects of norm change specified in Section 3, following can be observed:

1. Definitions of *Customer*, *beneficiary owner*, and

[2]See KYC Master Circular `http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9074`

other institutional concepts can be modeled as *counts-as* rules while the due diligence activities for each type of customer can be modeled as *legal* rules.
2. Distinction between norms and legal effects is observable in the regulation change in KYC 2014 from earlier KYC master circulars where introduction of new customer by existing account holders was no longer kept mandatory.
3. While most of KYC regulations are *Ex Nunc*, certain customer types have been introduced, such as foreign policy investors in 2014, and customers matching that profile but admitted in 2013 may be subjected to corresponding regulations *Ex Tunc*.
4. When KYC regulations are implemented as rules (say in DR-Prolog), expansion, contraction, and revision of KYC regulation can be carried out by rule addition/removal, addition of exceptions, and changing rule superiority.
5. Finally, RBI goal of anti money laundering and banks' goal of reducing risk liability while admitting customers across low to high risk profiles could be modeled using goals of norms and legal effects.

The key processes indicated by RBI KYC are new account opening, account transfer, third party transactions, and transaction monitoring. These are the processes to which changes in regulations are propagated. RBI KYC also provides guidelines for risk categorization of customers based on customer types and transaction history which can be used to model risks for specific customers and also changes in risk profiles as regulations change.

5 DISCUSSION

Change Sensitive Propagation Figure 3 shows that regulatory changes are propagated to business processes. It is less likely but possible that business processes change and now original regulations must be complied with again. In both these cases, propagation should be change sensitive. While we proposed such a way when propagating regulatory changes in terms of rules to business processes, when business processes change, the re-applicability of original regulations to changed processes should be change sensitive as well.
Enterprise Context In an earlier work, we showed how to capture enterprise transformation due to various change drivers from as-is to to-be architecture using enterprise architecture (EA), intentional, and system dynamics models (Sunkle et al., 2013). EA models act as descriptive models whereas intentional models and system dynamics models act as prescriptive or decision making models. We also showed how to incorporate directives such as internal policies and external regulations into enterprise to-be architecture (Sunkle et al., 2014). Existing business processes signify current courses of actions that an enterprise uses to achieve its Key Objectives. Since regulations essentially constrain business processes, it may be possible to relate compliance of specific regulations with achievement of specific Key Objectives. Once this interrelatedness is established, it might be possible to model and reason about how to make best decisions.

6 CONCLUSION

We have proposed a method that uses formal compliance checking, norm change, business process change propagation, and risk modeling to address regulatory change management with an integrated GRC perspective. We briefly discussed application of this method for compliance with KYC regulations. The integrated view paves way toward balancing achievement of business objectives while complying to regulations taking into consideration risks including those concerning compliance.

REFERENCES

Alberth, S., Babel, B., Becker, D., Kaltenbrunner, G., Poppensieker, T., Schneider, S., Stegemann, U., and Wegner, T. (2012). Compliance and control 2.0: Unlocking potential through compliance and quality-control activities. *McKinsey Working Papers on Risk*, 33.

Antoniou, G., Bikakis, A., Dimaresis, N., Genetzakis, M., Georgalis, G., Governatori, G., Karouzaki, E., Kazepis, N., Kosmadakis, D., Kritsotakis, M., Lilis, G., Papadogiannakis, A., Pediaditis, P., Terzakis, C., Theodosaki, R., and Zeginis, D. (2008). Proof explanation for a nonmonotonic semantic web rules language. *Data & Knowledge Engineering*, 64(3):662 – 687.

Becker, J., Delfmann, P., Eggert, M., and Schwittay, S. (2012). Generalizability and applicability of modelbased business process compliance-checking approaches — a state-of-the-art analysis and research roadmap. *BuR — Business Research*, 5(2):221–247. Publication status: Published.

Boella, G., Governatori, G., Rotolo, A., and van der Torre, L. (2009). *Lex Minus Dixit Quam Voluit*, *Lex Magis Dixit Quam Voluit*: A formal study on legal compliance and interpretation. In Casanovas, P., Pagallo, U., Sartor, G., and Ajani, G., editors, *AI Approaches to the Complexity of Legal Systems.*, volume 6237 of *Lecture Notes in Computer Science*, pages 162–183. Springer.

English, S. and Hammond, S. (2014). Cost of compliance 2014 (Thomson Reuters Accelus).

French Caldwell, J. A. W. (2013). Magic quadrant for enterprise governance, risk and compliance platforms (Gartner).

Gómez-Sebastià, I., Álvarez-Napagao, S., Vázquez-Salceda, J., and Felipe, L. O. (2012). Towards runtime support for norm change from a monitoring perspective. In Ossowski, S., Toni, F., and Vouros, G. A., editors, *Proceedings of the First International Conference on Agreement Technologies, AT 2012, Dubrovnik, Croatia, October 15-16, 2012*, volume 918 of *CEUR Workshop Proceedings*, pages 71–85. CEUR-WS.org.

Governatori, G., Hoffmann, J., Sadiq, S., and Weber, I. (2009). Detecting regulatory compliance for business process models through semantic annotations. In Ardagna, D., Mecella, M., and Yang, J., editors, *Business Process Management Workshops*, volume 17 of *Lecture Notes in Business Information Processing*, pages 5–17. Springer Berlin Heidelberg.

Governatori, G. and Rotolo, A. (2008a). Changing legal systems: Abrogation and annulment part I: revision of defeasible theories. In van der Meyden, R. and van der Torre, L., editors, *Deontic Logic in Computer Science, 9th International Conference, DEON 2008, Luxembourg, Luxembourg, July 15-18, 2008. Proceedings*, volume 5076 of *Lecture Notes in Computer Science*, pages 3–18. Springer.

Governatori, G. and Rotolo, A. (2008b). Changing legal systems: Abrogation and annulment. part II: temporalised defeasible logic. In Boella, G., Pigozzi, G., Singh, M. P., and Verhagen, H., editors, *Third International Workshop on Normative Multiagent Systems - NorMAS 2008, Luxembourg, July 15-16, 2008. Proceedings*, pages 112–127.

Koehler, J. (2011). The process-rule continuum - can BPMN & SBVR cope with the challenge? In Hofreiter, B., Dubois, E., Lin, K., Setzer, T., Godart, C., Proper, E., and Bodenstaff, L., editors, *13th IEEE Conference on Commerce and Enterprise Computing, CEC 2011, Luxembourg-Kirchberg, Luxembourg, September 5-7, 2011*, pages 302–309. IEEE Computer Society.

Liu, Y., Müller, S., and Xu, K. (2007). A static compliance-checking framework for business process models. *IBM Systems Journal*, 46(2):335–362.

Ly, L. T., Knuplesch, D., Rinderle-Ma, S., Göser, K., Pfeifer, H., Reichert, M., and Dadam, P. (2010). Seaflows toolset - compliance verification made easy for process-aware information systems. In Soffer, P. and Proper, E., editors, *Information Systems Evolution - CAiSE Forum 2010, Hammamet, Tunisia, June 7-9, 2010, Selected Extended Papers*, volume 72 of *Lecture Notes in Business Information Processing*, pages 76–91. Springer.

Neiger, D., Churilov, L., zur Muehlen, M., and Rosemann, M. (2006). Integrating risks in business process models with value focused process engineering. In Ljungberg, J. and Andersson, M., editors, *Proceedings of the Fourteenth European Conference on Information Systems, ECIS 2006, Göteborg, Sweden, 2006*, pages 1606–1615.

Racz, N., Weippl, E., and Seufert, A. (2011). Governance, risk & compliance (GRC) software - an exploratory study of software vendor and market research perspectives. In *Proceedings of the 2011 44th Hawaii International Conference on System Sciences*, HICSS '11, pages 1–10, Washington, DC, USA. IEEE Computer Society.

Racz, N., Weippl, E. R., and Seufert, A. (2010). A frame of reference for research of integrated governance, risk and compliance (GRC). In Decker, B. D. and Schaumüller-Bichl, I., editors, *Communications and Multimedia Security, 11th IFIP TC 6/TC 11 International Conference, CMS 2010, Linz, Austria, May 31 - June 2, 2010. Proceedings*, volume 6109 of *Lecture Notes in Computer Science*, pages 106–117. Springer.

Sadiq, S. W., Governatori, G., and Namiri, K. (2007). Modeling control objectives for business process compliance. In Alonso, G., Dadam, P., and Rosemann, M., editors, *Business Process Management, 5th International Conference, BPM 2007, Brisbane, Australia, September 24-28, 2007, Proceedings*, volume 4714 of *Lecture Notes in Computer Science*, pages 149–164. Springer.

Schäfer, T., Fettke, P., and Loos, P. (2011). Towards an integration of GRC and BPM - requirements changes for compliance management caused by externally induced complexity drivers. In Daniel, F., Barkaoui, K., and Dustdar, S., editors, *Business Process Management Workshops - BPM 2011 International Workshops, Clermont-Ferrand, France, August 29, 2011, Revised Selected Papers, Part II*, volume 100 of *Lecture Notes in Business Information Processing*, pages 344–355. Springer.

Sinur, J. (2009). The art and science of rules vs. process flows (Gartner Research Report G00166408).

Sunkle, S., Kholkar, D., Rathod, H., and Kulkarni, V. (2014). Incorporating directives into enterprise TO-BE architecture. In Grossmann, G., Hallé, S., Karastoyanova, D., Reichert, M., and Rinderle-Ma, S., editors, *18th IEEE International Enterprise Distributed Object Computing Conference Workshops and Demonstrations, EDOC Workshops 2014, Ulm, Germany, September 1-2, 2014*, pages 57–66. IEEE.

Sunkle, S., Roychoudhury, S., and Kulkarni, V. (2013). Using Intentional and System Dynamics Modeling to Address WHYs in Enterprise Architecture. In Cordeiro, J., Marca, D. A., and van Sinderen, M., editors, *ICSOFT*, pages 24–31. SciTePress.

Switzer, C. S., Suri, A., Kapoor, G., and Nazemoff, V. (2013). Governance, risk management, and compliance: Creating the right grc strategy for your company Books24x7.

Vicente, P. and da Silva, M. M. (2011). A conceptual model for integrated governance, risk and compliance. In Mouratidis, H. and Rolland, C., editors, *Advanced Information Systems Engineering - 23rd International Conference, CAiSE 2011, London, UK, June 20-24, 2011. Proceedings*, volume 6741 of *Lecture Notes in Computer Science*, pages 199–213. Springer.