Patterns for Understanding Control Requirements for Information Systems for Governance, Risk Management, and Compliance (GRC IS)

Manuel Wiesche[1], Carolin Berwing[2], Michael Schermann[1], and Helmut Krcmar[1]

[1] Chair for Information Systems, Technische Universität München
Boltzmannstraße 3, 85748 Garching, Germany
{wiesche,michael.schermann,krcmar}@in.tum.de
[2] Daiichi Sankyo Europe GmbH
Zielstattstr. 48, 81379 München, Germany
caro_berwing@yahoo.de

Abstract. Companies face a plethora of regulations, standards, and best practice frameworks for governance, risk management and compliance. Information systems (IS) for planning, controlling, and reporting on the compliance with these requirements are known as governance, risk management, and compliance (GRC) IS. However, the challenge lies in mapping control requirements with functionality of GRC IS. In this paper, we review existing regulations and derive a framework for key control requirements. We develop a pattern-based approach that allows to systematically evaluate GRC IS based on the current regulatory situation. We evaluate the pattern catalogue by classifying an existing GRC portfolio. As implications for research, we associate existing control requirements and GRC information systems. As implications for practice, we provide decision support for the selection of GRC IS, depending on situational factors and the expected value proposition. In sum, our framework adds to the understanding of the effects of GRC IS.

Keywords: Governance, Risk Management, Compliance, GRC, patterns, software evaluation.

1 Introduction

Internationally acting companies face the challenge of meeting an overabundance of governance regulations and reporting on the compliance with these regulations [1-3]. Even nationwide, legislators require companies to account for compliance with multiple regulations. Assuring compliance has turned into one of the key objectives of any chief financial officer (CFO).

Information systems dedicated to plan, control, and report on the compliance with regulations create significant potentials for coping with regulations more effectively [3, 4]. Commonly, features of such information systems are discussed under the label of GRC (governance, risk management, and compliance). Driven by regulatory compliance, companies established such GRC IS to prevent fines and penalties imposed by regulatory agencies [1]. Today, companies focus on integrated solutions of GRC

C. Salinesi and O. Pastor (Eds.): CAiSE 2011 Workshops, LNBIP 83, pp. 208–217, 2011.

without a clear value proposition for their individual situation [5]. Still, market research predicts that US-based companies spend almost $30B on GRC related technology and solutions [6] and its importance continues to grow [7].

Organizations face both, a variety of requirements [3, 8] and a broad portfolio of GRC IS with different emphasis [5, 9, 10]. Executives have to rely on product presentations, progress reports from other users, and consulting services to determine an application's potential to meet control requirements. However, they often lack understanding of which application can fulfill a certain control regulation [5, 8, 9]. Hence, there are no methods, guidelines, or procedures for executives to evaluate the potential of compliance assurance through existing GRC IS. This article aims at answering the following research question: *How can control requirements be classified to evaluate existing information systems in the field of GRC?* Our research provides a pattern catalogue, which summarizes central aspects of control requirements. It serves for evaluating potentials and shortcomings of GRC IS with the help of the predefined patterns.

The remainder of this paper is structured as follows: in the first section we develop a conceptual framework of pertinent control requirements for GRC IS. Then we discuss a pattern catalogue for compliance assurance and present two control pattern candidates. We explore SAP GRC 10.0, a prominent GRC IS, using the patterns. We discuss the results and provide implications for practice and research. The paper finishes with a conclusion and an outlook on future research activities.

2 A Framework of Control Requirements for GRC IS

In this section, we introduce the terms governance and compliance. We develop a conceptualization of control requirements through constructing a control requirements framework. We review existing control regulations and classify them according to the proposed framework.

All efforts management takes in seeking to assure stakeholders that they get a return on their investments can be defined as corporate governance (CG) [11]. Due to regional and industry specific conditions, CG cannot be implemented based on an internationally and intersectorally valid system. It is rather a system of internationally recognized regulations and national requirements, which need to be integrated into an organizational framework. Implementing CG within an organization depends on various factors, which we suggest to structure in three dimensions: (1) the inner circumstances of a company, (2) the national environment including its habits, and (3) regulatory obligations, laws, and standards.

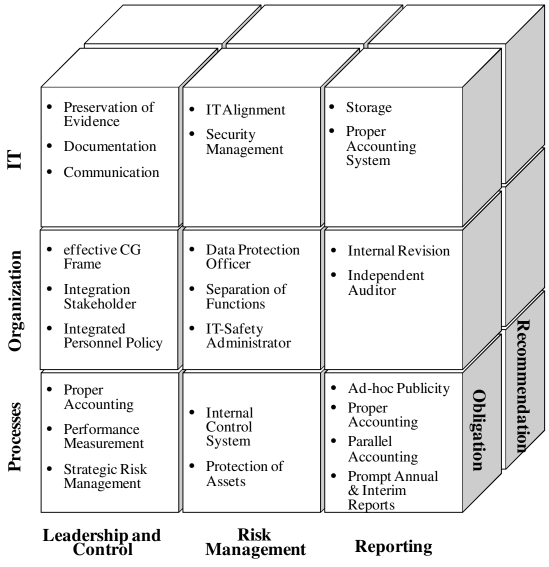
Although there is no formal or generally accepted definition, the understanding of compliance as duty of the board to ensure abidance of legal requirements and internal guidelines and assure appropriate behavior through the employees is out of question. Starting with financial constraints in the 1980s, today various GRC regulations, guidelines, standards, and frameworks have been developed, which organizations have to comply to.

These control requirements can be structured by the dimensions liability, area of responsibility and addressee. Regarding the dimension *liability*, requirements can be differentiated in either obligatory or recommended. *Area of responsibility* encompasses organizational setting, business processes and IT. Regarding *addressee*, GRC regulations can address internal and external dimensions.

The following examples shall demonstrate the broad scope and variety of GRC requirements: To be in compliance with e.g. the Sarbanes-Oxley Act (SOX), chief executives have to verify the accuracy and timely reporting of their financial results and establish procedures and controls which ensure the quality and integrity of their financial data [3]. On the other hand, privacy regulations require adequate data storage ensuring integrity and confidentiality. Furthermore, governance guidelines provide best practices for IS management and demand sound risk management.

We reviewed existing legal constraints, CG standards, corporate governance frameworks, IT-security and accounting standards, and selected pertinent industry-specific regulations from banking, insurance, medical, and chemical industry to provide an overview of this plethora of the diverse existing control requirements.[1] We classified them according to the dimensions introduced above.

In order to successfully comply with these regulations, various controls exist which cover the three management functions governance, risk management and reporting (Fig. 1). Governance controls include performance measurement, stakeholder integration, and audit. Risk management controls vary from implementing internal control systems, segregation of duties, and IT alignment. Reporting controls include proper book-keeping, internal audit, and archiving.



	Leadership and Control	Risk Management	Reporting
IT	• Preservation of Evidence • Documentation • Communication	• IT Alignment • Security Management	• Storage • Proper Accounting System
Organization	• effective CG Frame • Integration Stakeholder • Integrated Personnel Policy	• Data Protection Officer • Separation of Functions • IT-Safety Administrator	• Internal Revision • Independent Auditor
Processes	• Proper Accounting • Performance Measurement • Strategic Risk Management	• Internal Control System • Protection of Assets	• Ad-hoc Publicity • Proper Accounting • Parallel Accounting • Prompt Annual & Interim Reports

Fig. 1. Overview of categorized control activities

[1] In the field of laws, regulations, and standards for external addressees, we reviewed CobiT, COSO II, CGK, GxP, ISO 27000, IT-GSHB, ITIL, OECD principles, OCEG Redbook, EU guidelines 4,7 & 8, IFRS / IAS and US GAAP. Regarding internal addresses, we reviewed Basel III, DCGK, the German privacy regulations, KonTraG, MaRisk, BilReG, Solvency II, SOX, Liabilty, Market constraints, EU guidelines 4,7 & 8, FDA 21 CFR Teil 11, GDPdU, GoBS, and UMAG.

3 Establishing a Pattern Catalogue of Control Effectiveness

Since organizations face a vast amount of guidelines to comply with, we focus on a pattern repository that might serve as the distilled integration of control requirements. The patterns which will be introduced in the following, provide concrete requirements for IS functionality.

The term pattern was originally made up by Alexander [12] in the field of architecture and was formally defined as „IF: X THEN: Z / PROBLEM: Y". A pattern can be defined as the description of a reusable solution to a problem in a way that the solution can be used in similar situations. A pattern comprises the following elements [12]: the *context* comprises causes which lead to the problem described in a pattern and the conditions under which the problem occurs. The context should support acquiring the relevance of a pattern. The *problem* is described by explaining contradictions which cause the problem. The next section of a pattern explains the proposed *solution* by dissolving the elements described before. In order to make the patterns more actionable for software evaluation, we extended these dimensions by the elements *alias*, meaning alternative description, *aim* as key goal of the pattern, *regulation* as the names of the guidelines the pattern was derived from, *consequence* as positive and negative effects, and *related patterns* to describe how this pattern relates to others.

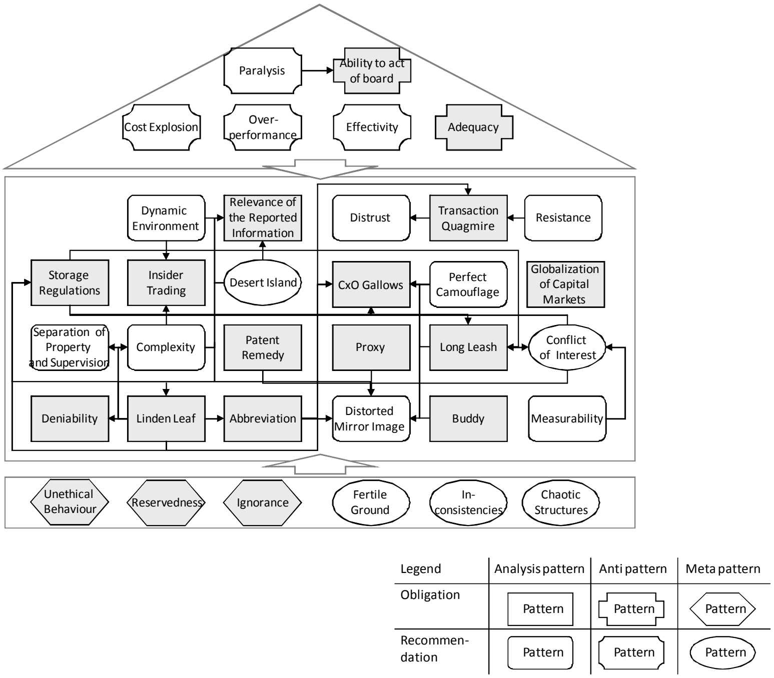


Fig. 2. A control pattern catalogue for structuring capabilities of GRC IS

To develop the patterns, we followed the suggestions of Buschmann et al. [13]: we reviewed existing guidelines, laws, best practices, and standards and classified them into the categories mentioned above. We reviewed what the guidelines, laws, best practices, and standards described as type of result and matched it to the identified control activities. We matched the requirements with the activities and used the description of the activities to define the supporting and enabling function of information systems. In general, GRC IS can provide real-time data processing, automation, and flexibility in the fields of reporting, logging, communication, simulation, central repository, role-based authorization systems, workflow, and archiving. Having the knowledge about the requirements, necessary activities and IS potentials, we developed a catalogue of 35 patterns to evaluate the potential of GRC IS (figure 2).

We identified four types of patterns as introduced in the literature: analysis patterns, anti patterns, Meta pattern, and modules. *Analysis patterns* support communicating and documenting domain knowledge. They ensure proper conceptualizing by helping understand the underlying business problem and define the requirements [14]. *Anti patterns* are negative examples of already implemented solutions, which include recommendations on how to fix it properly [15]. *Meta patterns* are general patterns which are universal and can therefore be used in various contexts [16]. *Modules* support in classifying existing patterns. Each module is a collection of single patterns, which can individually be seen as a pattern catalogue.

To evaluate existing software solutions for GRC, it is important to evaluate the overall potential from management perspective. Management must be able to understand the interplay between certain patterns to reveal the differing value propositions while evaluating GRC IS. Therefore, we propose the following eight categories to structure the control patterns: an effective corporate governance framework, preservation of evidence, segregation of duties, safety of assets, reporting, and corporate management under consideration of profitability and quality. By showing the various relationships between the different patterns the reader is offered a "navigator" for the complex area of corporate governance (figure 3).

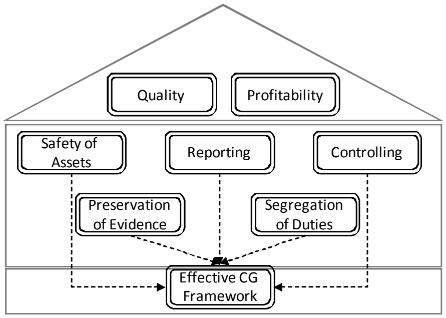
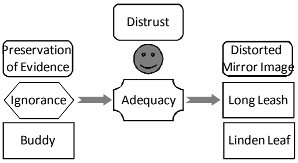
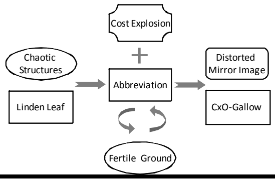


Fig. 3. Categories to structure control requirements

In the following, we will introduce two patterns to demonstrate the way the patterns are defined and structured. The patterns are structured according to the underlying modules (figure 2). The pattern *adequacy* is settled in the context of

Table 1. Patterns of Compliance Assurance

Name	**adequacy**	**shortcut**
Alias	underperformance	effectiveness
Aim	establish security	supervising employee's behavior with controls
Context	It is applied in the context of evaluating the effectiveness of the internal control systems. Since requirements are manifold and the organizational characteristics vary, annual audit also incorporates evaluating control effectiveness and adequacy of internal control system.	Employees conduct compliance work on top of their regular task, without a clear direct benefit. Caused by lack of time or disbelief, employees do not conduct compliance tasks properly or at all, which endangers successful audits.
Problem	The annual audit evaluates the existing internal control system ex-post. Found contradictions might require fundamental adoptions within CG which usually cannot be changed spontaneously and resulting in the auditors refuse the certificate. This situation of non-compliance affects stakeholder relationships and harms the external image.	In the annual financial statement a function check is conducted to reveal the effective match of control and associated risk. It refers to the fact that not only proper controls have to be proposed within the organization but also need to actually be implemented.
Solution	A solution for this issue would be continuous auditing. Internal resources including internal auditors can conduct a final rehearsal of the annual financial statement. Special focus should be laid on top management support to ensure cooperation with internal audit and communicate the importance of such topics.	The pattern provides a solution through workflow-based systems. Such systems services as reminder and provides guidance for employees to conduct compliance work properly. Such systems then document the accurate execution of the compliance task.
Consequence	+ continuous information on implementation of CG and audit acceptability - additional effort for testing and customizing	+ guarantee of the execution of compliance tasks within a reasonable period of time - requirement of initial effort for defining and implementing the system - reduced process performance
regulation	Basel III, IDW PS-330, MaRisk, SOX	MaRisk, SOX
related patterns	 Distrust Preservation of Evidence Distorted Mirror Image Ignorance Adequacy Long Leash Buddy Linden Leaf	 Cost Explosion Chaotic Structures + Distorted Mirror Image Abbreviation Linden Leaf CxO-Gallow Fertile Ground

quality-module and can also be described with the term underperformance (second column in table 2). The pattern *shortcut* can be classified in the prominent module segregation of duties with the aim of supervising employee's behavior with controls (third column in table 2).

Table 2. Evaluation of SAP GRC 10.0 with control patterns

Pattern		abbreviation	deniability	adequacy	storage obligations	buddy	CxO-gallows	relevance of the information given	Globalization of capital markets	ability to act of board	insider trading	conflict of interest	(long) leash	Linden leaf	easy solution	transaction quagmire	proxy	unethical behaviour	ignorance	reservedness	chaotic strucures	dynamic environment	effectiveness	desert island	fertile ground	inconsistencies	complexity	sky-rocketing costs	paralysis	measurability	suspicion	overperformance	perfect camouflage	separation of property and control	Distorted mirror image	resistance
Access Control	RAR			◕		◕	◑							◑		◕	◕				●	◕				◕	◕	◕		◕		◕			◔	
	ERM			◕		◕										◕	◕				◑	◕				◕	◑	◕		◕			◑		○	
	SUP	◕		◕	◕	◑							●			●	◕				◕	◕				◔	◑	◑		◕					○	
	CUP			◕		◕										◕	◕				◕	◕				◔	◑	◕		◕					○	
Process Control		●	◕	◕	○	◕	●				◑		◕	◑	◑	◕	◕		○	○	◕	◕	◑	◑		◕	●	◕		◕		◕			◑	
GTS			○	◕	◑		◔		○		◑					◔		○				◕			◕		◑	◔		◑					○	
Environmental			○	◕	◑		◔				◑							○				◕				◑	◑	◔		◑					○	
Risk Management		◑		◕			◕				◑			◔	◑			◔			◔	●	◑	◕		●	●	◑		◕	◔	●			◔	

Legend: insufficient ○ to some extent ◔ partly ◑ adequately ◕ innovative ●

4 Exploring GRC Solutions with Control Patterns

In this section, we will use the derived pattern catalogue to evaluate a popular GRC IS. Therefore, we use the recently launched SAP BusinessObjects GRC 10.0 solution portfolio. The predecessor of this portfolio has been ranked as visionary within Gartner's most recent magic quadrant [9]. After giving a short summary of the functionality of the particular modules, we will use the SAP GRC portfolio to reflect the control patterns.

As leading supplier of enterprise software, SAP integrated existing compliance applications into the GRC portfolio in 2006. The GRC portfolio consists of five functional elements (rows in table 3). Access Control allows securing segregation of duties, compliant provisioning, and consists of the functional elements Risk Analysis and Remediation (RAR) for implementing and monitoring access guidelines, Enterprise Role Management (ERM) for defining and managing organizational roles, Compliant User Provisioning (CUP) for assigning these roles to users, and Superuser Privilege Management (SUP), allowing automated and fully documented fire fighter solutions for emergency access. Process Control allows managing the internal control systems and consists of control documentation, control analysis, certificates and reporting. Global Trade Services (GTS) allows securing cross border transactions. The module Environmental ensures environmental execution and legal compliance. Finally, the aggregating Risk Management allows the strategic detection of risks and control monitoring across the organization. In addition to using the aforementioned systems as data source, it provides a global risk management process as suggested by best practice frameworks, which complies with legal requirements.

We used test installations and existing documentation to understand the functionality of each module as a basis to evaluate the developed patterns. We assessed the potential of each module for each pattern by means of the following criteria: *insufficient* when the underlying problem is not addressed at all, *to some extent* when the problem is mentioned, but not solved, *partly*, when the problem is solved at least in parts, *adequately*, when the problem is solved with the help of the system, *innovative* when an existing solution is used for a new problem-context combination. The results are displayed in table 3.

The results in table 3 reveal that the SAP GRC portfolio has strengths and weaknesses in implementing certain patterns. Especially the patterns CxO-gallows, transaction quagmire, shortcut, chaotic structures, dynamic environment, and complexity are implemented with innovative ideas and solutions, which can provide competitive advantages. Then again, the SAP portfolio reveals gaps regarding the patterns unethical behavior, ignorance, reservedness, globalization of capital markets, and distorted mirror image which are addressed, but lack proper implementation. Further analyses of these patterns reveal that the potential of IS in the context of these patterns can only be established through proper governance and organizational structure. A satisfactory result could be obtained by e.g. combining further solutions of SAP like ERP Financials or ERP Human Capital Management and integration into organizational structures.

5 Discussion

In this section we will discuss the potentials of this pattern-based approach regarding the integrated perspective on compliance to balance and resolve conflicts and how this approach enables the determination of GRC effectiveness. We further discuss three implications of applying the pattern catalogue to an existing GRC portfolio.

The developed pattern catalogue provides an overview on control objectives, which GRC IS should address in order to meet control requirements. The pattern catalogue serves as a road map for executives to get an overall perspective over possible control activities. Especially the developed module structure allows navigating through solutions for specific control objectives. This allows the evaluation of potential initiatives depending on their degree of effectiveness within this specific situation and potential of integration with other initiatives. Inefficient applications can be identified easily and duplication of effort can be avoided.

The developed patterns are therefore not only useful to analyze GRC IS value propositions through elaborating actionable control requirements, but also show the need to balance and resolve conflicts. Management has to balance contradictory patterns, e.g. distrust and overperformance, ignorance and paralysis, or transaction quagmire and patent remedy. Using the developed pattern catalogue enables management to prioritize and decide in every situation without losing the integrated perspective.

The integrated perspective further helps reveal GRC IS effectiveness. For example the introduced adequacy pattern ensures an economic perspective on implementing GRC IS. Implementing too much functionality in terms of governance, risk management, and compliance will not only reduce an employee's performance, but also limits his or her motivation regarding the tasks they have to complete. Therefore, using the pattern catalogue allows executives to determine the optimal degree of governance, control, risk management, and reporting, necessary to both create transparency and to run a value adding company effectively.

Companies benefit in three ways from applying the patterns to an existing GRC IS. First, it shows that the developed patterns are useful and can be found within existing applications. It further reveals the patterns which are covered by the given application. In the case of SAP GRC 10.0, not all patterns are covered. Third, applying the patterns to an existing GRC IS and analyzing the underlying concepts reveals that some patterns are not suitable for the automatic approach of GRC IS. The pattern for ensuring the board's ability to act and the anti pattern paralysis require effective organizational structure and integration and cannot be implemented within GRC IS.

This research contributes to the body of knowledge by consolidating requirements for GRC IS through conducting a regulations-driven approach. We thoroughly connect existing requirements with information systems, which are designed to support meeting these requirements. Our research indicates that requirements can be synthesized into a defined set of capabilities, which are necessary to meet the considered regulations. We aid practitioners to soundly evaluate existing GRC IS depending on their individual requirements. The actionable patterns allow the implementation of an output-oriented evaluation of GRC tools. This research contributes to theory by bridging the gap between actual control regulations and GRC IS through developing requirements and integrating them into patterns. We further show that GRC IS are not suitable to solely fulfill each regulation without an adequate organizational integration.

Limitations of this research include the fact that laws, regulations, and standards were selected from German perspective. We further used an IS perspective on laws, guidelines, regulations, and standards. This could be enhanced with various other regulations from other fields, which might lead to new patterns which should also be taken into account. In order to reflect the patterns, we concentrated on evaluating one software portfolio. Evaluating more vendors might derive further interesting insights into the usability of the patterns. Nevertheless, the pure functionality of software modules does not guarantee proper compliance work within organizations. The patterns might be integrated with additional research on workarounds where employees bypass the established controls within the systems [17].

6 Conclusion

In this article, we reveal a solution to bridge the gap between complex control requirements and information systems, which support meeting these requirements. We showed the variety of differing requirements and the complex task of understanding how specific applications meet certain requirements. Hence, we developed a framework to classify control requirements and derived 35 control patterns. Here we introduced two control patterns and demonstrated the benefits of using such patterns in synthesizing the variety of regulations and determining the potentials of GRC IS. Although our research is still in progress, our pattern-based approach already supports evaluating GRC IS for their potential to fulfill specific control requirements.

Acknowledgments. We thank SAP AG for funding this project as part of the collaborative research centre 'CVLBA - Center for Very Large Business Applications'.

References

1. Parry, E.: SOX Wars: CIOs share ideas, fears on Sarbanes-Oxley compliance. SearchCIO.com (7) (2004)
2. Ashbaugh-Skaife, H., Collins, D., Kinney Jr., W., LaFond, R.: The effect of SOX internal control deficiencies and their remediation on accrual quality. The Accounting Review 83(1), 217–250 (2008)
3. Volonino, L., Gessner, G.H., Kermis, G.F.: Holistic Compliance with Sarbanes-Oxley. Communications of the Association for Information Systems 14 (2004)
4. Fisher, J.: Compliance in the Performance Management Context: What technologies could simplify compliance and automate information gathering? Bank, Accounting & Finance 20(4), 41–49 (2007)
5. Wiesche, M., Schermann, M., Krcmar, H.: Exploring the contribution of information technology to Governance, Risk, and Compliance (GRC) initiatives. Paper to be presented at the 19th European Conference on Information Systems (ECIS), Helsinki, Finland (2011)
6. Hagerty, J., Kraus, B.: GRC in 2010: $29.8B. In: Spending Sparked by Risk, Visibility, and Efficiency, Boston, MA, p. 12 (2009)
7. OpenPages, Risk Management Investments to Rise in 2010 (2009)
8. Syed Abdullah, S.N.H., Induslka, M., Shazia, S.: A study of compliance management in information systems research. In: ECIS 2009 Proceedings (2009)
9. Heiser, J.: Hype Cycle for Governance, Risk and Compliance Technologies. In: Gartner Hype Cycles (2010), Gartner Research Report G00205229
10. Teubner, R.A., Feller, T.: Informationstechnologie, Governance und Compliance. Wirtschaftsinformatik 50(5), 400–407 (2008)
11. Shleifer, A., Vishny, R.W.: A survey of corporate governance. Journal of Finance 52(2), 737–783 (1997)
12. Alexander, C.: The timeless way of building. Oxford University Press, New York (1979)
13. Buschmann, F., et al.: A System of Patterns: Pattern-Oriented Software Architecture: A System of Patterns. John Wiley & Sons Inc., Chichester (1996)
14. Fowler, M.: Analysis Patterns: reusable object models. Addison-Wesley, Reading (1997)
15. Brown, W.J. (ed.): AntiPatterns: refactoring software, architectures, and projects in crisis, vol. 20. Wiley, Chichester (1998)
16. Pree, W., Sikora, H.: Design patterns for object-oriented software development. In: ICSE 1997 Proceedings of the 19th International Conference on Software Engineering. ACM, New York (1997)
17. Ignatiadis, I., Nandhakumar, J.: The Effect of ERP System Workarounds on Organizational Control: An interpretivist case study. Scandinavian Journal of Information Systems 21(2), 3 (2009)