Governance, Risk and Compliance in BPM - A Survey of Software Tools

Falko Koetter, Monika Kochanowski, Jens Drawehn
Fraunhofer Institute for Industrial Engineering IAO
and University of Stuttgart IAT
Stuttgart, Germany
Email: firstname.lastname@iao.fraunhofer.de

Abstract—**Governance, risk and compliance (GRC) are current research topics in business process management (BPM). However, the state of the art in research and practice does not match. In this work, we investigate the practice of GRC in BPM tools based on a survey of 14 software providers. Identifying commonly shared features and components we determine the state of the art of GRC support in BPM tools. We found software providers agree in their definitions of GRC. Today's tools provide mature solutions for GRC, displaying a common base of features. This provides a basis for further research in the area of GRC.**

Keywords–business process management; governance; risk; compliance; state of practice

I. INTRODUCTION

Compliance to laws and regulations is a growing challenge in Business Process Management (BPM) [1] and has become a mature research topic [2]. However, compared to research, which may tackle the topic of compliance independently, often rethinking solutions and processes from scratch, commercial software needs to integrate in existing business process management systems and organizational structures [3]. Thus, the solution provided by industry and research differ [2]. In our applied research projects, we cooperate with insurance companies, banks, etc. active in the German market [4]. To understand the challenges these companies face in achieving business process compliance, the current state of practice and available commercial software needs to be surveyed. In this work, we summarize the results of a survey of software tools for business process compliance [5]. Using the results, we determine the state of the art in Governance, risk and compliance (GRC) in business process management tools in the German market.

The remainder of this work is structured as follows. Related work investigating the state of the art in science and practice is described in Section II. In Section III, we describe the focus of the survey and how it was chosen. Section IV describes the methodology of the survey. In Section V, the role of GRC in the BPM lifecycle is described. The results of the survey are given in Section VI, both regarding the software providers as well as the tool support for GRC. Finally, a conclusion and outlook are given in Section VII.

II. RELATED WORK

In [2], we conducted preliminary interviews with different stakeholders in business process compliance: experts from a BPM department, from a compliance and law department, participants at a compliance conference and BPM tool providers. We used these interviews to construct the questionnaire [6] for the survey summarized in this work. Especially we found a divide between the feature set offered by tool providers and the features and tools used by the other stakeholders. While practitioners showed an organizational divide between IT, BPM and compliance departments, tool providers divided their functionality in GRC.

Two studies regarding the state of the art of compliance in German insurance companies have been conducted in 2010 [7] and 2013 [8]. Both studies find a lack of integration between compliance and other processes. Only 11 percent and 7 percent respectively state a full integration with other processes. In another survey [9], 93 percent of insurance companies state that their compliance activities are not or only partially supported by IT.

[1] provides an analysis of emerging IT challenges for compliance management by conducting interviews with Australian compliance experts. Challenges identified include the high cost and the difficulty of providing evidence for compliance. A need for affordable software tools is identified, which not only tackle compliance in BPM but also the communication to and among staff as well as the documentation of compliance knowledge and the incentivization of a compliance culture.

[3] presents the results of an exploratory study of 8 GRC software providers. The survey found differing understanding of GRC between the vendors and found solutions to differ in their degree of integration. As marketable software must be compatible to existing enterprise structures, it differs from GRC research, which may propose more sweeping changes and rethink GRC outside of the constraints of the status quo.

Forrester publishes a periodic report [10] on GRC platforms. For this, 66 GRC customers were surveyed, almost half of which use more than one GRC platform. Use cases among customers vary extremely, leading to tools with broad capabilities. Though users found benefit in the GRC tools, overall satisfaction with end user interfaces, dashboards and analytics was low. 18 software providers were studied and classified by current offerings, strategy and market presence, though the classification was not broken down to a feature level. Compared to the companies in this work, the chosen companies were larger global players and not limited to BPM tool providers.

Similarly, Gartner published multiple studies in the area of GRC. However, Gartner decided in 2014 to reset their approach to GRC, focusing on use cases and real life use [11] instead of features. Similarly to this work, they found feature sets and presentation to be similar and use this reset to better differentiate between tools.

III. FOCUS OF THE SURVEY

During preliminary interviews we discovered that *Compliance* as a general term does not fully match the features software tools provide [2]. Therefore, we extended the scope to GRC. In [12], a frame of reference for GRC is constructed, in which GRC is defined as *an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness‘* [12].

This frame of reference is used to define the focus of the survey, as shown in Figure 1. While GRC encompasses all aspects of an organization, the survey focuses on the aspects relevant to processes, though this distinction is not clear-cut. Governance in the context of BPM includes the governance of processes and the governance of IT which is used to realize these processes. Risk management is realized by internal controls or enterprise risk management (ERM). Compliance of business processes is often part of BPM products or realized by extensions or integrated components.

IV. Methodology

We invited all known BPM software providers active in the German market to participate in our survey. 28 providers partook in a general survey of BPM tools [13]. Of these providers, 14 opted to partake in an additional in-depth GRC survey. A full survey describing each provider in detail is available [5] in German. The providers were sent an online questionnaire containing 46 structured and unstructured questions regarding the software tool and the software provider. All 14 providers fully completed the questionnaire.

The full questionnaire can be found at [6] (in German).

The results of the questionnaire are listed in detail and analyzed in the GRC survey [5]. This work summarizes the findings of the survey to determine the state of the art among all 14 providers.

V. GRC in the BPM lifecycle

The BPM lifecycle shows the phases a business process goes through organized in a cycle to indicate that activities are performed continuously to optimize the process [14]. Figure 2 shows the lifecycle and GRC activities associated to each phase, which will be explained in the following section.

Governance spans the whole process lifecycle, prescribing frameworks, templates and best practices for all steps and artifacts. During process redesign and implementation different versions of a process need to be tracked as well as protected from unauthorized access and changes. Before a new version is implemented, a sign-off process can take place to make sure the new version is authorized.

In the area of risk management, during process discovery and process analysis risks need to be identified and assessed. These risks can be modeled and visualized during process (re)-design to make informed design decisions. This includes the definition of internal controls for risk management. During process execution risks need to be tracked and if necessary internal controls need to counteract occurring risks. Finally, the results of these activities need to be stored in a verifiable and traceable way, to provide data for analysis and reporting.

Compliance requirements are defined during process (re)-design and enforced at the appropriate parts of the process lifecycle. Requirements can be enforced during process (re)-design, implementation and execution. Requirement fulfillment needs to be monitored and stored to provide documentation and reports as well as provide a basis for analysis.

During our research we identified four types of BPM software supporting GRC functionality.

- **Process modeling tools** allow creating process models, but provide little functionality beyond that. In comparison to other tools, they have a low barrier to entry and are used if the main task is documenting processes. They may be used to model relevant risks and internal controls and to document compliance requirements already covered within the process models. Regarding governance, these tools provide process model management support, for example templates, sign-off and version control.
- **Process analytics tools** allow analyzing processes and may contain functionality for process simulation and optimization. These tools often contain process modeling functionality or are bundled with a process modeling tool to provide models as a basis for analysis.
- **Business process management tools** or BPM systems [14] support the whole process lifecycle including process execution. Typically process models are used to create and run process instances. This offers extensive possibilities to support internal controls, risk tracking, enforcement and monitoring of compliance requirements. Additionally, BPM tools can fully support governance processes. Some BPM tools may not offer a full execution environment but rather provide parts of the described functionality - for example by offering internal controls for a process executed by other means.
- **Workflow management systems** are focused on process execution. Similar to BPM tools they use process models to instantiate and run processes. Other parts of the process lifecycle are supported scarcely or not at all.

Note that the survey was limited to BPM providers, which is why dedicated GRC tools without a BPM component are not covered by the survey.

VI. Results

In this section, we give the results of the survey to illuminate the state of the art in business process management software regarding GRC.

A. Participants

All 14 participants are business process management software providers active in the German market, which offer GRC functionality as part of their tools. Of these 14 participants, 6 are companies with less than 100 employees, while 8 are companies with 100 or more employees.

For 6 providers, BPM is the only business segment. For 5 providers, it is the most important business segment. For the remaining 3 providers, it is one of several important business segments. All 14 companies offer BPM software and all but one additionally offer BPM consulting services. 6 companies offer other software. 6 companies offer other consulting services.

During the survey, companies were questioned since when compliance is a focus of their activities. All companies except one started focusing on compliance after the year 2000. 9 companies named a date between 2000 and 2009, 4 companies

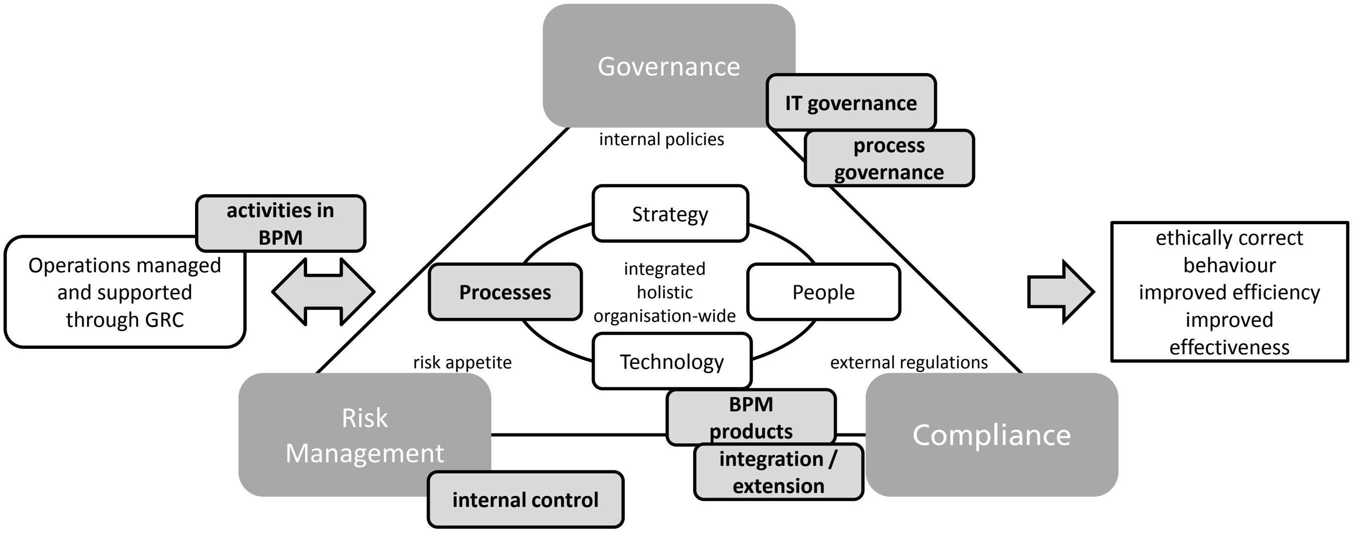

Figure 1. Framework for GRC with focus areas of survey (bolded, grey). Based on [12]

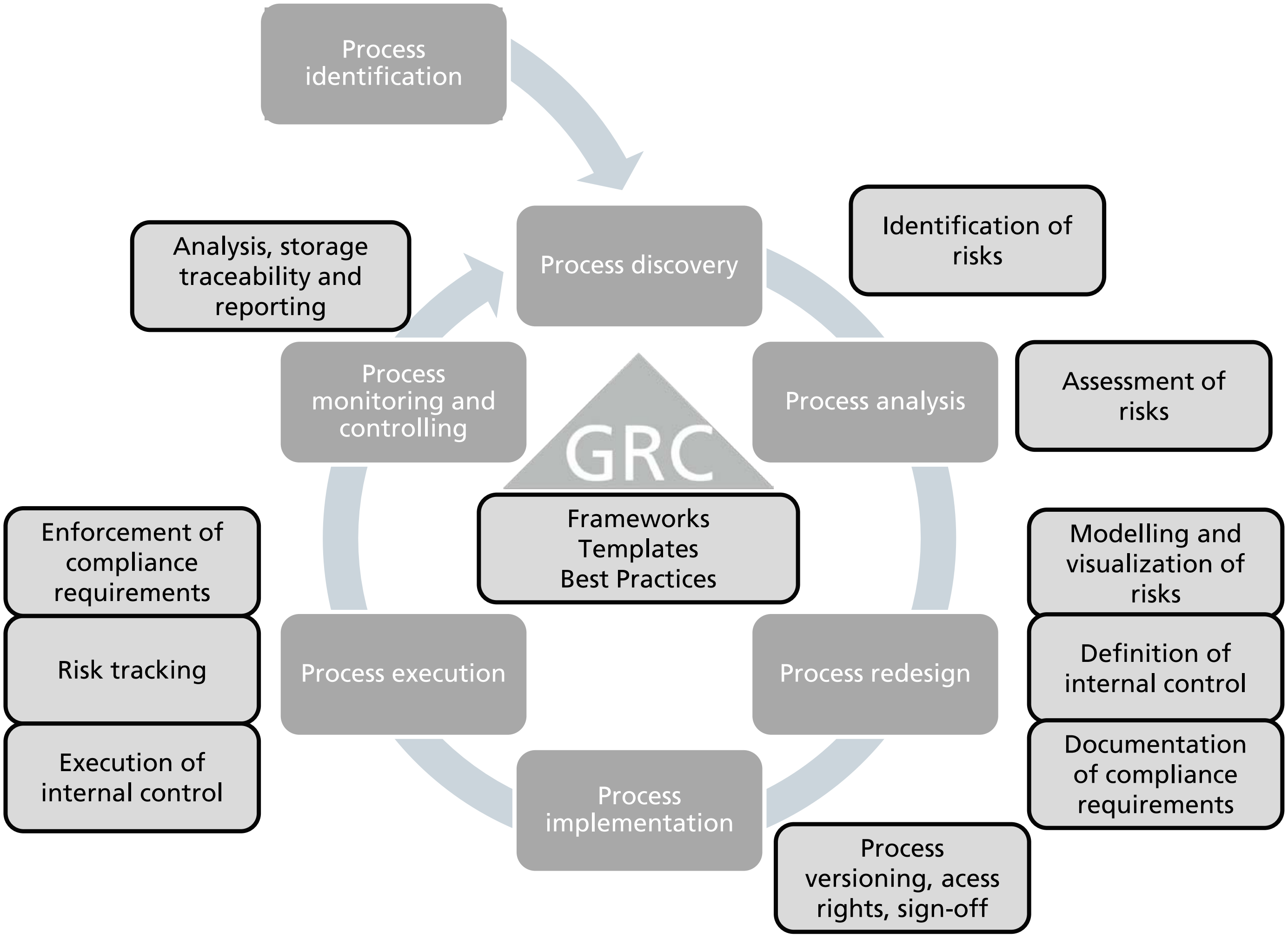
Process identification
Process discovery
Identification of risks
Analysis, storage traceability and reporting
Process monitoring and controlling
Process analysis
Assessment of risks
GRC
Frameworks
Templates
Best Practices
Enforcement of compliance requirements
Modelling and visualization of risks
Risk tracking
Process execution
Process redesign
Definition of internal control
Execution of internal control
Documentation of compliance requirements
Process implementation
Process versioning, acess rights, sign-off

Figure 2. GRC activities in the process lifecycle. Based on [14]

named a date 2010 or later. This indicates a rising demand for compliance functionality in business process management tools within the last 10 years.

B. Software tools

In this section, a general classification of the surveyed software tools is given to illustrate on which areas the software providers focus.

Regarding the BPM lifecycle (see Section V), all software providers support process discovery and process analysis. 9 providers support business process simulation. 11 providers support process execution, of which 7 provide a workflow engine. Process monitoring is supported by 9 providers.

Regarding tool classification, 3 software tools can be classified as process analytics tools, one can be classified as a workflow management system and 10 can be classified as business process management tools. It is to note that the bundling of software between providers varies. Some provide a single feature-rich solution, while others provide a collection of independent components that work together.

Looking at GRC, all software providers focus on all three areas. This indicates a trend to integrated GRC solutions.

In the survey, companies were allowed to indicate classes of business they focus on. However, no company named a special focus. This indicates that software tools are general purpose and not tailored to a specific industry.

C. Governance

To get the view of software providers on governance, we asked them for their definition of governance. Most providers see governance as a task for the enterprise as a whole, encompassing other topics besides process, e.g., organizational structure, roles, responsibilities and documentation. Governance is a leadership task, providing and enforcing rules and regulation frameworks as well as best practices.

Software components for governance encompass process organization (process versioning, access rights, sign-off, etc.), modeling and quality guidelines, modeling support and model checking, documentation and change management.

We identified the following software features as state of the art, which is supported by almost all software providers:

- Built in collections of best practices regarding modeling guidelines, etc.
- Creation and management of custom modeling guidelines
- Automated checking of process models using modeling guidelines
- Process portal or similar platform for collaborative business process management
- Support of management processes (e.g., sign-off)
- Version management of process models

As shown in Figure 2, Governance in BPM focuses on process design and implementation, aiding process modeling, collaboration and model management throughout the lifecycle. Governance also includes a knowledge management component, helping to communicate guidelines, templates and best practices.

Other features supported by some tools are:

- Process model templates and fragments enabling reuse
- Assisted modeling (automatic layout, model validation, etc.)
- Variant management of process models
- Governance dashboards
- Link of BPM and organizational structure

Several frameworks related to governance exist and may be used separately or in conjunction [15]. The following standards are most commonly supported by software providers:

- Control Objectives for Information and Related Technology (*COBIT*) [16] is supported by 8 of 14 providers
- Committee of Sponsoring Organizations of the Treadway Commission framework (*COSO*) [17] is supported by 4 of 14 providers
- Information Technology Infrastructure Library (*ITIL*) [18] is supported by 4 of 14 providers
- International Organization for Standardization (*ISO*) 9000/9001 is supported by 4 of 14 providers

Other supported standards include ISO 27001, ISO 31000, European Foundation for Quality Management (EFQM) model, Capability Maturity Model Integration (CMMI) and Software Process Improvement and Capability Determination (SPICE).

Several features to support these standards are included in most software tools:

- Checklists for requirements, etc.
- Reference process models
- Reference key performance indicators
- Linking of modeling elements to rules and requirements
- Linking of management processes to rules and requirements
- Support for reviews and audits

To summarize, all software providers focus on process governance, but link it to other areas of governance as well. The basic feature set is homogenous among the tools. Regarding governance frameworks the support varies among tools, indicating there is no dominant established governance standard, though a further investigation of industry sectors may give a clearer picture of standard proliferation.

D. Risk

Similarly to governance, we asked the software providers for a definition of risk management, showing a common view between all providers. Risk management is itself seen as a process by the software providers, including risk identification, assessment and management. Often used words include control and inspection measure. Aside from general risk management in the enterprise, providers emphasize the linking of risks to processes.

Software components for risk management include risk modeling and visualization, risk tracking and monitoring, risk analysis, documentation and reporting and risk control.

We investigated four areas of risk management to identify software features.

In the field of risk modeling and visualization, the following features are included in most software tools:

- Risk modeling
- Linking of risks to process activities
- Linking of risks to other modeling elements
- Linking of risks to other objects (e.g., roles)
- Visualization of risks within process models
- Documentation of risks in a table
- Visualization of risks in a risk matrix [19]
- Hierarchical aggregation of risks

Other features supported by some software tools include other visualizations (e.g., heat maps, dashboards, customized reports and portlets), import and export of risks in external risk management systems, integration of risk and document management. This indicates three main activities. First, the risks are identified and modeled, then they are located within the process and finally they are visualized and documented.

In the field of risk tracking and monitoring, the following features are included in most software tools:

- Management of risk amounts and probability of occurrence
- Questionnaires to assist in risk tracking
- Monitoring of risks during process execution
- Triggering of risk management processes for certain risks

Other supported features by some software tools include risk monitoring dashboards, management of risk metadata (e.g., mandatory and optional information, assets, etc.) and link to response management.

In the field of risk analysis, documentation and reporting, the following features are included in most software tools:

- Creation of risk reports
- Audit-proof storage of reports
- Export of risk reports

Other supported features include risk visualization and analysis (in portals, cockpits, dashboards, etc.), creation of a data warehouse and export functionality of raw data.

All software tools include internal controls, which allow companies to control their risks by defining and implementing controls, audits, countermeasures, etc.

For the definition and documentation of internal controls, the following features are included in all software tools:

- Definition of controls
- Assignment of controls to risks
- Assignment of controls to processes
- Definition of roles for internal controls
- Visualization of controls within a process model

Most tools support Visualization of risks and controls in a risk control matrix. Additional features supported by some tools are the assignment of control tests and results to controls and integration of document management, organizational structure and response management.

11 of 14 tools support the execution of internal controls. The following features are supported by most of these tools:

- Performing controls in the process execution environment
- Scheduling and performing controls outside of the execution environment
- Audit-proof records of performed controls
- Analysis of performed controls

To summarize, risk management is supported throughout the process lifecycle, though some tools do not provide risk management support during process execution. All tools contain internal controls as an integral part of risk management in BPM.

E. Compliance

Similar to the other topics, we asked the software providers for a definition of compliance. All providers define compliance as conformance to rules and regulations. Aside from process compliance they mention other parts of the enterprise, e.g., personnel, culture, strategy, goals, responsibilities and components. Compliance is not seen as an isolated BPM topic, but as an encompassing task throughout the enterprise.

Compliance features can be divided in two categories. Definition of compliance requirements and checking of compliance requirements. It is to note that checking may mean both the enforcement of a requirement or the monitoring of a requirement, depending on the tool and the kind of requirement. For example, structural requirements to a process model can be enforced, while timing requirements during execution can only be monitored.

The following features regarding compliance requirement definition are included in most software tools:

- Definition of compliance requirements for business processes
- Management of requirement documents (regulatory texts, etc.)
- Linking of compliance requirements to documents
- Linking of compliance requirements to process steps
- Linking of compliance requirements to other elements
- Documentation of compliance requirements in a table
- Visualization of compliance requirements within process models
- Audit-proof record of compliance requirements and changes to them

Similarly to risk management, three main activities can be identified. Compliance requirements are derived from regulatory documents and defined, then located within the process or related artifacts and finally documented for further modification as well as for audits.

Regarding compliance checking, not all tools support automated compliance monitoring, which seems to be not part of the state of the art. However, most tools support compliance enforcement with the following features:

- Creation and processing of checklists for compliance requirements
- Templates and fragments for common compliance requirements
- Visualization of current compliance status
- Aggregated visualization of overall compliance status
- Generation of compliance reports

This shows that automated compliance enforcement is not state of the art, as manual compliance enforcement using checklists is part of most tools. This may indicate both a lack of process automation as well as the difficulty of automated requirement checking. In our talks with users, they noted difficulties in defining precise compliance requirements from laws as well as in process automation, as processes are not yet fully documented [2]. Checklists can provide an interim solution to be compliant.

9 of 14 software providers offer a business rules engine, either as part of their tool or as a separate component. Business rules may be used to automatically monitor, enforce and document compliance requirements, but necessitate automated business processes.

8 of 14 software providers provide built-in rulesets for regulatory texts. 3 providers support Basel 2/3 [20], 3 providers support the SarbanesOxley Act of 2002 (SOX) [21]. Other rulesets are only supported by single providers. As no provider has named classes of business they specialize on, this may indicate a high level of customization in the compliance rulesets of their customers so built-in rulesets are of limited use.

To summarize, the definition of compliance requirements in the context of documents and business processes is supported by all software tools. Regarding compliance checking, the state of the art in compliance checking is more uneven. Some solution components help model compliant processes and check compliance manually (e.g., by checklists). For automated compliance checking, business rules engines are the prevalent solution.

VII. Conclusion and outlook

In this work, we summarized a survey of 14 BPM software providers active in the German market. This survey investigated the support of GRC in BPM tools.

Support of GRC in business processes is not only a mature research topic, but has also been incorporated in software tools. Software providers showed a common understanding of GRC, providing similar definitions for all three terms. Governance is supported by a homogenous feature set, indicating a proven approach in practice. Risk management is supported throughout the BPM life cycle with internal controls as an integral component. Definition of compliance requirements is supported uniformly, but compliance checking is realized more unevenly with business rules engines and checklists as the prevalent solutions.

Overall, the industry provides mature tools for handling GRC in business process management. While state of the art in industry can be a helpful indicator for scientific research, it alone does not suffice because the questions and constraints for industry and science are different. Examples are the questions of interoperability and integration, which were not covered by the survey.

Acknowledgment

The work published in this article was partially funded by the Co.M.B. project of the Deutsche Forschungsgemeinschaft (DFG) under the promotional reference SP 448/27-1. The authors would like to thank all participants.

References

[1] N. Syed Abdullah, S. Sadiq, and M. Indulska, “Emerging challenges in information systems research for regulatory compliance management,” in Advanced Information Systems Engineering, ser. Lecture Notes in Computer Science, B. Pernici, Ed. Springer Berlin Heidelberg, 2010, vol. 6051, pp. 251–265.

[2] M. Kochanowski, C. Fehling, F. Koetter, F. Leymann, and A. Weisbecker, “Compliance in bpm today - an insight into experts’ views and industry challenges,” in Proceedings of INFORMATIK 2014. GI, 2014.

[3] N. Racz, E. Weippl, and A. Seufert, “Governance, risk & compliance (grc) software-an exploratory study of software vendor and market research perspectives,” in System Sciences (HICSS), 2011 44th Hawaii International Conference on. IEEE, 2011, pp. 1–10.

[4] F. Koetter, M. Kochanowski, and M. Kintz, “Leveraging Model-Driven Monitoring for Event-Driven Business Process Control,” in 1. Workshop zur Ereignismodellierung und verarbeitung im Geschaeftsprozessmanagement (EMOV). to appear, 2014.

[5] M. Kochanowski, J. Drawehn, F. Koetter, and T. Renner, Compliance in Business Processes - Business Process Management Tools 2014 (in German). Fraunhofer Verlag, 2014.

[6] Kochanowski, Monika and Koetter, Falko, “Compliance in Business Process Management (in German),” 2014, last accessed 29.01.2015. [Online]. Available: http://www.e-business.iao.fraunhofer.de/de/projekte/beschreibung/compliance.html

[7] BDO AG Wirtschaftsprüfungsgesellschaft, “Compliance Survey of Insurance Companies (in German),” 2010, last accessed 29.01.2015. [Online]. Available: http://www.bdo.de/uploads/media/BDO_Compliance_Studie.pdf

[8] ——, “Compliance Study in Insurance Companies (in German),” 2013, last accessed 29.01.2015. [Online]. Available: http://www.bdo.de/uploads/media/-BDO_Compliance_Studie_Versicherung_web.pdf

[9] BearingPoint GmbH, “Agenda 2015 : Compliance Management as growing challenge for insurance companies (in German),” 2012, last accessed 29.01.2015. [Online]. Available: http://www.bearingpoint.com/de-de/7-4788/agenda-2015-compliance-als-stetig-wachsende-herausforderung/

[10] C. McClean, N. Hayes, and R. Murphy, “The forrester wave: Governance, risk, and compliance platforms, q1 2014,” 2014.

[11] Proctor, Paul, “Gartner Resets Approach to GRC,” 2014, last accessed 29.01.2015. [Online]. Available: http://blogs.gartner.com/paul-proctor/2014/02/03/gartner-resets-approach-to-grc/

[12] N. Racz, E. Weippl, and A. Seufert, “A frame of reference for research of integrated governance, risk and compliance (grc),” in Communications and Multimedia Security. Springer, 2010, pp. 106–117.

[13] J. Drawehn, M. Kochanowski, and F. Koetter, Business Process Management Tools 2014. Fraunhofer Verlag, 2014.

[14] M. Dumas, M. La Rosa, J. Mendling, and H. A. Reijers, Fundamentals of business process management. Springer.

[15] J. J. S. Peña, E. Fernández Vicente, and A. Moratilla Ocaña, “Itil, cobit and efqm: Can they work together?” International Journal of Combinatorial Optimization Problems and Informatics, vol. 4, no. 1, 2012, pp. 54–64.

[16] ISACA, “COBIT 5: A Business Framework for the Governance and Management of Enterprise IT,” 2014, last accessed 29.01.2015. [Online]. Available: http://www.isaca.org/cobit

[17] COSO, “Internal Control - Integrated Framework,” 2013, last accessed 29.01.2015. [Online]. Available: http://www.coso.org/ic.htm

[18] AXELOS, “Information Technology Infrastructure Library,” 2014, last accessed 29.01.2015. [Online]. Available: https://www.axelos.com/itil

[19] P. R. Garvey and Z. F. Lansdowne, “Risk matrix: an approach for identifying, assessing, and ranking program risks,” Air Force Journal of Logistics, vol. 22, no. 1, 1998, pp. 18–21.

[20] Bank for International Settlements, “International regulatory framework for banks (Basel III),” 2014, last accessed 29.01.2015. [Online]. Available: http://www.bis.org/bcbs/basel3.htm

[21] P. Sarbanes, “Sarbanes-oxley act of 2002,” in The Public Company Accounting Reform and Investor Protection Act. Washington DC: US Congress, 2002.