Understanding the Enabling Design of IT Risk Management Processes

Completed Research Paper

Manuel Wiesche
Technische Universität München
Chair for Information Systems
Boltzmannstr. 3, D 85748 Garching
Germany
wiesche@in.tum.de

Michael Schermann
Technische Universität München
Chair for Information Systems
Boltzmannstr. 3, D 85748 Garching
Germany
michael.schermann@in.tum.de

Helmut Krcmar
Technische Universität München
Chair for Information Systems
Boltzmannstr. 3, D 85748 Garching
Germany
krcmar@in.tum.de

Abstract

Although managing information technology (IT) risks is widely regarded as a critical in organizations, stakeholders often question the value provided by IT risk management (IT-RM) to an organization. Organizational research suggests the concept of 'enabling formalization' to design highly formalized organizational processes. Processes like IT-RM that are designed in an enabling way support organizational members through flexible guidelines that communicate best practices and empower them in resolving surprises and crises during process execution. It remains unclear, however, how organizations can implement enabling IT-RM processes. We conduct an exploratory study and identify four design decisions for IT-RM. We identify different solutions to these IT-RM design decisions and provide empirical evidence as to how these solutions facilitate enabling process design. Our results suggest that organizations need to balance rewarding and punishment-centered strategies in designing IT-RM to change it from an ineffective, costly, and detrimental endeavor into an enabling organizational process.

Keywords: IT risk management, design decisions, enabling, grounded theory techniques

Introduction

Managing information technology (IT) risks has become a critical part of regulations, standards, best practices, and consistently ranges among the top five issues of CIOs (Deloitte 2010). IT risks in an organization are heterogeneous and include technical incidents as well as human resource issues in software development projects (Schmidt et al. 2001), loss of control in outsourcing relationships (Aron et al. 2005), security concerns such as data loss (Straub and Welke 1998), electronic sales strategies (Dewan and Ren 2007), cloud computing strategies (Carr 2005), and mobile strategies (Wheeler et al. 2013). Thus, IT risks are characterized by heterogeneity and fragmentation and cover all organizational levels from operations to senior management (Alter and Sherer 2004; Dhillon and Backhouse 1996; Markus 2000; Sherer and Alter 2004; Wiesche et al. 2013a).

In order to cope with these challenges, researchers and practitioners suggest and develop formal IT risk management (IT-RM) processes covering all IT-related topics (COSO 2004; Purdy 2010; Rainer et al. 1991; Schermann et al. 2014). These processes comprise procedures, techniques, stakeholders, roles and decision-making hierarchies to manage IT risks on all levels within an organization (Gemmer 1997; Smith and McKeen 2009).

The involvement of organizational members and management are essential in IT-RM processes. Organizational members identify potential IT risks, assess exposure, conduct countermeasures, and support in reporting IT risks. Management provides a budget for countermeasures and uses IT-RM information for decision making. In practice, employees often shy away from the high expenditures of collecting and processing IT risk information (Boss et al. 2009; Chen et al. 2012) and managers rarely use recommendations of IT-RM in their decision making (Teneyuca 2001).

Current models for IT-RM process design follow a coercive strategy that does not encourage the participation of employees or managers. Based on deterrence theory from criminology, some literature suggests imposing formalized work procedures on employees and introducing punishment for non-compliance (D'Arcy and Herath 2011; Straub Jr and Nance 1990). Consequently, organizational members follow procedures only if they believe management is monitoring their activities (Boss et al. 2009). Otherwise, they use various reasons to justify non-compliance and even engage in workarounds or pretend to comply (Alter 2014; Gouldner 1954; Röder et al. 2014; Siponen and Vance 2010).

Organizational research suggests the concept of *enabling process design* to design highly formalized organizational processes requiring both routinization and creativity (Adler and Borys 1996). IT-RM processes rely on the initiative and judgement of both the operational business and the IT employee and requires their knowledge and creativity for identifying IT risks and assessing the exposure to these risks (Smith and McKeen 2009). As most IT risks occur seldom, differ in their characteristics and need individual assessment, IT-RM processes require flexible guidelines that communicate best practices and empower employees to resolve surprises and crises during process execution (Adler and Borys 1996). Thus, enabling formalization allows organizations to ensure both compliance and continuous improvement in IT-RM processes and motivates the participation of employees as well as managers.

We therefore seek to understand how organizations implement enabling IT-RM processes. We conduct an exploratory study to identify and analyze organizational solutions that foster enabling IT-RM processes. The question guiding this research is: *Which design choices exist in establishing IT-RM?* We answer this research question by applying grounded theory techniques on 31 interviews conducted in three organizations (Strauss and Corbin 1990). We identified four design decisions for IT-RM that are associated with enabling IT-RM process design and provide empirical evidence for these solutions. We contrast our findings with the literature and find two underlying strategies for IT-RM design. Our results suggest that organizations need to find a balance between rewarding and punishment-centered strategies in designing enabling IT-RM.

Related Research

IT risks have been the subject of information systems research from various perspectives (see, for example, Alter and Sherer 2004; Dhillon and Backhouse 1996; Markus 2000; Sherer and Alter 2004). Markus (2000) differentiates between the systems development and the operational perspective on IT risks and used Microsoft's IT risk categories to illustrate the breadth and variety of financial, project, political and functionality IT risks. Alter and Sherer (Alter and Sherer 2004; Sherer and Alter 2004) use a work systems perspective to illustrate overlaps in these categories. They structure IT risks using the following work systems elements: work practices, participants, information, technologies, product and services, customers, environment, infrastructure and strategies. This structure, however, does not cover all organizational requirements. Because software development projects comprise technical,

social and management elements (Schmidt et al. 2001), IT risk managers who use this classification would be challenged when processing different IT risks. IT risks are heterogeneous, inhibiting IT risk managers to compare and aggregate exposures of different types of IT risks (Wiesche et al. 2013a). The width and variety of IT risks highlight the challenge in developing an integrated IT-RM process that analyzes, mitigates and reports on all these different IT risks (Schermann et al. 2014).

An organization with silos for different IT risks may improve daily operations, but will lack guidance on the formal steps of managing IT risks across functions and IT risk information cannot be used by executives for decision making (Alter and Sherer 2004). An integrated approach to manage IT risks would involve executives in operational IT issues and improve decision making (Markus 2000; Sherer 2004). Similarly on an operational level, scattered IT-RM efforts cause duplicate work and miss methodological expertise on managing the risks (Dhillon and Backhouse 1996; Dhillon and Backhouse 2001). An integrated IT-RM process supports organizational members in exploiting synergies and providing the methodological support needed to adequately govern and use IT resources to achieve the organizational goals (Alter and Ginzberg 1978; Sharma and Dhillon 2009; Straub and Welke 1998; Westerman 2007).

The IT Risk Management Process

The unit of analysis in this research is the IT-RM process. We define IT-RM processes as collections of formal procedures, techniques, stakeholders, roles and decision-making hierarchies within the organization (Rainer et al. 1991; Schermann et al. 2014; Sharma and Dhillon 2009; Smith et al. 2001). The IT-RM process is a systematic, structured and reoccurring process capable of handling information on uncertainties in outcomes of technological, human and sociological aspects of information technology and thereby informs decision-making (Alter and Sherer 2004; Benaroch et al. 2006; Hahn et al. 2009; Nicolaou and McKnight 2006; Straub and Welke 1998). Literature targeted to practitioners provides guidance on designing IT-RM processes (Gemmer 1997; Marinos et al. 2009) and international standards such as ISO 31000 (Purdy 2010), ISACA's COBiT (ITGI 2005) and COSO (2004) suggest formal processes for IT-RM. Similarly, national recommendations, such as the CCTA Risk Analysis and Management Method in the UK (1993) or the German IT Basic Security Handbook (Ekelhart et al. 2007), define categories and structures for IT risk assessment.

Commonly, the IT-RM process is structured in phases, whereby each phase comprises a set of procedures and techniques to address distinct functions in the process (Schermann et al. 2014). We differentiate four cyclical phases of the IT-RM process: the purpose of the IT risk identification phase (1) is to identify potential IT risks that may harm the organization. The IT risk assessment phase (2) collects all relevant information to assess the identified IT risk. IT risk mitigation (3) comprises the compilation of alternative IT risk mitigation measures, decision-making and implementations of selected IT risk mitigation measures. IT risk reporting (4) collects, aggregates and reports IT risk information to stakeholders. Literature presents a variety of IT-RM processes that differ in the level of granularity (COSO 2004; ITGI 2005; Purdy 2010; Rainer et al. 1991; Straub and Welke 1998). These differences in granularity can be traced back to the four phases described above.

Stakeholders from different departments and organizational levels are involved in the IT-RM process: IT risk managers, IT department employees, other employees and managers. IT risk managers are accountable for establishing a formal IT-RM process within the organization. They do so by providing methodological guidance and judging the quality of the IT risk assessment conducted by employees (Hall et al. 2015; Mikes 2014). IT department employees identify and support the assessment of IT risks in their day-to-day work. Other employees support IT-RM in assessing the business impact of IT risks. Managers embed the IT-RM process within the business processes and are the target audience of the information gathered during the IT-RM process (Spears and Barki 2010). IT risk managers are in charge of ensuring participation of employees in the IT-RM process (Hall et al. 2015).

Getting all stakeholders involved in the IT-RM process is the key challenge facing IT risk managers (Wiesche et al. 2013b). From the employees' perspective, information generated in the IT-RM process is not used for decision making by executives (Teneyuca 2001). Further, IT risks are hard to aggregate and compare on cross-departmental issues during the IT-RM process (Iversen et al. 2004). From a managerial perspective, employees are often viewed as ignoring security principles and guidelines (Boss et al. 2009). Thus, management cannot completely rely on the information provided by IT-RM (Ciborra 2006; Wiesche et al. 2013b).

Despite likely opposition, employees and management need to participate in IT-RM processes. IT employees have knowledge of the existing systems and the transformation processes and thereby can identify IT risks (Sharma and Dhillon 2009; Spears and Barki 2010). Business employees know the impact of ill-functioning information systems and can assess the impact of IT risks. Management has

to support IT risk managers when ensuring employee participation. Furthermore, managers, as recipients of IT-RM information, define thresholds and decide on mitigation mechanisms such as budgets for IT risk reduction. IT risk managers cannot conduct IT-RM without these stakeholders as they require the technical knowledge of IT employees, the impact knowledge of business employees, and the financial support of management (Rainer et al. 1991; Smith et al. 2001) to act accordingly.

Enforcing compliance and punishment as forms of deterrence have been found to ensure participation in IT processes. Deterrence theory is frequently applied and suggests that sanctions increase IT security compliance (D'Arcy and Herath 2011). This theory assumes that potential rule-violators will reduce their non-compliant behavior when organizations control undesired behavior. Factors such as severity of punishment and certainty of control were found to affect process compliance (Chen et al. 2012). Computer abuse, for example, can be reduced with detection and punishment mechanisms such as providing information on acceptable system usage, disseminating statements on penalties, developing abuse awareness programs and monitoring computer activities (Straub Jr and Nance 1990).

The effectiveness of various deterrence strategies to ensure participation in IT processes has been studied but results are inconclusive. Anxiety, withdrawal, workarounds or pretending to comply have been identified as negative side-effects of deterrence strategies (Alter 2014; Chen et al. 2012; Gouldner 1954; Röder et al. 2014). Other authors found perceived justice of punishment to overshadow the punishment expectancy of IT non-compliance (Xue et al. 2011). According to neutralization theory from criminology, employees use neutralization to justify non-compliant behavior (Siponen and Vance 2010). They deny responsibility, consequences and necessity of the rule to justify their non-compliance. Hence, organizational members comply with policies if they believe their activities are being monitored by management (Boss et al. 2009).

Two Design Strategies for Organizational Processes: Coercive and Enabling

Formal processes can have either a positive or negative impact on the participatory behavior of employees depending on "whether the formalization enables employees to better master their tasks or functions as a means by which management attempts to coerce employees' effort and compliance" (Adler and Borys 1996). Following the previously described deterrence approach, IT-RM processes are formulated as mandatory, flat assertions of duties that do not provide employees with the rational for work procedures and do not give them freedom to adapt the processes for their individual situation (Gouldner 1954). This type of process design – referred to as coercive – does not support organizational members in performing their job nor does it explain the need to participate in organizational processes (Adler and Borys 1996). Thus, organizational members are not motivated to participate in IT-RM processes and only participate when they are forced to do so (Boss et al. 2009).

Table 1. Characteristics of Coercive and Enabling Process Design		
Criterion	**Coercive**	**Enabling**
Repair	Highlight compliance	Facilitate responses to process contingencies
Internal transparency	Flat assertion of duties	Visibility into the process
Global transparency	Asymmetrical intelligibility	Provide understanding of overall process
Flexibility	Specific sequence of steps	Learning opportunities

Table 1. Characteristics of Coercive and Enabling Process Design

By contrast, enabling processes enable employees to get their work done and encourage improvement and collaboration (Adler and Borys 1996; Heumann et al. 2014). Adler and Borys suggest four generic design principles for coercive and enabling processes (Table 1): repair, internal transparency, global transparency and flexibility. Repair refers to situations in which established processes break down and the strategies required to re-establish them. Internal transparency is about understanding local processes. Global transparency is the intelligibility of employees for the overall value creating process of the organization. Flexibility refers to employee's discretion over the process (Chapman and Kihn 2009).

Enabling formalization incorporates employee's knowledge and experience and integrates these into process design. Enabling processes are flexible guidelines that communicate best practices and empower employees to resolve surprises and crises during process execution (Adler and Borys 1996). Enabling formalization constitutes a shared understanding of process and is legitimized by both management and employee: the process is enforced by management and employee and buttresses informal sentiments, initiation and education of employees and management (Gouldner 1954). Enabling formalization increases comprehension, rapid response, precision and consistency of organizational processes (Zuboff 1988). Breakdowns and repair signals in enabling formalization highlight process shortcomings and opportunities for improvement (repair criterion). Enabling formalization enhances the employee's understanding of the process by outlining critical components and sharing best practices (internal transparency criterion). The contextual information provided to the employee aids his insight into the overall process (global transparency criterion). Enabling formalization treats deviations from defined processes not only as risks, but also as learning opportunities (flexibility criterion).

Potentials of Enabling IT Risk Management Processes

The use of a coercive process design for IT-RM processes does not necessarily motivate organizational members' participation in managing IT risks. Managers cannot assess the outcome quality of the IT-RM process due to several reasons and cannot design processes that capture all potential process alternatives for managing IT risks. According to control theory, the use of formal control mechanisms requires the ability to assess quality and knowledge outcomes of the transformation process (Ouchi 1979; Wiesche et al. 2012). IT risks occur only rarely, differ in their characteristics, and impact cannot be assessed in monetary values (Ciborra 2006; Markus 2000; Sherer and Alter 2004; Wiesche et al. 2013a). Thus, IT risk assessment quality and reporting completeness cannot be judged by IT risk managers and management. Similarly, the process of managing IT risks is individually tailored to the heterogeneous business processes where the information system is implemented and thus requires detailed IT and process knowledge which IT risk managers and management do not have (Coles and Moulton 2003; Dhillon and Backhouse 1996; Mikes 2014).

IT-RM processes would benefit from an enabling process design in several ways. Enabling IT-RM makes organizational members accountable for adapting and extending the IT-RM process, especially during the risk identification phase, thus facilitating coping with the dynamic structures when using IT (Dhillon and Backhouse 2001). Organizational members can use IT-RM to communicate ideas for improvement and delegate accountability for uncertainty and risks in their IT processes (Coles and Moulton 2003; Schermann et al. 2012). Development of sophisticated IT risk mitigation strategies requires employees to be creative and to freely voice opinions (Adler and Borys 1996; Schermann et al. 2014; Weinstein 2004). For IT-RM, it is essential to use the employee's knowledge and creativity in identifying potential risks to the organization and assessing exposure to these risks (Aron et al. 2005; Rainer et al. 1991; Smith et al. 2001; Tiwana and Keil 2004; Wiesche et al. 2013b).

Thus, enabling formalization allows organizations to ensure both compliance and continuous improvement in IT-RM process design. To the best of our knowledge, how organizations implement enabling IT-RM processes has not yet been examined. Therefore, we conduct an exploratory study to identify, structure, and understand organizational practices that foster enabling IT-RM processes.

Research Method

Research Strategy

We followed an exploratory research strategy and applied grounded theory techniques to analyze the data we collected in three organizations (Strauss and Corbin 1990). We interviewed 31 practitioners at Alpha, Beta, and Gamma who were either responsible for IT-RM processes or participated in these processes and could therefore provide thorough insights on the perception of IT-RM at their organization. We consider this inductive approach appropriate to answer our research question as the continuous interplay between data, analysis, and literature helped to elaborate on the underlying design decisions of particular IT-RM solutions. From our analysis of the literature, we know that IT-RM would benefit from enabling formalization but the literature does not provide an understanding of how to foster enabling IT-RM process. Our inductive approach enabled us to understand the type of formalization of particular solutions to design decisions. We followed the methodological guidance of Strauss and Corbin (1990) and Urquhart (2012) for conducting our research.

Sample

The imperative of our sampling was to avoid "research that adheres too closely to a single substantive area and, instead, draws from the several substantive areas that are frequently reflected in a given daily reality" (Suddaby 2006). For our study, we selected three industries with a long history of actively engaging in managing IT risks and for whom IT-RM is a long-standing and ongoing challenge. (1) Transportation: IT risks center on issues of organizing supply chains, information visibility and privacy. (2) Retail: automation, product data management and retail networks induce IT risks. (3) Banking: long-standing IT risks result from regulatory compliance, financial fraud and outsourcing. We conducted initial interviews with IT risk managers from organizations in these three industries and participated in practitioner-oriented workshops with potential participants. We were looking for organizations in our focal industries that invested substantial effort into IT-RM. We identified three organizations, Alpha, Beta, and Gamma.

Alpha is a large transportation company with several strategic business units (SBU). It provides infrastructure, transportation and logistics services. Alpha first implemented an IT-RM process 14 years ago and spent extensive efforts in establishing a group-wide IT risk department with a high formalized process.

Beta sells their products in Europe, the Americas and Asia. Because of its high variety of products and services, the organization is divided into several SBUs each of which has its own IT-department. Beta has a central IT department to control and support the SBUs and deliver standard IT services. Most operational IT services are outsourced to external IT service providers. Beta does not have to comply with IT risk management regulations, but started implementing an IT-RM process 10 years ago. Over time, Beta has made an effort to comply with IT risk management regulations by starting IT-RM projects and hiring external consultants. For instance, when focusing on security management, Beta started implementing a process following the ISO 27000 norm. While the established process was not accepted within the organization, the SBUs started pragmatic IT-RM approaches and ad-hoc solutions for IT-RM.

After interviewing practitioners from Alpha and Beta, we developed an initial understanding of the IT-RM process, but questioned theoretical saturation (Urquhart 2012). In particular, we were concerned with the many different solutions to IT-RM design decisions at Alpha and Beta. Therefore, we specifically looked for an organization with the potential to contrast our initial understanding of the IT-RM process. This lead us to Gamma where we conducted a second cycle of interviews to substantiate our initial theoretical saturation. We could not find any evidence of endogeneity.

Gamma is a medium-sized European IT service provider for the banking industry and provides banking applications, IT services, IT infrastructure and IT training for several hundred customers. Gamma has several SBUs and one central IT-RM department which focuses on collecting IT risk information and preparing and distributing this information to the relevant stakeholders. The IT-RM department interacts with IT risk managers in each of Gamma's departments. These department IT risk managers are responsible for all IT risks in their department and for supporting the employees in conducting IT-RM. Gamma started implementing an IT-RM process 12 years ago when German law first required formal IT-RM.

Data Collection

Our data set comprises 31 semi-structured interviews with 10 practitioners from Alpha, 15 from Beta, and 6 from Gamma.[1] The interviewees were iteratively chosen based on their role within the organization. In all three organizations, we interviewed the CIO, employees who were in charge of IT-RM processes and IT employees who had been involved in the IT-RM process several times. At Alpha, we interviewed two business experts who were in charge of providing IT-RM budget. At Beta and Gamma we interviewed external consultants who supported the IT-RM during risk identification and assessment. We asked questions on the IT-RM process, its strengths, weaknesses, challenges, typical IT risks and perceptions of the process itself. Our analysis of an interview served as the basis for our questions in future interviews. We recorded, transcribed, and pseudonymized all interviews. Due to confidentiality reasons, we were not allowed to record four interviews (three at Alpha, one at Gamma) so we took notes during the interview instead. However, in all interviews we observed that interview partners told us insightful aspects of their work "off the record" and we included these insights in our

[1] As all interviews were held in German, we translated quotes and codes for this publication into English.

notes. We integrated the resulting data set of 236,844 words (514 pages of text) with approximately 600 pages of archival information into a hermeneutic unit using the software AtlasTi.

Data Analysis

We applied grounded theory techniques for coding our data (Strauss and Corbin 1990; Urquhart 2012) and used previous work on the IT-RM process and formalization to support our reflection of the data and guide data analysis (Adler and Borys 1996; Gouldner 1954; Rainer et al. 1991). We followed Strauss and Corbin's (1990) guidelines for coding the data. That is, the first author read and coded the interview transcripts line-by-line using phrases from the transcripts that describe the phenomenon (open coding) and tagging similar phenomena with the same phrase. Following this step, the second author likewise coded the transcripts independently. All three authors discussed and agreed on the differing codes. The final list included 172 open codes.

We conducted axial coding to link the identified concepts and categories on enabling IT-RM to each other and explored specific subcategories among these. We coded for causal conditions, intervening conditions and contextual conditions, as well as actions and consequences (Strauss and Corbin 1990). This procedure took place in a cyclical manner; each cycle of interpretation guided our search for the next interview partner. We thereby gained a better understanding of design decisions in IT-RM including its antecedents and its perception.[2]

Axial coding identified four key categories of the core phenomenon (Table 3). We applied selective coding in order to move beyond description toward conceptualization. We therefore limited further coding to concepts related to the emerged categories and constantly compared instances of data within the same category (Urquhart 2012). Literature on formalization (Adler and Borys 1996; Gouldner 1954) supported our analysis efforts, allowed us to substantiate our preliminary theoretical understanding using the most recently collected data and then apply the types of formalization in an effort to understand how specific solutions to design decisions were perceived.

Results

In this section, we present the four design decisions for IT-RM: retaining participation, accountability, role, and reporting (see Table 3). We understand design decisions as situations occurring during the design of the IT-RM process where organizations can choose between different options. These options – or process alternatives – include one or more steps that transform some kind of input into an output. Design decisions in the IT-RM process are characterized by mutually exclusive solutions. These solutions may address different process goals (e. g., compliance vs. decision making) and thus different reasons for each option exist. The solutions have different effects on IT-RM process design. As for this research, in which we are particularly interested in the enabling design of IT-RM, we focus on the enabling type of formalization. We identify solutions that are associated with enabling formalization and provide empirical evidence as to how these solutions facilitate enabling process design (Table 2). In the following, we explain the four design decisions whereby we outline the situation within the IT-RM process and provide an overview of alternative solutions. We first outline coercive solutions which are then contrasted with solutions that are perceived as enabling.

Design Decision 1: Retaining IT-RM

Our study reveals that a central challenge in IT-RM is to ensure that the process is conducted on an ongoing basis. While interviewees reported on implementing ad hoc measures as straightforward, all interviewees reported on different solutions to ensure that IT-RM is treated as an ongoing concern. Alpha uses formal reporting cycles, schedules and deadlines to ensure ongoing participation in IT-RM. IT risk managers can deny the approval of new applications based on the completeness and quality of the IT risk assessment of this application. Every application has an IT risk expiration date and is taken off the system when the IT risk assessment (among other criteria) is not renewed. This compliance strategy allows continuity in reporting and thereby completeness of formal reporting. Management and IT risk managers are capable of acting immediately for exception reporting or in the case of incidents.

[2] Due to space restrictions, example quotes from our data and documents with the corresponding open and axial codes as well as data on the emerging themes from selective coding, are available through the first author upon request.

This compliance strategy is perceived as coercive formalization by organizational members. Employees do not see the benefits of the process and thus question the necessity of conducting IT-RM. As a result, employees do not concentrate on identifying or assessing new risks or mitigating existing ones. Rather, they comply with the tasks specified by management requiring the least effort. Hence, completeness and quality of the risk assessments are reduced. The example of one SBU at Alpha illustrates this perception:

> *„This is seen as cumbersome, an additional burden. We see it as a God-given sanction. […] The process […] forces you to think about things. If it wouldn't be mandatory on a regular basis, I would probably do it later … or never. But since they force you, you often just comply and do what you are asked." (Alpha SBU manager)*

Table 2: The Four IT-RM Design Decisions Identified in this Research

Design Decision	Definition
Retaining IT-RM	The design decision regarding retaining IT-RM occurs when organizations seek to ensure that organizational members in business and IT participate in IT-RM on an ongoing basis (Table 4). Organizations can choose a process-enforcing atmosphere that results in highly documented IT risks, or choose a motivational atmosphere that results in creative identification and motivated assessments
Accountability for IT risk mitigation	The design decision regarding the accountability for risk mitigation occurs when the department held accountable for the identified IT risk is identified (Table 5). Organizations can choose between an effect-oriented strategy that results in top-down decisions on mitigation or choose a cause-oriented strategy that ensures consensus and expertise for mitigation
Role of the IT risk manager	The design decision regarding the role of the IT risk manager occurs whenever organizations define the duties and competencies of the IT risk managers (Table 6). Organizations can either focus on enforcing compliance, which ensures proper reporting, or balance compliance and support for organizational members which results in high quality IT risk information
IT-RM reporting	The design decision regarding the IT-RM reporting occurs when organizational members report on IT risk (Table 7). Organizations choose between standardized IT risk reporting, which ensures comparability of IT risks, and individual IT risk reporting which fosters participation

Table 2. The Four IT-RM Design Decisions Identified in this Research

By contrast, Gamma ensures that employees understand the benefits of meeting formal reporting deadlines and contributing to risk assessments. Senior management appreciates the efforts of conducting IT-RM. The IT risk report is integrated in executive information sources and informs decision making. Senior management reviews this report with IT risk managers and discusses measures and reassessments of IT risks that have not been properly addressed. Then, senior management discusses the content of the risk report with their employees. As a result, employees sense that their concerns are taken seriously and that they play a role in improving daily operations. In this way, IT-RM provides learning opportunities for IT process design and creates flexibility within the process.

Table 3. Solutions used by Study Cases to Ensure Retaining IT-RM Design Decision

The strategy used by Gamma is also motivational and can be perceived as enabling formalization (Table 3). This motivational strategy does not only convince employees to report IT risks in order to get top management support for mitigation, but also motivates employees to use external information resources to stay informed of potential new risks:

> *„My team members […] browse through corresponding sources of information. Back in the days, we defined a handful [of sources]: I remember heise.de [one of the most successful German speaking IT news portals], cnet.com and various others. Some are specific to banking, while others are not. Whenever something important happened that could affect us, a colleague distributed the details in our knowledge management system and had someone else document it in our incident data base." (Gamma SBU IT risk manager I)*

Table 3. Solutions used by Study Cases to Ensure Retaining IT-RM Design Decision			
Observed Solution	**Case**	**Criterion**	**Enabling effect**
IT risk information is integrated into organizational decision making	Gamma	Flexibility	IT risk information provides learning opportunities for IT process design
Senior management communicates IT risk management strategy including focus topics on a biannual basis	Beta	Repair	Encourages employees to identify risks and propose solutions regarding certain topics
Global incident data base for IT incidents that occurred in the past	Gamma	Global transparency	The global incident data base informs employees of potential consequences, provides best practices within the process and fosters interaction
Decentral IT risk management roles in departments are re-staffed every two years	Beta	Flexibility	Through re-staffing the decentral IT risk manager every two years, Beta provides a new perspective on IT risks, including individual process adaptions, new templates and foci

Design Decision 2: Accountability for IT Risk Mitigation

In the mitigation phase of the IT-RM process, the department held accountable for the detected IT risk must be identified. Being accountable for an IT risk involves managing the formal process, i. e., providing the relevant information and conducting a formal sign-off process. Costs for mitigation efforts are usually covered by the cost center of the affected department. At Beta, SBUs negotiated for several months for funding a backup network connection between the two main buildings where the SBUs are located. The situation was similar at Alpha:

> *"As security consultant, the different functional units assign assessments for certain IT risks to me. I usually draft the assessment and moderate the discussion. This discussion includes myself, the risk manager, the functional unit – or if there are more than one involved all of them – the person in charge of the application and whomever else is involved. I try to suggest certain probabilities and impacts for this risk. Especially the latter enforces a discussion: 'who is affected, who caused this, how could this have been prevented, and so on'. I see myself as a detective here: understanding the real impact within this highly subjective discussion. At the end, I only suggest a solution [...] the most affected department will sign the risk declaration and ultimately pay." (Alpha security consultant II)*

Departments affected by a certain risk provide the resources for mitigation. For instance, at Gamma, the employee who identifies a risk for their application is responsible for its further reporting and mitigation. At Beta, the degree of benefit from the IT risk mitigation project determines the selection of the cost center responsible for providing the necessary financial backing. This results in a distinct allocation of budget: there is no negotiation and only important IT risks are identified. In the case of Beta, the affected unit can often be determined easily which means easy identification of the department responsible to provide the budget for mitigation.

This effect-oriented strategy for assigning responsibility to IT risks is perceived as coercive formalization. Employees will be swamped with mitigation efforts and important IT risks will be ignored. While those employees affected by the IT risks are held responsible for mitigation, as in the Beta example, these employees may not have the technical expertise to resolve the issue. The pressure of assuming responsibility for IT risks occurring in the employees' functional area may lead to a culture of deterrence.

However, the contrary is true: following a cause-oriented approach involves assigning responsibilities to the unit that caused the IT risk. Formal negotiation is required to identify the unit causing the IT risk and thus responsible for mitigation. In the case of Alpha, each IT risk is assigned to an application and since Alpha follows a cause-oriented strategy there is always a distinct risk owner. Because assignment to an IT risk involves certain duties and responsibilities, extensive discussions take place to decide who caused the IT risk:

> *„And we have to discuss all these issues over and over again. And at the end, somebody says 'okay, I will bear this risk. But should you put something different in there and I find out that you are hiding something that we did not talk about, I won't bear [the responsibility for the risk].' We always negotiate quite a while and there are many political decisions involved. […] It becomes more like horse-trading." (Alpha SBU IT risk manager II)*

Assigning accountability to the function causing the IT risk ensures enabling IT-RM by facilitating responses to the occurring IT risks. As all involved stakeholders conduct an analysis of the cause of the IT risk, the department ultimately identified agrees to mitigate the risk. This assumption of responsibility further guarantees that the most competent employees are involved to deal with the system, process or technology where the risk occurs. Table 4 illustrates further solutions to this IT-RM design decision that are perceived as enabling.

Table 4. Solutions used by Study Cases to Ensure Accountability IT-RM Design Decision

Observed Solution	Case	Criterion	Enabling-effect
During IT risk assessment, a workshop is conducted where all stakeholders, e. g., IT risk manager, business staff, IT staff and consultants develop risk scenarios and identify proper mitigation measures	Alpha, Gamma	Global transparency	The workshop character enforces collaboration and negotiation between involved parties. The moderating role is conducted by the security consultant and thus enables an ongoing discussion
IT risk assessment workshops focus on identifying the cause of IT risk. The risk-causing department will be in charge of mitigating this particular risk	Alpha	Repair	The involved parties conduct an analysis of the cause of the IT risk. This encourages the department causing the risk to respond and elaborate on a solution for IT risk
The organization does not assign budgets to IT-RM for risk mitigation. IT risk managers have the competency to provide methodological support and the power to sanction non-compliance through senior management	Gamma	Global transparency	Since the IT risk mitigation costs have to be negotiated between the involved departments, having no budget for the IT risk managers to deal with IT risks fosters interaction and negotiations between stakeholders

Table 4. Solutions used by Study Cases to Ensure Accountability IT-RM Design Decision

At Alpha, Beta, and Gamma, IT risk managers had different understandings of their job. While IT risk managers ensure formal compliance with the IT-RM process, enforce deadlines and emphasize completeness of reports, they can also support employees in managing their IT risks and develop individual solutions for specific risks. We found that IT risk managers prioritize the formal enforcement of the process and support organizational members in conducting IT-RM differently.

For instance, at Alpha and Gamma the IT risk manager values compliance with formal IT-RM process guidelines. At Alpha, the IT risk manager puts effort into communicating formal IT-RM process descriptions and establishes formal reporting cycles for every new application. At Gamma, one IT risk manager identifies his understanding of IT-RM as, most importantly, compliance with the formal IT-RM process requirements:

> *"I will check [the assessments] as precisely as possible. I first check whether any signature is missing and then I check for plausibility of assessments. If it is documented properly, that means long enough, and if I can understand it without having to request additional details […] I tell my people I want them to be able to provide every requested piece of information by pulling some file out of the drawer. Imagine some reviser coming in and requesting documents… we have to provide them as soon as possible." (Beta group security officer)*

Ensuring a formal process with fixed deadlines and content requirements reduces IT-RM costs, allows comparability, ensures a homogenous quality and allows management to exercise control. Standard processes and methodological support reduce the costs and efforts of managing IT risks by reducing duplicate efforts and achieving economies of scale. Resulting IT risk reports are comparable through a formal standard for reporting and quality is ensured by strict formal guidelines. Based on this information, executives are able to make informed decisions and enforce IT risk mitigation.

This process-enforcing strategy is often perceived as coercive. An employees' focus on the IT risk itself might be reduced since he is often confronted with standard reports and methodologically reoccurring steps. Motivation to think about new IT risks and rather unrealistic, yet highly relevant, IT risks (so-called black swan risks) is low. Employees perceive IT-RM as a formal vehicle to provide standard information on IT risks. However, there is a chance that they may start to reuse standard information leading to a decrease in the quality of assessments.

While Alpha predominantly focuses on ensuring compliance, Gamma balances compliance and support. This is characterized by IT risk managers who value the quality of IT risk assessments, mitigation and reporting. While most of the IT risks are still managed through a formal process, these managers find specific solutions for urgent, particularly sophisticated or rather unimportant IT risks.

> *"Personally, I have my rules of the game. And everybody has to follow these rules. No tolerance. But of course, I also support the colleagues in doing IT-RM. Everyday somebody needs help. I even work on projects and support them in doing IT-RM […] One thing that is so often misconceived is that we can actually help: we can improve daily operations. It is not as if we only cause additional trouble. Okay, of course we often have to force people to report some stuff, think about certain IT risks carefully, etc., but we can also help. We provide experience, solutions, foresight and many other things. So we really have to strive to provide a well-balance relationship between additional work and supporting daily business." (Gamma SBU IT risk manager I)*

Table 5. Solutions used by Study Cases Regarding the Role of the IT Risk Manager Design Decision

Observed Solution	**Case**	**Criterion**	**Enabling-effect**
The IT risk manager focuses on ensuring high-quality IT risk assessments rather than enforcing pre-defined processes. The IT risk manager discusses individual solutions and (if necessary) adopts the IT-RM process	Beta, Gamma	Repair Flexibility	Instead of providing and enforcing strict process descriptions, IT risk managers at Beta and Gamma adapt processes depending on the IT risks and therefore facilitate discussions on the IT-RM process
IT risk managers judge the severity of IT risk by experience and discussion with business and IT. For non-severe risks, the IT risk manager directly supports employees in solving issue. For severe IT risks, the IT risk manager supports and enforces compliance with a formal IT-RM process	Gamma	Flexibility Global transparency	This trade-off provides learning opportunities within IT risk management and provides employees and management with the necessary information on IT risk issues
IT risk managers are selected based on their passion for managing IT resources to minimize risks and maximize returns including an interest in continuous learning	Gamma	Flexibility	By their continuous interest in detecting and mitigating potential deficiencies in organizational processes involving IT, IT risk managers provide learning opportunities and improve organizational processes

Table 5. Solutions used by Study Cases Regarding the Role of the IT Risk Manager Design Decision.

This content-valuing strategy is perceived as enabling (Table 5). With its focus on sharing IT risk content, the process achieves good IT risk estimates that allow informed decision making. IT risk managers are seen as valuable business advisors who increase organizational responsiveness. The constant interaction and individual adoption ensures an adequate fit of IT risk and corresponding IT-RM approach. With IT risk managers focusing on individual requirements and a flexible IT-RM process, employees see the benefit of IT-RM for improving daily operations and thus deliver high quality IT risk information. Employees perceive IT risk managers as supportive and interested in improving daily operations:

> *"I see [central IT-RM] as a moderator for technological developments and perceptions for our organization. Otherwise, we will always be a step behind and we would have to invest an awful lot of effort and resources to solve this." (Beta SBU IT manager II)*

Design Decision 4: IT-RM Reporting

A reappearing issue across all cases was the type of information that was processed for IT-RM reporting. Depending on the different stakeholder requirements, IT risk information has to be aggregated differently to be useful in daily operations. At Gamma, employees refer to this as 'internal marketing':

> *"Internal marketing is important to convince people in the departments to participate. Why is it important to manage IT risks? How does the organization profit? […] Here at [Gamma] the most popular argument is preparing audits: when external audit wants certain information, it is helpful to have talked about that beforehand, have it documented, and be able to pull out certain reports when needed." (Gamma SBU IT risk manager II)*

One strategy to inform stakeholders is to assemble standard reports on a regular basis. These reports are formalized, presented to stakeholders and archived. This process compels employees to think about IT risk independent of incidents. The formal report with documented IT risks is presented to executives on a regular basis to ensure continuity, acknowledgement and a comparison of different IT risks. Alpha collects IT risk information on a regular basis on a standardized form which is presented to executives at board meetings. While executives at Beta and Gamma reported on challenges in prioritizing mitigation due to lack of comparability of IT risks, Alphas formal structure in assessing and reporting IT risks allows a comparison of these risks across all IT functions.

This standard reporting strategy is perceived as coercive. Employees question the practicability of comparing IT risks across different assessments in different departments. Certain risks just do not fit the provided templates and employees have to be creative to "fit" the risk into report. The resulting reports has to be compared to other reports and thus does not allow individual solutions. Management therefore highlights the importance of compliance with the defined templates for assessment.

Following an individual-reporting strategy accounts for the differences in organizational structures, responsibilities, reporting and risk culture across different departments. With an individual-reporting strategy, organizations strive to fulfill all information requirements. In the case of Beta, dedicated IT risk assessments are compiled in management reports for certain issues. As a result, reported IT risks are not invented just for the purpose of documentation, referred to as 'chimera' by one of Beta's executives, and all identified IT risks are relevant and appropriate for requesting a mitigation budget.

This individual-reporting strategy is perceived as enabling (Table 6) as it engages senior management in IT-RM. Provided with individual reports that meet their information requirements and options to collect additional IT risk information if needed, senior management is more likely to provide feedback and engage in risk-informed decision making. One of Gamma's risk managers illustrates the importance of top management support for IT risk management:

> *"You can do really good IT-RM on a grassroots level, but if you have the feeling that management doesn't really care, it won't work. The bottom-up reporting chain will gradually get worse. If senior management doesn't care, you have lost. Then you can't heckle the people which is necessary for good IT-RM." (Gamma SBU IT risk manager II)*

Table 6. Solutions to the Design Decision on IT-RM Reporting and Corresponding Enabling Effect.			
Observed Solution	**Case**	**Criterion**	**Enabling-effect**
IT-RM offers individual assessments and reports in order to fulfill the particular information needs to all involved stakeholders – especially management	Beta, Gamma	Global transparency	Being provided with self-selected IT risk information and being able to request additional reports engages stakeholders in the IT-RM process
Discussions on IT risk reporting are conducted across departments on both the management and operational level	Gamma	Global transparency	This not only fosters exchange on operational IT risk issues that could affect others, but allows joint discussions on mitigation efforts on management level
IT risk reports are discussed with senior IT management including the CIO on a monthly basis	Gamma	Global transparency	Regular discussions foster interaction by alerting top management to issues employees struggle with

Table 6. Solutions to the Design Decision on IT-RM Reporting and Corresponding Enabling Effect.

Discussion

The purpose of this study was to understand how organizations implement enabling IT-RM. We applied grounded theory techniques to data collected in three organizations to identify design decisions for IT-RM. For each design decision, we identified solutions perceived as enabling by organizational members. Placing value on high quality risk assessments over formal documentation and conducting workshops to identify the cause of IT risks seems to facilitate responses to IT-RM process contingencies. Comprehensive templates communicating best practices and individual discussions on difficult assessments provide visibility into the IT-RM process. Providing a budget for IT risk managers, developing individual reports for stakeholders, and regular discussions with senior management, provide stakeholders with an understanding of the overall IT-RM process. Adoption of a formal IT-RM process (if necessary), the passion and expertise of the IT risk manager and continuous re-staffing of the role contribute to learning opportunities for improving IT-RM processes.

Reflecting on the identified design decision reveals both rewarding and punishment-centered elements of enabling IT-RM design. The punishment-centered elements value compliance with the formal process and penalize non-compliance (Boss et al. 2009; D'Arcy and Herath 2011) while entailing a highly standardized reporting procedure with a scheduled information flow from employees to management. The goal of this strategy is to establish an efficient and repeatable IT-RM process in order to document efforts requested by either external or internal stakeholders. Thus, IT-RM is perceived as mandated work requiring compliance.

The rewarding elements center on acknowledging employees' initiative and efforts. This strategy necessitates extensive effort in communicating the benefits of IT-RM to employees and relies on the active participation of key members of the organization to be successful. Employees perceive IT-RM as an important source of information to guide management decision-making and daily operations. Thus, IT-RM is seen as a value-adding vehicle for improving the IT organization.

According to our analysis, when designing enabling IT-RM processes organizations need to balance the rewarding and the punishment-centered elements. IT risk managers orchestrate individual IT-RM processes comprising both rewarding and punishment elements in different combinations. However, we found that across all cases the rewarding elements were designed in the earlier phases of the IT-RM process and in the later phases the punishment-centered elements were applied. The example of Gamma illustrates this observation: When identifying and analyzing IT risks, Gamma's IT risk managers provide extensive templates and encourage employees to creatively identify risks. When moving to IT risk mitigation and reporting, IT risk managers at Gamma moderate workshops for determining and allocating mitigation efforts, enforce thorough documentation of risks, and discuss shortcomings with senior management.

These practices indicate that enabling IT-RM requires rewarding elements in situations that are relevant for collecting, processing, and sharing IT risk information and requires punishment-centered elements for aligning the heterogeneous and incomparable objectives of stakeholders and for reporting IT risks. A possible explanation for this phenomenon could be that the earlier IT-RM phases depend

on employee creativity in identifying risks and employee operational knowledge for assessing the risks (Coles and Moulton 2003; Dhillon and Backhouse 1996). Organizations need to motivate employees to participate by outlining the usefulness of IT-RM and by providing rewards. Applying punishment-centered elements would result in employees fulfilling the requirements with least possible efforts (Boss et al. 2009). This situation would lead to IT-RM where only easy or obvious IT risks are identified and newer, complex and hidden risks, potential black swan candidates, with a potential to harm the organization are not identified (Alter and Sherer 2004; Rainer et al. 1991). In the later IT-RM phases, focus lies on negotiating mitigation responsibilities and ensuring proper documentation (D'Arcy and Herath 2011; Smith and McKeen 2009). Since additional costs and efforts for mitigation are misaligned with employees' personal interests, organizations motivate using punishment-centered elements. Following a rewarding strategy, in this case, would not enforce proper documentation and would challenge comparability of IT risks at management levels.

Our results further reveal the ambidextrous role of the IT risk manager in managing the IT-RM process. The IT risk manager appears to be in charge of balancing the rewarding and the punishment-centered elements. Considering the example of Gamma, this task was divided between two positions. The decentral IT risk manager within each department focuses on rewarding elements and motivates employees to participate in risk assessment. On a group level, the central IT risk manager focuses on punishment-centered elements and ensures timely and proper documentation. In the case of Alpha, the IT risk manager combines both rewarding and punishing elements in his role. While the case of Gamma is in line with research on the role of the IT risk manager in enterprise risk management (Hall et al. 2015), the Alpha case suggests that organizations need to integrate different tasks to be carried out by one IT risk manager (Hall et al. 2015). Balancing the challenge of compliance and continuous improvement can be enabled by IT risk managers who understand their work as facilitating IT-RM through motivating employees and providing knowledge and methodological support, but also exercise power to ensure IT-RM continuity.

Implications, Limitations, and Future Research

This study advances existing knowledge on IT-RM design in several ways. First, we identify four design decisions that foster enabling IT-RM for ensuring compliance and continuous improvement. We characterize context, options, and consequences for each design decision. Second, our analysis reveals several solutions to these design decisions that are perceived as enabling (Adler and Borys 1996). Third, the underlying challenge of designing IT-RM is to balance rewarding and punishment-centered elements to ensure continuous participation of all involved stakeholders. Enabling IT-RM applies the rewarding elements in functions relevant for collecting and processing IT risk information and applies the punishment-centered elements for aligning the heterogeneous and incomparable objectives of stakeholders.

According to our study results, formal procedures, techniques, and structures developed in the literature are widely applied in IT-RM practice (Barki et al. 2001; COSO 2004; Keil et al. 1998; Tiwana and Keil 2004). The challenge of creating enabling IT-RM lies within orchestrating the various solutions – an issue which has not been addressed thoroughly in the literature. Best practices and standards on IT-RM should be designed as a collection of building blocks. The important challenge is to guide IT risk managers in choosing compatible building blocks for designing enabling IT-RM (Hall et al. 2015).

We acknowledge several limitations to our study. Our analysis was based on 31 interviews in three organizations, admittedly a small sample size. Given the exploratory nature of the study (Barki et al. 1993) and our broad interest in understanding enabling process design, this research presents a first step toward understanding enabling IT-RM design. Although we specifically sampled for contrasting data, analyzing IT-RM in other industries might reveal additional design issues which would complement our results. Beyond the type of formalization, other factors such as the type or degree of reward or punishment and the certainty of the incentive mechanisms could provide additional insights on IT-RM processes (Liang et al. 2012).

Future research could examine how the identified design decisions are interrelated to understand patterns of enabling IT-RM design. Our results suggest that the IT-RM design decisions can be seen as a continuum. It might be interesting to study the degree of rewarding and punishment-centered elements with possible influence on participation in IT-RM processes. Future research could study industries with other regulations for IT risk management such as automotive or healthcare. Studies could also apply different research methods such as surveys or experiments to validate our exploratory findings. The application of different lenses, such as goal setting (Locke and Latham 2002) or mindfulness (Swanson and Ramiller 2004) could provide additional insights on the design of IT-RM

processes. Gamma, in our study, regularly appointed new IT risk managers and each IT risk manager had a different perspective, different network and different risk preference, and provided new ideas and focus on other areas. This change in outlook provided new motivation for organizational members. We therefore suggest future research to study the dynamics of the IT-RM process to ensure continuous participation. IT risk managers differ in their understanding of their role and different role interpretations affected IT-RM process design and the type of participation of organizational members. Future research might study the impact of different personalities and roles of IT risk managers on IT-RM participation.

Conclusion

In this study, we investigated how organizations design enabling IT-RM processes. We employed grounded theory techniques to identify, structure and understand organizational solutions that foster enabling IT-RM processes. Design decisions for IT-RM exist when ensuring continuous participation in IT-RM, when determining accountability for risk mitigation, regarding the role of the IT risk manager, and during IT-RM reporting. We identify different solutions to these IT-RM design decisions that are associated with enabling formalization and provide empirical evidence how these solutions facilitate enabling process design. We contrast our findings with literature and find two underlying rationales for IT-RM design. Organizations need to balance rewarding and punishment-centered rationales in designing enabling IT-RM. Our research contributes to the design of IT-RM by providing solutions to ensure enabling IT-RM process design and explaining the underlying rationales. Further research may investigate how organizations design enabling IT-RM in situations where IT risks have not previously caused damage as this could complicate communicating the need for and benefits of IT-RM. While this research assumes that conducting IT-RM in large organizations requires a high degree of formalization, future research could examine how much IT-RM is necessary and identify the corresponding degree of formalization.

References

Adler, P.S., and Borys, B. 1996. "Two Types of Bureaucracy: Enabling and Coercive," *Administrative Science Quarterly* (41:1), pp. 61-89.

Alter, S. 2014. "Theory of Workarounds," *Communications of the Association for Information Systems* (34; Article 55).

Alter, S., and Ginzberg, M. 1978. "Managing Uncertainty in MIS Implementation," *Sloan Management Review* (20:1), pp. 23-31.

Alter, S., and Sherer, S.A. 2004. "A General, but Readily Adaptable Model of Information System Risk," *Communications of the AIS* (14:1), pp. 1-28.

Aron, R., Clemons, E.K., and Reddi, S. 2005. "Just Right Outsourcing: Understanding and Managing Risk," *Journal of Management Information Systems* (22:2), pp. 37-55.

Barki, H., Rivard, S., and Talbot, J. 1993. "Toward an Assessment of Software Development Risk," *Journal of Management Information Systems* (10:2), pp. 203-225.

Barki, H., Rivard, S., and Talbot, J. 2001. "An Integrative Contingency Model of Software Project Risk Management," *Journal of Management Information Systems* (17:4), pp. 37-69.

Benaroch, M., Lichtenstein, Y., and Robinson, K. 2006. "Real Options in Information Technology Risk Management: An Empirical Validation of Risk-Option Relationships," *MIS Quarterly* (30:4), pp. 827-864.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.a., and Boss, R.W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.

Carr, N.G. 2005. "The End of Corporate Computing," *MIT Sloan Management Review* (46:3), pp. 67-73.

CCTA. 1993. "The CCTA Risk Analysis and Management Method (CRAMM) User Guide," IT Security and Privacy Group, London, UK.

Chapman, C.S., and Kihn, L.-A. 2009. "Information System Integration, Enabling Control and Performance," *Accounting, Organizations and Society* (34), pp. 151–169.

Chen, Y., Ramamurthy, K., and Wen, K.-W. 2012. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *Journal of Management Information Systems* (29:3), pp. 157-188.

Ciborra, C. 2006. "Imbrication of Representations: Risk and Digital Technologies," *Journal of Management Studies* (43:6), pp. 1339-1356.

Coles, R.S., and Moulton, R. 2003. "Operationalizing It Risk Management," *Computers & Security* (22:6), pp. 487-493.

COSO. 2004. "Enterprise Risk Management," in: *Integrated Framework: Application Techniques*. Committee of Sponsoring Organizations of the Treadway Commission.

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643-658.

Deloitte. 2010. "Shaping a Risk Intelligent Strategy - Confronting Assumptions to Find Risk and Opportunity," Deloitte, Dallas, TX.

Dewan, S., and Ren, F. 2007. "Risk and Return of Information Technology Initiatives: Evidence from Electronic Commerce Announcements," *Information Systems Research* (18:4), pp. 370-394.

Dhillon, G., and Backhouse, J. 1996. "Risks in the Use of Information Technology within Organizations," *International Journal of Information Management* (16:1), pp. 65-74.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal* (11), pp. 127-153.

Ekelhart, A., Fenz, S., Klemen, M., and Weippl, E. 2007. "Security Ontologies: Improving Quantitative Risk Analysis," *40th Annual Hawaii International Conference on System Sciences*, Big Island, Hawaii, pp. 156-156.

Gemmer, A. 1997. "Risk Management: Moving Beyond Process," *IEEE Software* (30:5), pp. 33-43.

Gouldner, A.W. 1954. *Patterns of Industrial Bureaucracy*. Toronto, Ontario: Free Press.

Hahn, E.D., Doh, J.P., and Bunyaratavej, K. 2009. "The Evolution of Risk in Information Systems Offshoring: The Impact of Home Country Risk, Firm Learning, and Competitive Dynamics " *MIS Quarterly* (33:3), pp. 597-616.

Hall, M., Mikes, A., and Millo, Y. 2015. "How Do Risk Managers Become Influential? A Field Study of Toolmaking in Two Financial Institutions," *Management Accounting Research* (26), 3, pp. 3-22.

Heumann, J., Wiener, M., Remus, U., and Mähring, M. 2014. "To Coerce or to Enable? Exercising Formal Control in a Large Information Systems Project," *Journal of Information Technology* (advance online publication).

ITGI. 2005. *Cobit: Control Objectives for Information and Related Technology*, (4.0 ed.). Rolling Meadows, IL: IT Governance Institute.

Iversen, J.H., Mathiassen, L., and Nielsen, P.A. 2004. "Managing Risk in Software Process Improvement: An Action Research Approach," *MIS Quarterly* (28:3), pp. 395-433.

Keil, M., Cule, P., Lyytinen, K., and Schmidt, R. 1998. "A Framework for Identifying Software Risks," *Communications of the ACM* (41:11), pp. 76-83.

Liang, H., Xue, Y., and Wu, L. 2012. "Ensuring Employees' IT Compliance: Carrot or Stick?," *Information Systems Research* (Articles in Advance).

Locke, E.A., and Latham, G.P. 2002. "Building a Practically Useful Theory of Goal Setting and Task Motivation," *American Psychologist* (57:9), pp. 705-717.

Marinos, L., Kirchner, L., and Junginger, S. 2009. "Integration of an IT-Risk Management/Risk Assessment Framework with Operational Processes," in: *9th International Conference on Wirtschaftsinformatik*. Verona, IT.

Markus, M.L. 2000. "Toward an Integrated Theory of IT-Related Risk Control," in *Organizational and Social Perspectives on Information Technology,* R. Baskerville, J. Stage and J.I. DeGross (eds.). Boston, MA: Springer, pp. 167-178.

Mikes, A. 2014. "The Triumph of the Humble Chief Risk Officer," Harvard Business School, Boston, MA.

Nicolaou, A.I., and McKnight, D.H. 2006. "Perceived Information Quality in Data Exchanges: Effects on Risk, Trust, and Intention to Use," *Information Systems Research* (17:4), pp. 332-351.

Ouchi, W.G. 1979. "A Conceptual Framework for the Design of Organizational Control Mechanisms," *Management Science* (25:9), pp. 833-848.

Purdy, G. 2010. "Iso 31000: 2009—Setting a New Standard for Risk Management," *Risk Analysis* (30:6), pp. 881-886.

Rainer, R.K., Snyder, C.A., and Carr, H.H. 1991. "Risk Analysis for Information Technology," *Journal of Management Information Systems* (8:1), pp. 129-147.

Röder, N., Wiesche, M., and Schermann, M. 2014. "A Situational Perspective on Workarounds in IT-Enabled Business Processes: A Multiple Case Study," in: *European Conference on Information Systems*. Tel Aviv.

Schermann, M., Wiesche, M., Hoermann, S., and Krcmar, H. 2014. "Information Technology Risks: An Interdisciplinary Challenge," in *Risk - a Multidisciplinary Introduction,* C. Klüppelberg, D. Straub and I.M. Welpe (eds.). Springer International Publishing, pp. 387-405.

Schermann, M., Wiesche, M., and Krcmar, H. 2012. "The Role of Information Systems in Supporting Exploitative and Exploratory Management Control Activities," *Journal of Management Accounting Research* (24:1), pp. 31-59.

Schmidt, R., Lyytinen, K., Keil, M., and Cule, P. 2001. "Identifying Software Project Risks: An International Delphi Study," *Journal of Management Information Systems* (17:4), pp. 5-36.

Sharma, S., and Dhillon, G. 2009. "IS Risk Analysis: A Chaos Theoretic Perspective," *Issues in Information Systems* (X:2), pp. 552-650.

Sherer, S.A. 2004. "Managing Risk Beyond the Control of IS Managers: The Role of Business Management," in: *37th Annual Hawaii International Conference on System Sciences*. Big Island, HI.

Sherer, S.A., and Alter, S. 2004. "Information System Risks and Risk Factors: Are They Mostly About Information Systems?," *Communications of the AIS* (14:2), pp. 29-64.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), p. 487.

Smith, H.A., and McKeen, J.D. 2009. "Developments in Practice XXXIII: A Holistic Approach to Managing IT-Based Risk," *Communications of the Association for Information Systems* (25:1), p. Article 41.

Smith, H.A., McKeen, J.D., and Staples, S. 2001. "New Developments in Practice I: Risk Management in Information Systems: Problems and Potential," *Communications of the Association for Information Systems* (7:13).

Spears, J.L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp. 503-522.

Straub, D.W., and Welke, R.J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Straub Jr, D.W., and Nance, W.D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), pp. 45-60.

Strauss, A., and Corbin, J.M. 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Newbury Park, CA: Sage.

Suddaby, R. 2006. "What Grounded Theory Is Not," *Academy of Management Journal* (49:4), pp. 633-642.

Swanson, E.B., and Ramiller, N., C. 2004. "Innovating Mindfully with Informationtechnology," *MIS Quarterly* (28:4), pp. 553-583.

Teneyuca, D. 2001. "Organizational Leader's Use of Risk Management for Information Technology," *Information Security Technical Report* (6:3), pp. 54-59.

Tiwana, A., and Keil, M. 2004. "The One-Minute Risk Assessment Tool," *CACM* (47:11), pp. 73-77.

Urquhart, C. 2012. *Grounded Theory for Qualitative Research: A Practical Guide*. London, UK: Sage.

Weinstein, L. 2004. "Outsourced and out of Control," *Communications of the ACM* (47:2), pp. 120-121.

Westerman, G. 2007. "IT Risk Management: From IT Necessity to Strategic Business Value," MIT Sloan School of Management Cambridge, MA.

Wheeler, J.A., Caldwell, F., and Proctor, P.E. 2013. "Predicts 2014: Advances in Risk Management Technology Will Improve Corporate Performance and Public Policy," Gartner, Stamford, CT.

Wiesche, M., Bodner, J., and Schermann, M. 2012. "Antecedents of It-Enabled Organizational Control Mechanisms," *20th European Conference on Information Systems (ECIS)*, Barcelona, Spain.

Wiesche, M., Keskinov, H., Schermann, M., and Krcmar, H. 2013a. "Classifying Information Systems Risks: What Have We Learned So Far?," *46th Hawaii International Conference on System (HICSS)*, Grand Wailea, HI.

Wiesche, M., Schermann, M., and Krcmar, H. 2013b. "When IT Risk Management Produces More Harm Than Good: The Phenomenon of 'Mock Bureaucracy'," *46th Hawaii International Conference on System (HICSS)*, Grand Wailea, HI.

Xue, Y., Liang, H., and Wu, L. 2011. "Punishment, Justice, and Compliance in Mandatory IT Settings," *Information Systems Research* (22:2), pp. 400-414.

Zuboff, S. 1988. *In the Age of the Smart Machine*. New York, NY: Basic Books.