Regulatory Compliance in Information Systems Research – Literature Analysis and Research Agenda

Anne Cleven and Robert Winter

Institute of Information Management, University of St. Gallen
Mueller-Friedberg-Strasse 8, 9000 St. Gallen, Switzerland
{anne.cleven, robert.winter}@unisg.ch

Abstract. After a period of little regulation, many companies are now facing a growing number and an increasing complexity of new laws, regulations, and standards. This has a huge impact on how organizations conduct their daily business and involves various changes in organizational and governance structures, software systems and data flows as well as corporate culture, organizational power and communication. We argue that the implementation of a holistic compliance cannot be divided into isolated projects, but instead requires a thorough analysis of relevant components as well as an integrated design of the very same. This paper examines the state-of-the-art of compliance research in the field of information systems (IS) by means of a comprehensive literature analysis. For the systemization of our results we apply a holistic framework for enterprise analysis and design. The framework allows us to both point out "focus areas" as well as "less travelled roads" and derive a future research agenda for compliance research.

Keywords: compliance, regulations, information systems research, literature analysis.

1 Introduction

As of shortly, information systems (IS) and the IS discipline were rather marginally affected by compliance concerns. One of the reasons for the comparatively inferior meaning of compliance can be seen in the various deregulation endeavors that have characterized past years. Another reason lies in the fact that – with regard to companies – compliance has long been seen as an unswayable factor that only limits the flexibility of organizational design, but not as an element of design itself like, for example, in the context of electronic government.

In the more recent past, however, – not least because of the current financial crisis – growing legal and regulatory burdens demand for the development of new strategies, processes, and systems that adequately support organizations in a compliant conduct of business. Some approaches like the Control Objectives for Information and Related Technology (COBIT) framework, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) model, or the information security

T. Halpin et al. (Eds.): BPMDS 2009 and EMMSAD 2009, LNBIP 29, pp. 174–186, 2009.

principles of the Code of Practice for Information Security Management ISO/EIC 17799, developed by different non-profit organizations, already provide valuable guidelines.

Nonetheless, organizations are still struggling with a holistic implementation of regulatory and legal requirements. This fact holds true for several reasons which include a lacking sense of urgency [19], indistinct responsibilities [14], and missing insights into the interplay of design elements that are relevant for an integrated compliance management [28]. However, "holistic compliance is an enterprise-wide and long-term approach" [33] that "stands in contrast to simply complying with the rules" [33] and, thus, imperatively requires an integrated design of both relevant elements and the relationships amongst these.

This paper intends to provide an overview of the existing body of knowledge on compliance in the IS discipline. The focus of our literature analysis lies on legal and regulatory compliance and respective contributions from an information systems research (ISR) perspective. Our aim is to identify both areas that have already gained some attention in the discipline and those that have so far rather been neglected. We systematize the results of our search based on a framework for enterprise analysis and design. On this basis, we point out demand for further research.

The remainder of this paper proceeds as follows. In section 2, we introduce a framework as a basis to analyze and systemize our findings. Our literature search strategy as well as the junction of the results is presented in section 3. In section 4, we recapitulate the current state of research on legal and regulatory compliance in the IS discipline, point out those areas that require for the development of further solutions, and present a potential future research agenda.

2 Business Engineering

The enterprise-wide character of regulatory compliance usually influences many, if not all business areas. In every affected business area, it impacts all layers of analysis/design from purely business related aspects (strategy, organization) to purely IT related aspects (software, data, IT infrastructure). Since enterprise architecture (EA) intends to cover all business areas over the entire "business-to-IT" range, suitable frameworks for the analysis and design of regulatory compliance might be identified in the EA field.

According to ANSI/IEEE Standard 1471-2000, architecture is defined as the "fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution" [15]. On this basis, EA is understood as the fundamental organization of a government agency or a corporation, either as a whole, or together with partners, suppliers and/or customers ("extended enterprise"), or in part (e.g. a division, a department), as well as the principles governing its design and evolution [21]. According to its primary purpose to support "coherency management", EA covers all relevant artifacts and structures in the "business-to-IT" range in a "wide and flat" manner, i.e. EA focuses on aggregate models and dependencies [1].

The above definition of architecture restricts comprised components to be "fundamental". Due to the broad range of relevant component types, EA may nevertheless

comprise a huge number of such artifacts. As a consequence, most EA frameworks distinguish several architecture layers and architecture views in order to reduce the number of artifacts per model type and per model [25]. When several architecture layers and architecture views are differentiated, design and evolution principles have to address consistency and integration issues.

As a basis for consolidating artifact types that are considered as being important for EA, widely used EA frameworks such as The Open Group Architecture Framework (TOGAF), the Federal Enterprise Architecture Framework (FEAF) and the ARIS Framework have been analyzed in [37]. The following set of core EA artifact types has been identified:

- *Business strategy layer:* organizational goals and success factors, products/services, targeted market segments, core competencies and strategic projects
- *Organization/business process layer:* organizational units, business locations, business roles, business functions, business processes including inputs/outputs (internal and external business services including service levels), metrics (performance indicators) and service flows, business information objects and aggregate information flows
- *IT/business alignment layer:* enterprise services, applications and domains
- *IT implementation layer:* software components and data resources, hardware and network architecture

While an EA framework constitutes a suitable foundation to represent EA models and their (static) dependencies, dynamic aspects as well as "soft" factors are not sufficiently covered. "Soft" factors like company culture, leadership style, behavior patterns, incentive/sanctioning systems and communication practices are considered to have a pivotal role for business analysis and successful business engineering [22]. Although such factors are much harder than "hard" artifacts to analyze, represent and include in solution design, there is ongoing research in integrated analysis/design approaches. Regarding the framework, the traditional "hard" EA layers are therefore often complemented by a "soft" layer which, due to the fact that cultural issues, leadership issues and behavioral issues are relevant over the entire "business-to-IT" range, is modeled along all "hard" layers [22].

The system of four "hard" layers and one complementary "soft" layer is limited to static as-is or to-be modeling. In order to capture the dynamics of business innovation, a transformation process view has to be added. Regarding regulatory compliance, (1) an analysis and evaluation process and (2) a transformation process should be differentiated [22]. While the "innovation management style" analysis and evaluation process continuously tracks legislation and current industry developments in order to identify transformation triggers, the transformation process defines and implements discrete transformation projects which apply regulatory measures consistently throughout the organization.

It is important to mention that the holistic, enterprise wide character of regulatory compliance demands an integrated, consistent methodological analysis/design approach. By means of such an approach, the compliance-related knowledge base (terminologies, theories, generic methods and reference models, exemplary successful practices, etc. [36]) is translated into consistent, effective compliance solutions.

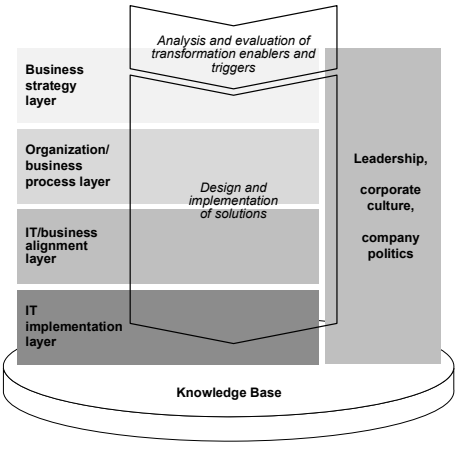

Fig. 1. Business Engineering Framework

Figure 1 illustrates the described architectural framework that includes not only "business-to-IT" as well as "soft" representation layers ("models"), but also the innovation and transformation process view ("methods").

3 Literature Analysis

3.1 Source Selection

Compliance is not a new concept. However, not least due to the current financial crisis it just now experiences an enormous hype in both practice and academia. New laws and regulations are changing IT work, structure, and governance and confront IT managers with a myriad of novel challenges [30]. In order to grasp the meaning of compliance in the context of ISR, "bring coherence and perspective" [9] to this field of research, and identify areas that demand for further solutions from the IS discipline, we conduct a systematic review of existing literature. We base the selection of sources to be included in the review on a capacious catalog of IS outlets provided by the London School of Economics (LSE) [35]. We consider this catalog to be particularly appropriate for our purposes, since it incorporates not only the mainstream IS journals, but covers also those focusing on the social study of IS as well as practitioner journals and the most significant IS conferences [35].

Subsequently, we work out an understanding of compliance that allows us to delineate the body of papers to become part of our analysis. The term compliance is often sloppily used as an umbrella term for the adherence to any piece of rule or directive. Due to the ongoing evolution of the topic, however, it is indeed challenging, if at all feasible to provide a universal definition [31]. Consequently, we decide to limit the scope of our literature analysis to take into consideration only those papers that directly address issues of regulatory and/or legal compliance.

As our aim is to provide a broad overview of recent research on compliance within the IS discipline the time span we cover with our analysis ranges from 2002 – the year the most popular and most cited regulation, the Sarbanes-Oxley Act , was enacted – until present. We identify relevant papers by first conducting a keyword search using the search term 'compliance' and then limiting the results by means of an abstract evaluation. Following this search strategy, 26 IS articles on legal and regulatory compliance are analyzed and systemized in the subsequent section.

No.	Title	Source
1	Regulation as a Barrier to Electronic Commerce in Europe: The Case of the European Fund Management Industry *(Fisher, J.; Harindranath, G.)*	European Journal of Information Systems
2	How to Build Enterprise Data Models to Achieve Compliance to Standards or Regulatory Requirements (and share data) *(Schekkerman, J.)*	Journal of the AIS
3	Diffusing Management information for Legal Compliance: The Role of the Is Organization Within the Sarbanes-Oxley Act *(Braganza, A.; Hackney, R.)*	Journal of Organizational and End User Computing
4	The Role of External and Internal Influences on Information Systems Security – A Neo-Institutional Perspective *(Hu, Q.; Hart, P.; Cooke, D.)*	Journal of Strategic Information Systems
5	Information Technology and Regulatory Policy: New Directions for Digital Government Research *(Coglianese, C.)*	Social Science Computer Review
6	Compliance to the Fair Information Practices: How Are the Fortune 500 Handling Online Privacy Disclosures? *(Schwaig, K. S.; Kane, G. C.; Storey, V. C.)*	Information & Management
7	An Overview of Leading Current Legal Issues Affecting Information Technology Professionals *(Matsuura, J. H.)*	Information Systems Frontiers
8	Cybercrime: Legal Standards Governing the Collection of Digital Evidence *(Schwerha IV, J. J.)*	
9	Managing the False Alarms: A Framework for Assurance and Verification of Surveillance Monitoring *(Goldschmidt, P.)*	
10	Analyzing Regulatory Rules for Privacy and Security Requirements *(Breaux, T. D.; Antón, A. I.)*	IEEE Transactions on Software Engineering
11	Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit *(Merhout, J. W.; Havelka, D.)*	Communications of the AIS
12	A Framework for Integrating Sarbanes-Oxley Compliance into the Systems Development Process *(Mishra, S.; Weistroffer, H. R.)*	
13	Implementing Section 404 of the Sarbanes Oxley Act: Recommendations for Information Systems Organizations *(Braganza, A.; Desouza, K. C.)*	
14	Developments In Practice XXI: IT in the New World of Corporate Governance Reforms *(Smith, H. A.; McKeen, J. D.)*	
15	Spreadsheets and Sarbanes-Oxley: Regulations, Risks, and Control Frameworks *(Panko, R. R.)*	
16	Framing the Frameworks: A Review of IT Governance Research *(Brown, A. E.; Grant, G. G.)*	
17	ISO 17799: "Best Practices" in Information Security Management? *(Ma, Q.; Pearson, J. M.)*	
18	Holistic Compliance with Sarbanes-Oxley *(Volonino, L.; Gessner, G. H.; Kermis, G. F.)*	
19	The Ethical Commitment to Compliance: Building Value-based Cultures (Tyler, T.; Dienhart, J.; Thomas, T.)	California Management Review
20	SOX, Compliance, and Power Relationships *(Braganza, A.; Franken, A.)*	Communications of the ACM
21	The Sarbanes-Oxley Act: Implications for Large-Scale IT-Outsourcing *(Hall, J. A.; Liedtka, S. L.; Gupta, P.; Liedtka, J.; Tompkins, S.)*	
22	Corporate Governance of IT: A Framework for Development *(Raghupathi, W. "Rp")*	
23	The Unexpected Benefits of Sarbanes-Oxley (Wagner, S.; Dittmar, L.)	Harvard Business Review

Fig. 2. Literature Search Results (part 1)

No.	Title	Source
24	Adopting IT to Manage Compliance and Risks: An Institutional Perspective *(Butler, T.; McGovern, D.)*	European Conference on Information Systems
25	Risk Management and Regulatory Compliance: A Data Mining Framework Based on Neural Network Rule Extraction *(Setiono, R.; Mues, C.; Baesens, B.)*	International Conference on Information Systems
26	Institutionalization of IT Compliance: A Longitudinal Study *(Currie, W.)*	

Fig. 3. Literature Search Results (part 2)

Figure 2 and 3 list the contributions on regulatory compliance that we identified in our literature search.

3.2 Literature Systemization

Systemizing the literature according to the different layers of the proposed BE framework reveals that some research areas have gained a lot of attention whereas others show only a small number of solutions. In the following, we briefly outline which contribution addresses which layers and/or relations of the framework.

Transformation enablers and triggers: Due to the multitude of laws and regulations that has come up for different industry sectors, countries, and application areas it is complicated for organizations to firstly identify relevant regulations and secondly derive adequate measures to actually achieve compliance. With his paper MATSUURA aims at providing an overview of leading current legal issues that affect IT and IT professionals [18]. Structured subject to major application areas, he briefly introduces the most important laws IT professionals are likely to encounter in the course of their daily business. Exemplary fields include information privacy and computer security, trade secrets and proprietary information, intellectual property, and antitrust, competition, and commercial law.

SCHWERHA concentrates on legal standards regulating the collection of digital evidence in the case of cybercrime [27]. Starting from the Fourth Amendment that preserves citizens from unreasonable search and seizure he introduces a variety of statutory provisions that have been issued to supplement the initial law. The author points out that the rapid evolution of new technologies requires a continuous adjustment of the respective laws. He emphasizes that not only officers but also civil litigants have to be familiar with the Fourth Amendment and its complementing laws as they are held to these standards when acquiring digital evidence.

VOLONINO et al. focus on the Sarbanes-Oxley Act and its impact on IT [33]. They discuss the act's mandates as well as the purpose of regulatory agencies and point out the line of accountability from the Security and Exchange Commission via executives through to the IS departments and IS auditors that are ultimately expected to implement compliance requirements. The authors point out why and how a variety of research areas, e.g. information quality assurance, business intelligence, transaction control and integration are affected by Sarbanes-Oxley compliance requirements.

Knowledge Base: Three of the above itemized papers are considered to primarily contribute to the compliance-related knowledge base. FISHER and HARINDRANATH investigate the effect of financial services regulation on electronic commerce in the European Union (EU) [11]. On the basis of an exploratory study the authors reveal that current regulations – tough established to support the electronic distributions of

funds – in fact rather act as a barrier and inhibitor. They conclude that due to a missing consistency of present regulations with their theoretical underpinnings the EU is far from realizing a single market in the financial services.

Fair information practices (FIP) represent another example of regulations that especially organizations dealing with the acquisition and use of personal consumer information must adhere to. SCHWAIG et al. investigate the privacy policies of the Fortune 500 in order to assess the degree to which these companies comply with the FIP [26]. Based on their examinations the authors develop a reference-matrix that allows for the evaluation of a company's maturity stage with regard to its privacy policy implementation. Four stages are identified that range from mature privacy policies to policies that merely serve a public relations tool.

Business strategy layer: The intention to implement and establish a holistic compliance management represents a strategic project. Such projects require a sound cost-benefit analysis, a mandate at the top management level, and a thorough project plan. MERHOUT and HAVELKA pick up on the fact that IT auditing is often seen as a "necessary evil" by IT management rather than as a means that may generate value [19]. The authors elaborate an extensive list of explicit benefits of an internal IT function and propose a capacious framework comprising 8 fundamental success factors for quality IT auditing. It is argued that adhering to rules and regulations should be regarded as an opportunity to constitute governance frameworks and establish partnerships between IT management and auditors. This in turn enhances top management's appreciation of the role of IT, leads to better decision making, and frees up resources for other value-added projects.

In their article HALL and LIEDTKA explore how the Sarbanes-Oxley Act affects large-scale IT outsourcing [13]. The authors identify key clauses of the act and derive a capacious list of risks and negative implications for outsourcing thereof. They defer to the need of a tight relation of corporate and IT strategy and appeal to view the act as an opportunity to (re-)integrate IT departments and invest in strategic IT assets.

Four years after the Sarbanes-Oxley Act went into effect, WAGNER and DITTMAR analyze the different ways organizations deal with the new law and discover that only a minor group was able to gain benefits from its implementation [34]. While the majority of companies complained about having to comply with the act, a few used the law as an opportunity to strategically and rigorously redesign their business. The authors portray how benefits like e.g. process standardization and consolidation, were achieved by those companies that successfully implemented the Sarbanes-Oxley Act.

Organization/business process layer: New laws and regulations not only require organizations to provide a more detailed disclosure of their operating results but also imply the need for change in organizational structures and processes. In their contribution 'IT in the New World of Corporate Governance Reforms' of the series 'Development in Practice' SMITH and MCKEEN survey how compliance frameworks and governance reforms affect and change IT work [30]. In collaboration with a focus group of senior IT managers the authors investigate the following five areas: general implications of regulatory acts for IT, the short-term impact, impacts on IT processes as well as impacts on IT structure and governance, and finally the anticipated long-term impacts. The survey reveals that IT managers expect a much more professional, controlled, and bureaucratized IT.

Leadership, corporate culture, and company politics: The successful implementation of a holistic compliance approach not only requires adequate organizational structures and IT. It furthermore necessitates the commitment of a company's workforce and the willingness of every employee to support the whole project. An article written by TYLER ET AL. explores the effect of the 1991 Federal Sentencing Guidelines for Organizations on the way organizations set up culture and policies to assert a compliant behavior of their employees throughout the whole organization. The authors find out that a common behavior of ethics and compliance officers is to promote a "values-and-integrity approach" to the outside but live a "command-and-control approach" at work [32]. The latter approach, however, proves to be the more effective in assuring a compliant behavior. The authors provide a number of cross-organizational benchmarks regarding relevant compliance procedures.

Organization/business process layer & Leadership, corporate culture, and company politics: There are several contributions that examine the combined impact of regulatory and legal compliance on 'hard' organizational and 'soft' cultural aspects and provide solutions for their design. BRAGANZA and HACKNEY, for example, use institutional theory as a lens through which they investigate experiences made by three global organizations with the implementation of Section 404 of the Sarbanes-Oxley Act [4]. Following institutional theory, the authors take a distinct set of implementation tactics as a basis and survey how these are applied to change controls, processes, and behavior. Based on the insights won in their exploratory study they suggest a number of intervention drivers that are considered most appropriate for reducing the potential for financial deficiencies. Another paper by BRAGANZA and DESOUZA addresses the same topic, but directly focuses on providing and discussing six action guidelines for the implementation of Section 404 of the Sarbanes-Oxley Act [2]. BRAGANZA and FRANKEN investigate the relationships between different stakeholders of Sarbanes-Oxley compliance, namely: the chief executive officer (CEO), the chief financial officer (CFO), the chief information officer (CIO), and the auditors [3]. Again, institutional theory and the concept of power relationships are used as the theoretical basis. The authors conclude with a set of compliance implementation tactics that fit best for four given types of power relationships.

In her contribution CURRIE goes into the matter of how societal, organizational and individual pressures change institutionalized processes over time [10]. The author focuses on how the introduction of an investment management system influences the compliance function and its respective processes. For the analysis of data won in a longitudinal study she develops a conceptual framework that borrows from the concepts of institutional theory. With her findings she contributes to the knowledge on implications of technology change.

BUTLER and MCGOVERN likewise apply institutional theory to scrutinize the exogenous factors influencing IT adoption decisions on compliance solutions[7]. The authors complement their findings by additionally using organizational theory to describe endogenous institutional arrangements. On the basis of a case study the authors derive general rules for the adoption of compliance software.

A contribution by HU et al. aims at providing a better understanding of external and internal influences on the success of intentions to establish a corporate IS security [14]. Neo-institutional theory is applied as a framework for analyzing the data

gathered in a case study. The authors observe coercive, normative, and mimetic forces that affect an organization's success with the implementation of IS security practices and controls. The investigation shows that regulatory forces, such as the Sarbanes-Oxley Act, are potent drivers for motivating top managers to set off and execute company-wide security initiatives. The contribution points out how regulatory and legal requirements influence an organization's IS security and presents valuable guiding principles for enterprises developing an IS security.

Organizational/business process layer & IT/business alignment layer: Based on the concluding thoughts from two workshops held by Harvard University's Regulatory Policy Program, COGLIANESE discusses how IT affects government in making regulatory decisions [8]. The author points out the necessity of an integrated consideration of both the opportunities associated with new information technologies and the organizational design of regulatory policy making. He provides advice on how to enhance the receptiveness, efficiency, and manageability of decision making in regulatory concerns and outlines objectives for future research on digital government.

Organization/business process layer, IT/business alignment layer, IT implementation layer & Leadership, corporate culture, and company politics: The assurance of an integrated and holistic compliance management calls for approaches that involve all of the layers outlined in the BE framework. However, existing practitioner frameworks often only address specific aspects and neglect the required holism. In his contribution PANKO picks up on the compliance risks that are induced by the widespread use of spreadsheets in financial reporting [23]. Based on the alarming fact that on average 94% of these spreadsheets are faulty the author analyses how general as well as IT-specific control frameworks can be used in order to reduce spreadsheet-related compliance risks. He comes to the conclusion that existing frameworks mainly support error-testing and that "operational procedures, auditing, documentation methods, and secure spreadsheet operations" are still in need of development.

The demand for rigorous and transparent frameworks for corporate governance was significantly increased when the Sarbanes-Oxley Act went into effect. BROWN and GRANT use this as an opportunity to conduct a comprehensive review on existing governance research and literature [6]. They identify two main research streams, one on IT governance forms and the other one on IT governance contingency analysis which conjointly led to the contemporary IT governance research. The author's analysis reveals that especially the fit between IT and organization remains to be of dominant importance and that both practitioners and academicians show a constant effort to further refine instruments and methods to govern corporate IT decisions.

MA and PEARSON conduct a survey of information security professionals in order to validate if the standard ISO 17799 actually represents a best practice approach for information security and if the framework's dimensions address the right aspects [17]. The second objective of their survey consists in the improvement of the standard by generating a parsimonious model. The author's findings indicate that ISO 17799 dimensions and items are highly valid, but should be complemented by a new dimension that additionally addresses the aspect of business partner security.

A lot of regulations and standards require a complete control of the corporate IT. RAGHUPATHI picks up on this fact and discusses how enterprise-wide IT governance

(ITG) can be established [24]. He identifies three different stages in corporate ITG. Starting from the finding that IT needs to generate a high return on investment (ROI) the author analyzes the role of the CIO and the IS organization as well as the way the IS function is regulated by the top management.

IT implementation layer: "Increasingly, regulations are requiring software engineers to specify, design, and implement systems that are accountable to and in compliance with laws and regulations" [5]. The subsequent contributions explicitly focus on technological solutions for the implementation of compliance requirements. KIM et al. propose a concept for model-based proof of compliance [16]. They postulate the use of computational ontologies for the development of enterprise data models in order to both overcome business analysis problems – in particular those related to compliance issues and improve the possibility to inter-organizationally share data models. The paper not only introduces the concept but also provides an exemplary implementation that proves the applicability of the approach.

Another characteristic subject of legal compliance is addressed by GOLDSCHMIDT, who suggests a method to support the assertion of surveillance monitoring alarms by means of the so called compliance verification knowledge management (CV-KM) [12]. Primary monitoring systems (PMS) are systems that ensure internal control and generate exceptions in case of potential anomalies and possible non-compliance events, e.g. fraud or intrusion detection. CV-KM systems represent second-tier monitoring systems that assist the user in analyzing and categorizing the exceptions reported by the PMS and in identifying evidence either verifying or refuting generated alarms. Thus, CV-KM systems act as decision support systems for analysts.

One of the major challenges of automating compliance lies in the fact that regulatory requirements are mostly specified in complex and betimes ambiguous legal language. BREAUX and ANTÓN attend to this defiance and propose a method for extracting rights and obligations from laws and other regulatory texts [5]. Therewith, the authors contribute a design artifact that supports organizations in assuring and systematically demonstrating their compliance with policies and regulations.

The Sarbanes-Oxley Act not only concerns aspects of corporate governance and financial practice but also introduces a set of requirements regulating software development processes. On the basis of the COBIT reference structure MISHRA and WEISSTROFFER develop a conceptual framework that integrates respective requirements into the workflows of software development and, thereby, facilitates the internal control over systems development activities [20].

For the simple reason that an increasing number of regulations require the disclosure of management control SETIONO ET AL. propose a new type of IS designed to support quality decision making [29]. Their novel data mining algorithm is especially designed for verification, validation, and performance monitoring in the Basel II context.

Figure 4 displays how the 26 papers considered in our literature analysis scatter on the BE framework according to the content they address. The papers can be identified based on the numbers they have been assigned in figures 2 and 3.

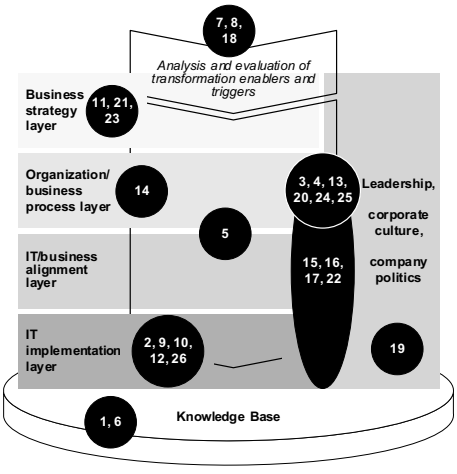

Fig. 4. Systemization of literature

4 Conclusion

The objective we pursued with this paper was to bring light into the darkness of compliance research in the IS discipline. As has been said by a variety of authors, new regulations and laws have huge impacts on how organizations conduct their daily business [30], [33], [34]. Thus, a number of publications address different aspects of implementing regulatory compliance. We conducted a literature analysis and systemized the results according to the BE framework. The systemization reveals that some layers and relations have been considered intensely while others have fairly been neglected. Especially the influences of regulations on organizational and behavioral structures of organizations have thoroughly been investigated, often applying institutional theory as a conceptual basis. Furthermore, a number of contributions propose different software or IT solutions that support the implementation of compliance. Other areas, however, remain clearly under-researched. In particular the relations between different layers have been neglected so far. We could not find any contribution that addresses the topic of how to operationalize strategic compliance objectives. Moreover, methods and approaches for the identification of those regulations that are especially relevant for an organization are missing. The knowledge base alike is still lacking in sound theories, methods and terminologies for the context of regulatory compliance. Moreover, an approach to combine existing methods and adapt these according to specific organizational contexts is not yet available. We thus conclude that – although the implications of regulatory compliance have been thoroughly investigated [20] – the IS discipline is limping behind with the development of suitable concepts and solutions. Compliance represents a challenging new research area in ISR and demands for a unified system of concepts and a pool of methods and models that can be combined for a holistic compliance implementation.

References

1. Aier, S., Kurpjuweit, S., Saat, J., Winter, R.: Business Engineering Navigator – A Business to IT Approach to Enterprise Architecture Management. In: Bernard, S., Doucet, G., Gøtze, J., Saha, P. (eds.) Coherency Management – Architecting the Enterprise for Alignment, Agility, and Assurance Ed. (2009)
2. Braganza, A., Desouza, K.C.: Implementing Section 404 of the Sarbanes Oxley Act: Recommendations for Information Systems Organizations. Communications of the Association for Information Systems 18, 464–487 (2006)
3. Braganza, A., Franken, A.: SOX, Compliance, and Power Relationships. Communications of the ACM 50(9), 97–102 (2007)
4. Braganza, A., Hackney, R.: Diffusing Management Information for Legal Compliance: the Role of the IS Organization within the Sarbanes-Oxley Act. Journal of Organizational and End User Computing 20, 1–24 (2008)
5. Breaux, T.D., Antón, A.I.: Analyzing Regulatory Rules for Privacy and Security Requirements. IEEE Transactions on Software Engineering 34(1), 5–20 (2008)
6. Brown, A.E., Grant, G.G.: Framing the Frameworks: A Review of IT Governance Research. Communications of the Association for Information Systems 15, 696–712 (2005)
7. Butler, T., McGovern, D.: Adoption IT to Manage Compliance and Risks: An Institutional Perspective. In: Proceedings of the 16th European Conference on Information Systems (ECIS), Galway, Ireland, pp. 1034–1045 (2008)
8. Coglianese, C.: Information Technology and Regulatory Policy: New Directions for Digital Government Research. Social Science Computer Review 22(1), 85–91 (2004)
9. Cooper, H.M.: Organizing knowledge syntheses: A taxonomy of literature reviews. Knowledge in Society 1, 104–126 (1988)
10. Currie, W.: Institutionalization of IT Compliance: A Longitudinal Study. In: Proceedings of the 29th International Conference on Information Systems (ICIS), Paris, France (2008)
11. Fisher, J., Harindranath, G.: Regulation as a barrier to electronic commerce in Europe: the case of the European fund management industry. European Journal of Information Systems 13, 260–272 (2004)
12. Goldschmidt, P.: Managing the false alarms: A framework for assurance and verification of surveillance monitoring. Information Systems Frontiers 9(5), 541–556 (2007)
13. Hall, J.A., Liedtka, S.L., Gupta, P., Liedtka, J., Tompkins, S.: The Sarbanes-Oxley Act: Implications for Large-Scale IT-Outsourcing. Communications of the ACM 50(3), 95–100 (2007)
14. Hu, Q., Hart, P., Cooke, D.: The Role of External and Internal Influences on Information Systems Security – A Neo-Institutional Perspective. Journal of Strategic Information Systems 16, 153–172 (2007)
15. IEEE: IEEE Recommended Practice for Architectural Description of Software Intensive Systems (IEEE Std 1471-2000). IEEE Computer Society, New York (2000)
16. Kim, H.M., Fox, M.S., Sengupta, A.: How To Build Enterprise Data Models To Achieve Compliance To Standards Or Regulatory Requirements (and share data). Journal of the Association of Information Systems 8(2), 105–128 (2007)
17. Ma, Q., Pearson, J.M.: ISO 17799: Best Practices in Information Security Management? Communications of the Association for Information Systems 15, 577–591 (2005)
18. Matsuura, J.H.: An Overview of Leading Current Legal Issues Affecting Information Technology Professionals. Information Systems Frontiers 6(2), 153–160 (2004)

19. Merhout, J.W., Havelka, D.: Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit. Communications of the Association for Information Systems 23, 463–482 (2008)
20. Mishra, S., Weistroffer, H.R.: A Framework for Integrating Sarbanes-Oxley Compliance into the Systems Development Process. Communications of the Association for Information Systems 20, 712–727 (2007)
21. Opengroup: TOGAF Enterprise Edition Version 8.1. The Open Group (2003)
22. Österle, H., Winter, R.: Business Engineering - Auf dem Weg zum Unternehmen des Informationszeitalters. In: Österle, H., Winter, R. (eds.) Business Engineering, 2nd edn., pp. 3–19. Springer, Berlin (2003)
23. Panko, R.R.: Spreadsheets and Sarbanes-Oxley: Regulations, Risks, and Control Frameworks. Communications of the Association for Information Systems 17, 647–676 (2006)
24. Raghupathi, W.R.: Corporate Governance of IT: A Framework for Development. Communications of the ACM 50(8), 94–99 (2007)
25. Schekkerman, J.: How to Survive in the Jungle of Enterprise Architecture Frameworks: Creating or Choosing an Enterprise Architecture Framework. Trafford Publishing, Victoria (2004)
26. Schwaig, K.S., Kane, G.C., Storey, V.C.: Compliance to the Fair Information Practices: How are the Fortune 500 handling Online Privacy Disclosures? Information & Management 43(7), 805–820 (2006)
27. Schwerha IV, J.J.: Cybercrime: Legal Standards Governing the Collection of Digital Evidence. Information Systems Frontiers 6(2), 133–151 (2004)
28. Securities Industry Association, C., Legal, D.: The Role of Compliance. Journal of Investment Compliance 6(3), 4–22 (2005)
29. Setiono, R., Mues, C., Baesens, B.: Risk Management and Regulatory Compliance: A Data Mining Framework Based on Neural Network Rule Extraction. In: Proceedings of the 27th International Conference on Information Systems (ICIS), Paris, France (2006)
30. Smith, H.A., McKeen, J.D.: Developments In Practice XXI: IT in the New World of Corporate Governance Reforms. Communications of the Association for Information Systems 17, 714–727 (2006)
31. Taylor, C.: The Evolution of Compliance. Journal of Investment Compliance 6(4), 54–58 (2005)
32. Tyler, T., Dienhart, J., Thomas, T.: The Ethical Commitment to Compliance: Buildung Value-Based Cultures. California Management Review 50(2), 31–51 (2008)
33. Volonino, L., Gessner, G.H., Kermis, G.F.: Holistic Compliance with Sarbanes-Oxley. Communications of the Association for Information Systems 14, 219–233 (2004)
34. Wagner, S., Dittmar, L.: The Unexpected Benefits of Sarbanes-Oxley. Harvard Business Review 84(4), 133–140 (2006)
35. Willcocks, L., Whitley, E.A., Avgerou, C.: The ranking of top IS journals: a perspective from the London School of Economics. European Journal of Information Systems 17, 163–168 (2008)
36. Winter, R.: Design Science Research in Europe. European Journal of Information Systems 17, 470–475 (2008)
37. Winter, R., Fischer, R.: Essential Layers, Artifacts, and Dependencies of Enterprise Architecture. In: Society, I.C. (ed.) Proceedings of the EDOC Workshop on Trends in Enterprise Architecture Research (TEAR 2006). IEEE Computer Society, Los Alamitos (2006)