Approach to the Classification of Information Technology Governance, Risk and Compliance Frameworks

Mike Krey
Center for Business Information Technology
Zurich University of Applied Sciences
Winterthur, Switzerland
krey@zhaw.ch

Bettina Harriehausen and Matthias Knoll
Department of Computer Sciences; Faculty of Economics and Business Administration
Darmstadt University of Applied Sciences
Darmstadt, Germany
B.Harriehausen@fbi.h-da.de; Matthias.Knoll@h-da.de

***Abstract*— The issues, opportunities and challenges of effectively governing an organization's Information Technology (IT) demands and resources have become a major concern of the Board and executive management in many organisations today. The Swiss healthcare is currently searching for methods and practices for the solution of operational planning and optimisation of IT processes. To make sure that the corporate hospital strategy leads to adequate business decisions an IT GRC Framework for Healthcare will be needed. This paper presents the first task – the classification of existing IT governance frameworks – within the development process. After the dissociation of IT management and corporate governance – a proposal for a classification scheme for IT governance frameworks is described and the application of the classification template is explained.**

Keywords- Governance, Risk, Compliance, Healthcare, Classification, Framework

I. INTRODUCTION

Governance, Risk Management and Compliance (GRC) is an executive level concern in many enterprises today. It is an approach that addresses not only the establishment of business rules but more importantly how those rules are integrated into sensible organisational structures, embedded into the day-to-day business processes of the organisation, communicated (including ongoing training) and monitored for compliance (Menzies, 2006). In this paper the GRC context governance means IT related governance and describes the topics that the executive management needs to address to govern IT within their hospital.

As ascertained by a survey with several Swiss hospital CIOs in 2009 the majority (64%) replied that the healthcare sector is a complex and heterogeneous economic sector and cannot be compared to other industry sectors where Control Objectives for Information and related Technology (CobiT) and other IT governance framework have been successfully applied. Organisational structures, legal restraints and over the years increased heterogeneous IT systems are just a few aspects which would make the healthcare sector a sensible field for the implementation of IT governance. It is pleasing to see that hospitals appear to be taking IT governance as a part of their governance realm and that 45% of the hospitals surveyed adopt IT Infrastructure Library (ITIL) as an IT governance framework, while about 8% of hospitals have or will adopt CobiT, IS0-17799 or a proprietary framework. The majority believed that their ITIL approach is 'repeatable but intuitive', whilst no one thought their ITIL approach is 'fully optimised' and the processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modeling with other hospitals (Krey et al., 2010).

To make sure that the corporate hospital strategy leads to adequate business decisions an IT GRC Framework for Healthcare will be needed. This framework can help to minimise risks and should consider the special requirements of the healthcare sector. The development of a healthcare specific IT GRC framework consists of three main phases. (1) Classification of existing IT governance frameworks. With the help of a classification scheme users as well as framework developers are provided with an overview of the framework e.g. relating to its addressed GRC area, framework design or framework application. (2) Exploration and systematisation of the factors influencing IT governance structures, processes and outcome and the requirements and expectations within the healthcare. To enhance the future reusability of such a framework, detailed information about the application method, requirements from the healthcare processes (business and IT), accessibility and levels of mutability are required. (3) Mapping of the existing IT governance frameworks and the derived requirements within the healthcare. This identifies a requirements overlap which can be fully or partly covered by the existing frameworks. In addition to it the mapping points out explicitly the gaps where healthcare specific requirements cannot be fulfilled with functionalities provided by the frameworks and where further research will be needed.

To give a widespread and lasting approach for IT governance in the healthcare sector, it is not sufficient to analyse only one framework like CobiT. Instead, it is necessary to complement it with the knowledge of other frameworks and the findings of academic research. This paper presents a classification system for IT governance frameworks. This task is discussed in the following sections. After the dissociation of IT management and corporate governance – a proposal for a classification scheme for IT governance frameworks is described and the paper ends with some concluding remarks.

978-0-7695-4376-5/11 $26.00 © 2011 IEEE
DOI 10.1109/UKSIM.2011.73

II. IT GOVERNANCE AND IT MANAGEMENT

The difference between IT management and IT governance has been subject to confusion and myths in the IT community (van Grembergen, 2004; Johannsen et al., 2007). Peterson (2003) provides a clear insight into the differences between these two notions. “Whereas the domain of IT management focuses on the efficient and effective supply of IT services and products, and the management of IT operations, IT governance faces the dual demand of (1) contributing to present business operations and performance, and (2) transforming and positioning IT for meeting future business challenges”. As depicted in figure 1, Peterson (2003) suggests positioning IT management and IT governance along two dimensions, business orientation and time orientation.

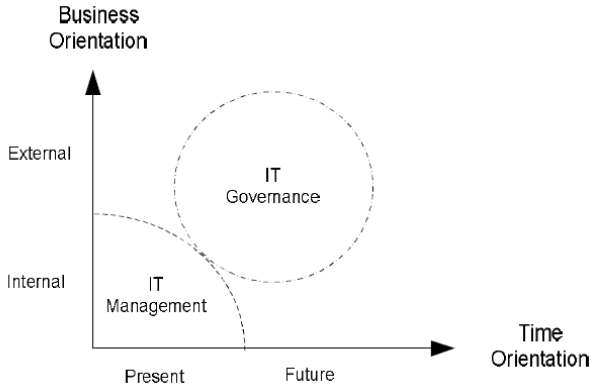

Figure 1. IT governance and IT management (Peterson, 2003)

Even today much of the literature does not differentiate IT management from IT governance. The two concepts are often regarded as synonymous, even though they clearly differ (Sohal and Fitzpatrick, 2002). An important key differentiator is that management tasks have an internal focus and are done at the departmental level, while IT governance is a corporate level activity with a purposeful external focus (Sohal and Fitzpatrick, 2002). Management is concerned with what kind of decisions are made, while governance is concerned with who should make decisions and how these decisions will be monitored. A change to an organisation’s strategy may well require changes to the management but not the governance of an asset (Weill and Ross, 2007). In IT management, the provision of IT services and products can be assigned to an external provider (as in outsourcing), while IT governance is specific to an organisation. Since governance gives direction and control over IT expenditures, it cannot be outsourced and is the direct responsibility of the senior executive (Peterson, 2003).

III. IT GOVERNANCE AND CORPORATE GOVERNANCE

Lee and Lee (2009) characterised IT governance by the attributes transparency, control, effectiveness and efficiency. Transparency and control are bequested by the discipline of corporate governance seeking to ensure the transparent management and control of IT assets through forms of committee. In other words they accentuate the integral part of an organisation to be represented in IT governance, however most researchers looks more narrowly to the processes of IT management than to the structure of IT organisations (Heier et al., 2007).

According to the literature, IT governance is concerned with the board's responsibility to ensure that the company's IT meets the present and future demands of the business and of the business's customers (Standards Australia, 2005; Peterson, 2003) and that the risks arising from IT are mitigated (Standards Australia, 2005; Cilli, 2003). It does this by assessing, directing and monitoring the company's IT to ensure that the required benefits and business outcomes are being achieved (Standards Australia, 2005). Jordan and Silcock (2005) suggest that an organisation that is able to do this is "IT-capable" and summarise this capability in the following terms: "The board must be assured that the organisation is able to identify needs and opportunities to exploit IT, and is then able to satisfy them".

The Board is assisted in these tasks by the company's executive management and its IT management. According to van Grembergen and de Haes (2008) IT governance is practised at three levels within the organisation. These are:

- The strategic level, which they take to be the company board,
- The senior management level, and
- The operational management level.

All of these levels thus need to be addressed by any explanation of IT governance. Johnstone et al. (2006) propose that there are three components to IT governance. These are:

- An authority structure,
- A set of board policies, and
- A set of mechanisms or processes.

They note that the authority structure is that set up by the board to manage IT, which includes both appointments such as the IT manager and (often) an oversight committee. The board policies are those "decision guidelines and restraints" (Johnstone et al., 2006) devised by the board to control the use of IT in the company, including the business and IT strategies (p. 4).

IV. PROPOSAL FOR A CLASSIFICATION SYSTEM

Several frameworks, reference models and best practices, issued by both international standardisation organisations and private organisations exist in addition to the de facto standard CobiT for managing the different aspects of IT and its organisation (Lahti and Peterson, 2005; IT Governance Institute, 2008; van Grembergen and de Haes, 2008; Johannsen et al., 2007; Addy, 2007).

A variety of approaches to classify IT governance frameworks can be found in academic literature.

- mostly a listing of the frameworks is provided,
- a detailed comparison of individual frameworks (Guldentops et al., 2010) can be found or
- sections of the frameworks are analysed by specific fields of application (e.g. IT security) (ISACA Switzerland Chapter, 1998).

Just a few approaches deal with the systematisation of frameworks, whereby it is the fact the tabulation of IT governance frameworks that is meant here and not so much the survey-like textual description of the actual stock of frameworks found in literature. The author conducted two parallel reviews, one focusing on the scientific literature and the other drawing on alternative sources available via the World Wide Web.

A couple of those approaches provide a deeper comparison of more than two models. Mostly the comparison is limited to the features of the model itself structured by abstract attributes without a deeper analysis of the provided scope of the process description (Walter and Krcmar, 2006). Based on this, there is also a lack of studies regarding the question of which framework or parts of it should be used in which situation. With regard to the purpose of this work an independent classification system for IT governance frameworks is needed. Whatever classification principle is used, the main problem in developing an appropriate classification lies in limiting the scope to as few descriptive characteristics as possible which should at the same time explain the diversity and be as mutually exclusive as possible. For this purpose the characteristic-based approach has been used to develop the classification scheme as an unambiguous placement is not always possible.

For the classification of IT governance frameworks the set of characteristics is summed up in three different dimensions: (1) general framework attributes, (2) framework design and (3) framework application. The three dimensions are derived from the considerations by (Fettke et al., 2005; Walter and Krcmar, 2006; IT Governance Institute, 2006b; 2003; Schmidt, 2007) and their approaches for criteria for characterising process reference models.

General framework attributes (1) are used to describe the basic characteristics of an IT governance framework. The purpose of the selected attributes is to provide users as well as framework developers a first overview of the framework relating to its addressed GRC area, the targeted audience, origin of the framework, and the primary sources, where the framework is described in more detail. Comparable attributes also have been applied for reference models (Schmidt, 2007). In addition, and along with the classification scheme provided by the IT Governance Institute (IT Governance Institute, 2006b), further characteristics concerning the design and use of IT governance frameworks are provided (the list is not exhaustive).

For the *framework design* (2) attributes pertaining to the construction and organisation of the model such as the used concept of "IT governance" or the basic structure of the model are proposed. The intention here is to help potential users or framework developers to better understand the concepts behind an IT governance framework. For the *framework application* (3) differentiating attributes with respect to the deployment of the framework such as tool support or practicality of evidence are proposed. The identified attributes should help users in the selection of a proper framework as well as show developers possibilities for improvement of their framework.

Table 1 illustrates an exemplary application of the classification scheme by using the CobiT framework. A detailed description of the differentiating attributes is given in the following subsections. This template helps to map the attributes of the existing IT governance frameworks and the derived requirements within the healthcare to get a requirement overlap on which the IT GRC Framework for Healthcare will be based on.

TABLE I. EXAMPLE OF A CLASSIFIED IT GOVERNANCE FRAMEWORK

Dimension	Attribute	Example
General framework attributes	Name	Control Objectives for Information and Related Technology
	Acronym	CobiT
	Current Version (year of publication)	4.1 (2007)
	Primary source	Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)
	Seconary source	www.itgi.org/cobit
	GRC area	Governance, Risk, Compliance
	Origin	Practice
	Targeted audience	Management-oriented
	Access	Freely available
	Domain	Public-domain
Framework design	Concept of IT governance	CobiT recognises 34 IT processes that are grouped into four domains. The four domains are: Plan and Organise, Acquire and Implement, Deliver and Support, Monitor and Evaluate.
	Composition	Each process has a level of maturity (numerical) from 0-5. (0 is non-existent and 5 is optimised.) This scale can be used for a number of key evaluations, such as the level of maturity a process is currently at within your organisation, what level of maturity the processes should be at, what level is considered best practice, & what level the best of your competitors/other organisations have achieved.
	Reliability	Validated & verified
	Mutability	Industry-neutral, mutable
Framework Application	Support	Textual description & tool support
	Practicality of evidence	Implicit improvement activities

A. Framework Design

The framework design attributes are used to describe the form and style of a framework. For this purpose, the attributes concept of IT governance, composition, reliability, and mutability are proposed. The attribute concept of IT governance answers the question how the topic of IT governance is approached and to which extent the examined frameworks address the different delimitations which have been discussed in the sections 3 and 4. As Spafford (2003) points out, there is limited overlap between the IT governance standards – most frameworks or best practices

are reflected on an one-dimensional manner by the related literature, either focusing on (1) processes, i.e. how IT processes deliver the information that the business needs to achieve its objectives (IT Governance Institute, 2007), on (2) lifecycle, i.e. the way service management is structured, and the way the various lifecycle components are linked to each other and to the entire lifecycle system within the IT (Office of Government Commerce; 2005), or on (3) people capability, i.e. to which extent the management is able to create a mechanism through which it can provide the business with technology leadership (Calder, 2005). The concept of IT governance often motivates the composition of the framework. The attribute composition examines the aspect of the methodical approach applied within the frameworks (i.e. Six Sigma, balanced scorecard or maturity model approaches). Maturity models are increasingly being applied within the field of IT, both as informed approach for continuous improvement (Ahern et al., 2004) or as means of benchmarking or self-assessment (Conwell et al., 2000; Hakes, 1996). Conwell et al. (2000) distinguish three basic maturity model designs: (1) Maturity grids aim at illustrating a number of levels of maturity in a simple, textual manner (normally not exceeding a few pages of text), (2) Likert-like questionnaires are comparable with maturity grids, but the focus is more inclined on to scoring specific statements of "good practice" and not to describing the overall levels of maturity, and (3) CMM-like models, which are based upon a more formal architecture, specifying a number of goals and key practices to reach a predefined level of sophistication. Although more elaborate, CMM-like models also entail a greater complexity due to a wide range of scales and subscales for the assessment of maturity. Another important characteristic to enhance the reusability of an IT governance framework is its degree of reliability (Betz, 2007; Lee and Lee, 2009). Conwell et al. (2000) differentiate between verified and validated frameworks. Verification is thereby the process of determining that a framework "represents the developer`s conceptual description and specifications with sufficient accuracy" and validation is the degree to which a framework is an "accurate representation of the real world from the perspective of the intended uses of the framework. If we examine the identified framework, it can be concluded that most of them cannot be categorised as validated (perhaps at most as verified). Thus, in order to enhance the reusability and reduce criticism on the poor theoretical grounding of IT governance frameworks in literature (Keyes-Pearce, 2002; Gottschalk, 2006; Calder, 2005) the emphasis on developing new IT governance frameworks should lay on extensively testing these models in terms of validity, reliability and generalisability.

The last characteristic concerning the design of the IT governance frameworks is the level of mutability. This is of particular importance – but for all that sometimes neglected – as, on the one hand, the business requirements are growing and therefore the framework`s solutions stages and improvement activities have to be refaced from time to time (Krey et al., 2010) (e.g. modify requirements for reaching a certain maturity level due to the emergence of new best practices and technologies), on the other hand, changes in the form and function are needed to ensure the standardisation and industry acceptance of the framework (e.g. amend the framework focus areas to be compliant with changed organisational structures or legal restraints).

B. Framework Application

To describe the framework application, the attributes support of application and practicality of evidence are proposed. As regards the support of the model application, three stages of assistance are differentiated. In the first case, the users are given no supporting materials at all. Especially de facto standards tend to omit what the best starting point is and which methods should be use to achieve the objectives. The more sophisticated frameworks, also deliver a textual description or handbook how to configure the deployment of the framework. However, the most advanced auxiliary means is the instantiation of the IT governance framework or parts of it on form of software tools (Johannsen et al., 2007). Another interesting characteristic concerning a framework for IT governance use is the practicality of evidence (i.e. the way how suggestions for improvement are made). In this regard, it is distinguished between implicit improvement activities, i.e. a general recommendation on the tacit assumption of the predefined objectives, and explicit recommendations, for example telling exactly what to do in order to enhance a particular activity, process or skill. In the case of the reviewed IT governance frameworks, a clear tendency to implicit recommendations exists. However, this is not astonishing given that the definition of explicit improvement activities is difficult or sometimes even futile. Nevertheless, explicit recommendations are desirable when a framework addresses a precisely delimited problem domain and the dissimilarity of the organisational realities does not play a major role.

V. CONCLUSION

Despite extensive research in the field of IT governance, considerable work is needed to further the understanding of IT governance, and to develop a successful holistic measure of IT governance. To enable IT governance to become an accepted part of organisational strategic and operational governance processes, it is important that researchers develop more practical methods for organisations to use in establishing and assessing IT governance (Johannsen et al., 2007; Lee and Lee, 2009). It is thus necessary to clarify the concept of IT governance through systematically classifying and drawing together various definitions so far offered. The conduct of future research addressing the issues raised in the prior sections should lead to improved IT governance within each GRC area and the establishment of holistic frameworks of IT governance. A number of researchers including van Grembergen (2004) and Peterson (2003) have attempted to develop holistic IT governance frameworks but there is still much room for improvement in fusing IT governance into one process. New work could then specify its theoretical framework and begin to offer operative guidelines to hospital practitioners, for example, through suggesting some of the practical implications of different IT governance designs. To

make sure that the corporate hospital strategy leads to adequate business decisions a Healthcare IT Governance Framework will be needed. This framework can help to minimise risks and should consider the special requirements of the healthcare sector.

REFERENCES

[1] Addy, Rob, ed. *Effective IT Service Management: To ITIL and Beyond!* Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2007. http://dx.doi.org/10.1007/978-3-540-73198-6 / http://www.dandelon.com/intelligentSEARCH.nsf/alldocs/3274F6B5C35858C1C12572DC001A3305/.

[2] Ahern, D. M., A. Clouse, and R. Turner, eds. *CMMI distilled: A practical introduction to integrated process improvement*. Bosten: Addison Wesley, 2004.

[3] Betz, Charles T. *Architecture and patterns for IT service management, resource planning, and governance: Making shoes for the cobbler's children*. Amsterdam: Morgan Kaufmann/Elsevier, 2007. http://www.gbv.de/dms/hbz/toc/ht014953145.pdf.

[4] Calder, Alan, ed. *It Governance: Guidelines for Directors*: IT Governance Publishing, 2005.

[5] Cilli, C., ed. *IT governance: Why a guideline?* Information Systems Control Journal, vol. 3, p. 22-24, 2003. http://www.itgi.org/Template.cfm?Section=Home&CONTENTID=35752&TEMPLATE=/ContentManagement/ContentDisplay.cfm, accessed May 2010.

[6] Conwell, C. L., R. Enright, and M. A. Stutzman, eds. *Capability maturity models support of modeling and simulation verification, validation, and accreditation: Winter Simulation Conference 2000*. San Diego, USA, 2000.

[7] Fettke, Peter, Loos, Peter, and Zwicker, Jörg. "Business Process Reference Models: Survey and Classification." In *Workshop on Business Process Reference Models,* edited by Christoph Bussler and Armin Haller. Nancy, France, 2005.

[8] Goeken, Matthias, and Stefanie Alter, eds. *IT Governance Frameworks as Methods: Proceedings of the 10th International Conference on Enterprise Information Systems, ICEIS 2008, 12 - 16, June*. Barcelona, Spain, 2008.

[9] Gottschalk, Peter, ed. *E-business strategy, sourcing, and governance*. Hershey PA: Idea Group Pub., 2006.

[10] Guldentops, Erik, Gary Hardy, Jimmy Gary Heschl, and Sharon Taylor, eds. *Aligning Cobit, ITIL and ISO 17799 for Business Benefit: A Management Briefing from ITGI und OGC*. www.itil.co.uk/includes/ITIL-COBiT.pdf, accessed May 2010.

[11] Hakes, C., ed. *The corporate self assessment handbook*. London: Chapman and Hall, 1996.

[12] Heier, Hauke, Hans P. Borgman, and Mervyn G. Maistry, eds. *Examining the relationship between IT governance software and business value of IT: Evidence from four case studies: Proceedings of the 40th Hawaii International Conference on System Sciences*. Hawaii, 2007.

[13] ISACA Switzerland Chapter, ed. *CoP, Cobit, Marion, IT-Grundschutzhandbuch: vier Methoden im Vergleich,* 1998. http://www.isaca.ch/files/DO6_Arbeitsgruppen/igcop_broschuere.pdf.

[14] Johannsen, Wolfgang, Goeken, Matthias, Just, Daniel, and Tami, Farsin. *Referenzmodelle für IT-Governance: Strategische Effektivität und Effizienz mit COBIT, ITIL & Co*. 1st ed. Heidelberg: dpunkt-Verl., 2007. http://deposit.d-nb.de/cgi-bin/dokserv?id=2838359&prov=M&dok_var=1&dok_ext=htm.

[15] Johnstone, D., S. L. Huff, and B. Hope, eds. *IT projects: Conclict, governanace and systems thinking*. Proceeding on the 39th Hawaii International Conference on System Sciences, 2006.

[16] Jordan, Ernie, and Silcock, Luke. *Beating IT risks*. Chichester: J. Wiley, 2005. http://www.gbv.de/dms/hbz/toc/ht014249257.pdf.

[17] Keyes-Pearce, Susan. "Rethinking the Importance of IT Governance in the e-World." In *Proceedings of the 6th Pacific Asia Conference on Information Systems PACIS-2002*. Tokyo, 2002.

[18] Krey, Mike, Bettina Harriehausen, Matthias Knoll, and Steven Furnell, eds. *IT Governance and its spread in Swiss Hospitals: Proceedings of the IADIS International Conference e-Health 2010*. Freiburg, 2010.

[19] Lahti, Christian, and Roderick Peterson, eds. *Sarbanes-Oxley Compliance Using COBIT and Open Source Tools*: Syngress, 2005.

[20] Lee, Junghoon, and Lee, Changjin. "IT Governance - Based IT strategy and Management: Literature Review and Future Reserach Directrions." In *Information technology governance and service management: Frameworks and adaptations,* edited by Aileen Cater-Steel. Hershey: Information Science Reference [u.a.], 2009.

[21] Menzies, Christof, ed. *Sarbanes-Oxley und Corporate Compliance: Nachhaltigkeit, Optimierung, Integration*. Stuttgart: Schäffer-Poeschel, 2006. http://deposit.ddb.de/cgi-bin/dokserv?id=2749173&prov=M&dok_var=1&dok_ext=htm / http://www.gbv.de/dms/bsz/toc/bsz250745674inh.pdf.

[22] Office of Government Commerce, ed. *Service delivery: ITIL The key to managing IT services*. 9th ed. London: TSO (The Stationery Office), 2005.

[23] Peterson, Ryan R., ed. *Exploring the impact of electronic business readiness on leadership capabilities in information technology governance: In Proceedings of the 35th Hawaii International Conference on System Sciences,* 2003.

[24] Schmidt, Andreas, ed. *State of the Art des IT-Service Managements*. GRIN Verlag, 2007.

[25] Sohal, A. S., and P. Fitzpatrick, eds. *IT governance and management in large Australian organizations.,* 2002.

[26] Spafford, George, ed. *The Benefits of Standard IT Governance Frameworks,* 2003. http://www.itmanagementonline.com/Resources/Articles/The_Benefits_of_Standard_IT_Governance_Frameworks.pdf, accessed June 2010.

[27] Standards Australia, ed. *AS 8015-2005: Corporate governance of information and communication technology,* 2005. http://standards.com.au, accessed May 2010.

[28] van Grembergen, Wim, ed. *Introduction to the minitrack: IT governanace ants its mechnisms: Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS),* 2002.

[29] van Grembergen, Wim, ed. *Strategies for information technology governance*. Hershey, Pa., London: Idea Group Publishing, 2004. http://www.gbv.de/dms/hbz/toc/ht013914680.pdf.

[30] van Grembergen, Wim, and de Haes, Steven. *Implementing information technology governance: Models, practices, and cases*. Hershey, Pa.: IGI Publ., 2008. http://www.gbv.de/dms/hbz/toc/ht015362476.pdf.

[31] Walter, S., and H. Krcmar, eds. *Reorganisation der IT-Prozesse auf Basis von Referenzmodellen: Eine kritische Analyse*. it-Service-Management, Heft 2, 2006.

[32] Weill, Peter, and Jeanne W. Ross, eds. *IT governance: How top performers manage IT decision rights for superior results*. Boston, Mass.: Harvard Business School Press, 2007. http://www.gbv.de/dms/bowker/toc/9781591392538.pdf.