Communications of the Association for Information Systems

Volume 41 Article 3

8-2017

Shadow Systems, Risk, and Shifting Power Relations in Organizations

Daniel Furstenau
Freie Universität Berlin, daniel.furstenau@fu-berlin.de

Hannes Rothe
Freie Universität Berlin

Matthias Sandner
Freie Universität Berlin

Recommended Citation
Furstenau, Daniel; Rothe, Hannes; and Sandner, Matthias (2017) "Shadow Systems, Risk, and Shifting Power Relations in Organizations," *Communications of the Association for Information Systems*: Vol. 41 , Article 3.
DOI: 10.17705/1CAIS.04103
Available at: https://aisel.aisnet.org/cais/vol41/iss1/3

Communications of the
Association for Information Systems

Research Paper ISSN: 1529-3181

Shadow Systems, Risk, and Shifting Power Relations in Organizations

Daniel Furstenau
Freie Universität Berlin
Department of Information Systems
daniel.furstenau@fu-berlin.de

Hannes Rothe
Freie Universität Berlin
Department of Information Systems

Matthias Sandner
Freie Universität Berlin
Department of Information Systems

Abstract:

Drawing on notions of power and the social construction of risk, we build new theory to understand the persistence of shadow systems in organizations. From a single case study in a mid-sized savings bank, we derive two feedback cycles that concern shifting power relations between business units and central IT associated with shadow systems. A distant business-IT relationship and changing business needs can create repeated cost and time pressures that make business units draw on shadow systems. The perception of risk can trigger an opposing power shift back through the decommissioning and recentralization of shadow systems. However, empirical findings suggest that the weakening tendency of formal risk-management programs may not be sufficient to stop the shadow systems cycle spinning if they fail to address the underlying causes for the emergence of shadow systems. These findings highlight long-term dynamics associated with shadow systems and pose "risk" as a power-shifting construct.

Keywords: Shadow Systems, IT Governance, Power, Risk, Business IT Alignment.

This manuscript underwent peer review. It was received 06/12/2016 and was with the authors for 8 months for one revision. Jackie Rees Ulmer served as Associate Editor.

1 Introduction

In this paper, we study the importance of power relations between business units and central IT units to understand the persistence of shadow systems in organizations. By shadow systems, we refer to autonomous software systems or extensions to existing systems that a central IT department neither develops nor controls (Behrens, 2009; Fürstenau & Rothe, 2014; Zimmermann, Rentrop, & Felden, 2014). *Shadow systems* and related terms[1] have increasingly grown in practical and academic attention due to the emergence of cloud computing (Mell & Grance, 2011; Müller, Holm, & Søndergaard, 2015), software-as-a-service (Winkler & Brown, 2013), bring-your-own-device (BOYD) programs (Miller, Voas, & Hurlburt, 2012), IT-related workarounds (Alter, 2014), low-entry programming in spreadsheets (Leon, Abraham, & Kalbers, 2010), and other important trends in the technological landscape toward decentralized and user-driven computing innovations (György, Cleven, Uebernickel, & Brenner, 2012).

The term "shadow systems" suggests a need to balance autonomy in decentralized units with central governance. As studies on IT governance have long described (Brown & Magill, 1994; Sambamurthy & Zmund, 1999; Winkler & Brown, 2014), autonomy without central governance may lead to diverse and incompatible systems that become decoupled from the rest of the organization (Tanriverdi, 2005), whereas too strict central accountability can result in an organization that neglects important benefits from being responsive to and leveraging user-driven innovation (Winkler & Brown, 2014). Therefore, organizations need to carefully assess the level and type of autonomy granted to business users in decentralized units (Tiwana & Konsynski, 2010).

Although some organizations explicitly allow shadow systems because they believe in their innovative potential, most use a range of formal risk-management tools (e.g., IT service management, IT governance, and IT security management) to direct, restrict, and control the activities of business units. In recent years, managers have paid greater attention to minimizing costs and risks partly in response to high IT costs and partly in response to increasing regulations in sectors such as financial services or the pharmaceutical industry (e.g., Gozman & Willcocks, 2015; Leon et al., 2010; Panko, 2006).

Many organizations fail to eliminate or reduce the amount of shadow systems despite serious attempts and repeated efforts to do so (Rains, 2015; Walters, 2013). This observation is paradoxical because it suggests that most organizations use more formal risk-management tools and still achieve less of the desired outcome (a reduction of shadow systems). Often, shadow systems persist or return even though managers have begun efforts to eliminate them.

Researchers have rarely analyzed the long-term dynamics that drive the persistence of shadow systems in detail. The literature on IT governance and shadow systems has produced a rich contextual understanding of what shadow systems are and what schemes one can implement to govern and control them (Andriole, 2015; György et al., 2012; Zimmermann & Rentrop, 2014; Zimmermann et al., 2014). Yet, it fails to account for the dynamic complexity that drives the ongoing rise and fall of shadow systems in contemporary organizations with hundreds and thousands of decentralized devices and systems. It also says relatively little about why many organizations fail to eliminate shadow systems. Thus, it tends to overvalue the control that managers and other interest groups can exert to influence the evolution of shadow systems in organizations. To analyze the long-term dynamics associated with shadow systems' persistence, we draw on notions of power and the social construction of risk to build theory that establishes new relationships between theoretical constructs that researchers have not previously expressed. In particular, we address the following research question:

RQ: How do shadow systems affect the power relations between central IT and business units?

To explore these aspects, we conducted a single case study in a German bank. Drawing on in-depth observations and interviews, we suggest that the emergence and decommissioning of shadow systems is a multi-faceted process that unfolds over time: the simultaneous presence of various factors can trigger a reinforcing process in which particular shadow systems gain critical importance for an organization. In consequence, the power of the shadow system organization increases, which undermines the control of the central IT unit. We label this tendency as "governance problem" because it results in an emerging void in the exertion of decision rights and an increasing imbalance in favor of decentralized goals and priorities. In other words, certain actor groups in the organization purposefully and deliberately use a vaguely

[1] Refer to Kopper and Westner (2016) for a literature review and a distinction of related terms (e.g., shadow IT, feral systems, and workarounds). We focus on "shadow systems" as defined above and in Section 2.1.

described or less rigorously enforced IT governance strategy to achieve their own goals. In consequence, shadow systems thrive and the IT landscape drifts apart. Managerial attempts to eliminate shadow systems by constructing them as a "risk" may then run dry and the inflow of shadow systems continues as the underlying governance problem persists.

This paper proceeds as follows: in Section 2, we introduce the theoretical and conceptual background. In Section 3, we refer to the methods of this study. In Section 4, we present the results. Finally, in Section 5, we summarize the findings and discuss their implications and future research opportunities.

2 Conceptual Background

2.1 Shadow Systems are Sociotechnical Phenomena

We start with the observation that organizational work systems comprise individuals and organizational structures that contribute to the success of technical solutions. According to this view—known as the sociotechnical systems view (Bostrom & Heinen, 1977)—social (human and organizational) elements and technical systems are deeply "intertwined in complex webs of mutual causality" (Winter et al., 2014, p. 253).

We contend that one must understand shadow systems as sociotechnical phenomena. First, research shows that individuals are key for establishing a shadow system. Thus, understanding their intentions and motivations is central (Haag & Eckhardt, 2014a; Haag, Eckhardt, & Bozoyan, 2015). Shadow systems can help individuals to work around the limitations of existing information systems or processes in an organization (Alter, 2014; Berente & Yoo, 2012; Strong, Volkoff, & Elmes, 2001). Actors tend to individualize systems according to business needs if they meet their individual requirements (e.g., prior computing experience) and social context conditions (e.g., beliefs or norms of a peer group) to adopt new or adapt existing IT (Gaß, Ortbach, Kretzer, Maedche, & Niehaves, 2015). Shadow systems are often readily available and perceived as being easier to use than central systems and more cost effective (György et al., 2012). The adaptation of external cloud services, for instance, often reduces the perceived up-front investment and ongoing operation costs (Müller et al., 2015). Second, over time, establishing organizational structures and processes becomes more important for the survival of a shadow system. Without proper support, a shadow system stays small and organizationally unimportant (Behrens, 2009). The "hit-by-a-bus" scenario (Behrens, 2009) describes a situation in which business processes that a shadow system supports are threatened as key individuals leave the organization. Thus, some scholars see sustainable support structures for shadow systems as vital (Zimmermann et al., 2014). Taken together, we can see the importance of *both realms*, the technical and the social, to understand shadow systems.

2.2 Shadow Systems Affect Power Relations in Organizations

One important implication from taking a sociotechnical perspective on organizational work systems is that one must view shadow systems as an instrument of power and a mechanism to influence power relations (see also Kerr, Houghton, & Burgess, 2007; Spierings, Kerr, & Houghton, 2012). Researchers often refer to power as a personal value that describes an individual's ability to exert influence (Hauke, 2006). In this sense, power is usually associated with related concepts such as "social status" (Bothner, Smith, & White, 2010), "prestige" (Henrich & Gil-White, 2001), and a feeling of control and dominance. Power relations affect the actions that individuals take in groups and organizations (Weick, 1993). In particular, individuals can create a feeling of control to trigger the action of another by drawing on direct command, strategic manipulation, and politics (Cropanzano, Howes, Grandey, & Toth, 1997), resource dependency exploitation (Pfeffer, 1981), or techniques of observation and anticipatory obedience (Foucault, 1995). Power has long been a central theme in the IS literature (Jasperson et al., 2002; Silva & Backhouse, 2003; Xue, Liang, & Boulton, 2008). We have learnt from many studies that IT tends to reinforce the existing power base in organizations (George & King, 1991) not only on an individual but also on a group level (Markus, 1983) (e.g., of departments or divisions). Accordingly, one important force behind economic rationales for centralizing or decentralizing computing resources is the attempt to gain control and power (King, 1983). This implies that shadow systems—as a form of decentralized computing by individual users, work groups, and business units—are subject to power struggles as they potentially change power relations in organizations (i.e., between business units and between business units and central IT). Behrens (2009) observes that politics will be central for understanding the rise and fall of shadow

systems. According to her view, "shadow systems are exposed to a greater depth and range of politics than formal systems" (p. 128).

Based on this reasoning, we observe that shadow systems will often emerge if a business unit does not perceive the ability (has the power) to influence the actions that a central IT department takes to fulfill its demands. Prior research indicates that this inability may arise if the official IT unit lacks resources (Winkler & Brown, 2014), business knowledge (Tiwana, 2009; Winkler & Brown, 2013), openness and honesty (Nwankpa & Roumani, 2014), or agility (see György et al., 2012). Thus, the central IT "refuses" to act. As a result, shadow systems appear to be a "quick fix" or "workaround" (Alter, 2014) to enable action and overcome "blocks" (Koopman & Hoffman, 2003) in work processes. A consistent explanation to this pattern—but one absent in the literature—is that another business unit (or senior manager) that becomes a "preferred partner" dominates the central IT. Thus, the respective business unit may turn to another partner (e.g., a cloud provider) to compensate for lacking IT support or agility by the central IT. This situation is common in organizations that must prioritize the needs of different units.

On a second note, we argue that the established power relations may shift over time with the growth of shadow systems. In particular, a shadow system is often a reaction to novel business needs (Behrens, 2009; Jones, Behrens, Jamieson, & Tansley, 2004) and infuses innovation into organizations (György et al., 2012). Novelty, in turn, produces situations of ambiguity—it allows for "multiple interpretations, contradictions, or disagreements about boundaries, principles, or solutions" (Levina & Orlikowski, 2009, p. 672). Moreover, the inherent ambiguity of novel situations creates openings for reconfiguring power relations (Levina & Orlikowski, 2009). Whereas many shadow systems start as small systems with a limited user base and a narrow scope, these systems grow over time as their functional scope and/or the number of stakeholders expand. In turn, this growth will again challenge existing power relations in organizations. Shadow systems may grow stronger, which also affects the knowledge base and social status of individuals concerned with them. Thus, existing power relations are constantly challenged with the rise and fall of shadow systems.

2.3 Shadow Systems as a "Risk" that can Shift Power Relations

In consequence of shadow systems' growing importance, IT executives and senior managers may reevaluate and reengineer existing IT governance and risk-management schemes to counteract shifts toward decentralization (Xue et al., 2008). In particular, we view "risk" as socially constructed and, thus, subject to power struggles (Power, 2007). According to this view, what is perceived as a risk and how it is managed depends critically on managerial "systems of representation, and on instruments for framing objects for the purpose of action and intervention" (Power, 2007, p. 4). Thus, equating risks with potential underlying hazards and dangers, which are uncertain by nature, fails to account for the fact that risk management is at the same time a device for rationalizing and legitimizing actions by certain groups of actors (Power, 2007). A shadow system brings many undisputable dangers and challenges for security and privacy (Silic & Back, 2014) and IT governance (Zimmermann et al., 2014). They arise, for instance, from reliance on a single person (Behrens, 2009); poor code quality, design, and documentation (Raden, 2005); errors and fraud (Leon et al., 2010; Panko, 2006); poor architectures (Fürstenau & Rothe, 2014); and vendor-related issues (Furneaux & Wade, 2011; Tanriverdi, 2005). Thus, shadow systems may be more vulnerable in the case of contextual changes such as organizational restructurings or IT transformations (Behrens, 2009; Fürstenau, Sandner, & Anapliotis, 2016; Gregory, Keil, Muntermann, & Mähring, 2015). Yet, given a range of potential measures and "participatory" modes of IT governance (Andriole, 2015), if a shadow system becomes a risk, it may be easier for IT executives and senior managers—possibly in coalition with external consultants (Lyytinen & Newman, 2015)—to argue for its decommissioning or recentralization. By definition, these central measures occur before an adverse event (e.g., the exit of key employees) actually does because it is intended as a preventive measure that "secures" the corporate environment. Thus, we argue that a central IT department can depict shadow systems as a risk to regain power by recentralizing computing resources.

2.4 Summary

We put forward three arguments. First, we contend that shadow systems affect the power relations between the business units that create shadow systems and central IT and between different business units themselves (in the empirical analysis, we focus on the first relationship). Second, we argue that power relations shift over time with the rise and fall of shadow systems. Third, we argue that a central IT department can construct shadow systems as a way to regain power. However, we have little systematic

knowledge on how shadow systems actually change the existing power relations in organizations. A more systematic understanding of the dynamic interaction between shadow systems, risk, and power would be important for IT managers and for governance professionals to set impulses that increase the long-term alignment of business and IT (Coltman, Tallon, Sharma, & Queiroz, 2015; Gerow, Grover, Thatcher, & Roth, 2014; Tiwana, Konsynski, & Venkatraman, 2013) and may also shed light on why shadow systems persist or return despite repeated efforts to eliminate them.

3 Methods

3.1 Case Context

To address our research question on how shadow systems, risk, and power relate to each other in organizations, we conducted a qualitative single case study (Yin, 2013) in a mid-sized German bank that we anonymize as Savings Bank[2]. A case method suited the study because it allowed us to explore shadow systems in a real-world context and, thereby, build theory. We selected the banking industry due to the need to reduce risks from shadow systems in a highly regulated environment on the one hand and to be innovative in a competitive market on the other hand. After the financial crisis, banks such as Savings Bank began to implement tighter risk-management systems as a consequence of more restrictive regulatory obligations (see Leon et al., 2010; Panko, 2006). On the other hand, direct banking and the Internet put increased pressure on established institutes, which created resource scarcity and, thus, potential power struggles. Savings Bank was founded in the 19th century and has a long tradition of providing its customers with banking services such as saving and cash accounts, credits, and investment banking. The case is revelatory because, in 2014, the bank underwent a major restructuring in which it outsourced investment banking to another institute. During this process, the bank dismissed 6,000 of its 12,000 employees and ceased many lines of business. This restructuring intensified the resource scarcity and, thus, created conflicts over contested terrain such as the legitimacy of and the control over shadow systems. In our case, two units represented IT (collectively referred to as “central IT”). The group IT (GroupIT) provided central systems and infrastructure and operated data centers for a group of banks in Germany, among them Savings Bank. The business unit IT (BusIT) managed local IT projects and applications. As part of the restructuring, the bank transferred several processes from BusIT to GroupIT.

We collected data from interviews, observations, and archival material. We conducted 11 semi-structured interviews (see Table 1). With two exceptions, these interviews took place over a four-month period in 2015. To balance opposing views, we consulted experts from both business units and IT. Their roles include shadow system developers and users and IT governance. They had worked for company experience from two to 25 years. Interviews lasted between 45 and 60 minutes. We tape-recorded, transcribed, and stored all interviews in a case database. The questions firstly delved into the interviewees’ specific first-hand experiences with one or few shadow systems before delving into more general observations related to them. A final question clarified the specific governance arrangements in the firm and the relationships between business and IT units (see interview guide in Appendix 1). We used these interview questions to obtain critical or revelatory examples that would be theoretically useful to understand why shadow systems persist and their temporal dynamics in a real-world context. In the process, we could leverage the first-hand experience of one key informant (#6) who had several years of working experience with the institute (2012-2014). Because he was part of a trading unit team that had developed a shadow system, he could report from numerous occasions where shadow system-related questions were discussed. He also helped us to locate other well-informed people in the company who were either using or developing shadow systems in their daily work. This procedure followed the principle of snowball sampling (Miles & Huberman, 1994). Another key informant helped us to get in contact with the IT governance roles. Analogously, we applied snowball sampling. We made sure that all interviewees had direct access to shadow systems to foster the credibility of their statements (Madill, Jordan, & Shirley, 2000). We confirmed their credibility by asking them for specific examples and events that indicated their involvement in developing, using, or overseeing a shadow system. We triangulated the primary data with a range of internal and external documents, among them system documentations and architecture plans.

[2] We altered the names of the company, departments, and systems to ensure anonymity.

Table 1. Expert Interviews

No.	Area	Role	Exp. (years)
#1	Treasury	Developer	21
#2	Trading	Developer / user	8
#3	Trading	Developer / user	19
#4	Back Office	User	12
#5	Treasury	User	6
#6	Trading	Developer / user	3
#7	BusIT	IT governance	25
#8	Management	IT governance	11
#9	Management	IT governance	10
#10	GroupIT	IT governance	18
#11	GroupIT	IT governance	2

3.2 Data Analysis

Following established approaches in qualitative data analysis (Miles & Huberman, 1994), we analyzed the data in several steps. First, we identified factors driving the emergence and discontinuation of shadow systems in the case company. To do so, we developed a coding scheme based on existing theoretical constructs (Table 2 and Figures 1-3 show the results). We refined the scheme further in an "abductive" process (Gioia, Corley, & Hamilton, 2012) while drawing on empirical insights. To gain in-depth empirical insights, we developed case stories for two shadow systems. The stories serve as information system biographies (Williams & Pollock, 2012) that shed light on the entire lifecycle of the systems. Based on these materials, we then prepared feedback loop diagrams (Perlow, 1999) to abstract from our empirical insights and synthesized them into a graphical model. The resulting model helps one build theory (Eisenhardt, 1989) because it establishes relationships between theoretical constructs that research has not previously expressed (Burton-Jones, McLean, & Monod, 2015).

4 Results

In the following, we present our results. In Sections 4.1 and 4.2, we introduce two feedback cycles regarding the emergence and discontinuation of shadow systems. In Section 4.3, we integrate these cycles and discuss their interrelationship. In Section 4.4, we conclude the case.

4.1 Emergence of Shadow Systems and the Governance Problem

Our data confirmed that several credible reasons existed for why shadow systems appeared in the case company. Table 2 summarizes these reasons and Appendix 2 exemplifies data codes as part of the conceptualization. One reason was the company's loose compliance policy: it did not restrict employees from extending Microsoft Excel or Access with macros, which let many users consider this alternative because it was readily available.

These reasons (see Table 2) typically occurred in combination. To illustrate that, we draw on an example of a shadow system for market data delivery that we anonymize as "order book tool". The tool emerged in the trading department to process market data and place automatic orders, and the treasury and back office also later used it. The first important reason for the emergence of the system was the *necessity to diversify* the product portfolio in a competitive market place. To that end, the order book tool promised to speed up the delivery process of market data by several milliseconds, which would provide an edge over the market. One of the shadow system developers (#3) noted: "market data was provided by an external party. Our system has achieved to process that data faster, which enabled pooling and using it earlier".

Table 2. Reasons for Emergence of Shadow Systems at Savings Bank

Reason		Explanation	Number of interviewees
Distant business–IT relationship	Lacking business knowledge of central IT	The tasks of business units require context-specific business knowledge that was often not available in the IT department.	6
	Business lacks trust in abilities or benevolence of central IT	The business units felt that the central IT was too far away or too slow due to cultural, personal, and/or spatial conditions.	5
Need to diversify		While the IT department typically offered out-of-the-box standard solutions, they often did not fit the specific business unit demands.	4
Cost pressure		Solutions that IT offered were perceived as too expensive (in comparison to shadow systems); often, they did not fit the business unit budget.	3

A second reason for the emergence of shadow systems in general and the order book tool in particular was a *distant relationship*. We refer to the distance between business and IT as the spatial, personal, and cultural distance between users of an information system in a business unit with the actors who develop, customize, maintain, and deploy them. Accordingly, for shadow systems, the distance is minimal by definition because users are in most cases also the developers of such systems.

At Savings Bank, the increasing distance between business and IT positively moderated the emergence of shadow systems in two ways. The increasing distance became apparent firstly in the central IT's *lack of business knowledge*. As an example, the business unit team from trading, commissioned with the development of the order book tool, considered a solution from central IT. Yet, they rejected it because central IT did not have the required knowledge. As one interviewee (#3) noted, the knowledge is very "specific" (e.g., commission trades). Furthermore, the team assumed that it would take too long to pass on the knowledge. Another interviewee (#5) from the treasury, who later came to use the system, noted that "some colleagues just don't have the time or patience to pursue the official path…. They don't want IT on board as IT lacks the knowledge and as it takes them too long to explain it to them." A distant relationship became apparent secondly in the *level of trust* between business units and central IT. Nwankpa and Roumany (2014) have shown that trust is a major driver for why business users adapt systems from central IT. As Mayer, Davis, and Schoorman (1995) and Rousseau, Sitkin, Burt, and Camerer (1998) discuss, we observed that both parties less often tested and reinforced each other's abilities, benevolence, and integrity.

Altogether, several interviewees confirmed that a *distant relationship* was an important driver for the emergence of shadow systems. As an example, we refer to the observation that BusIT's office was located in a building separate from the business units, and GroupIT was located in a different city. Collectively, decisions on the introduction of information systems by central IT were made in "application and planning meetings at [central IT], which basically allocate development budgets to different subsidiaries" (#11). These meetings took place twice a year. The business units were also reluctant to negotiate with the central IT. For instance, an employee from central IT (#7) remarked: "Despite the fact that we had a central contract database, contracts existed of which management simply did not know and even though we were the central IT department, for long we didn't have a clue what's going on in the company". The employee continued: "Until recently, business unit employees bought their own servers and contracted consultancy firms without our [central IT] knowledge. You can't do that in a decentralized way." A business unit employee (#5) reflected on the company's situation:

> *Sometimes we had conflicts over responsibilities. Other companies pool "business" and "IT" together as the processes heavily involve IT. But if you separate both parts than business does not know about IT and IT does not pay attention to the workflows.*

In sum, these examples show that the emergence of shadow systems in the case company was a complex process. It resulted from the company's need to diversify and a distant business-IT relationship, which manifested itself in IT unit's lacking business knowledge and the business unit's lacking trust.

The emergence of shadow systems started a vicious circle that we refer to as the "governance problem" (see Figure 1). As expected from the sociotechnical view, the growth of shadow solutions triggered a need for support and maintenance personnel. Internal employees and contracted external parties fulfilled this

need. For example, power users in the trading unit and contracted external IT consultants operated the order book tool. Business unit employees and temporary staff maintained another shadow system in the trading unit, an algorithmic trading system. With the increasing number of shadow systems and with higher levels of technical skills and emotional attachment to them in business units, shadow systems grew in importance and criticality.

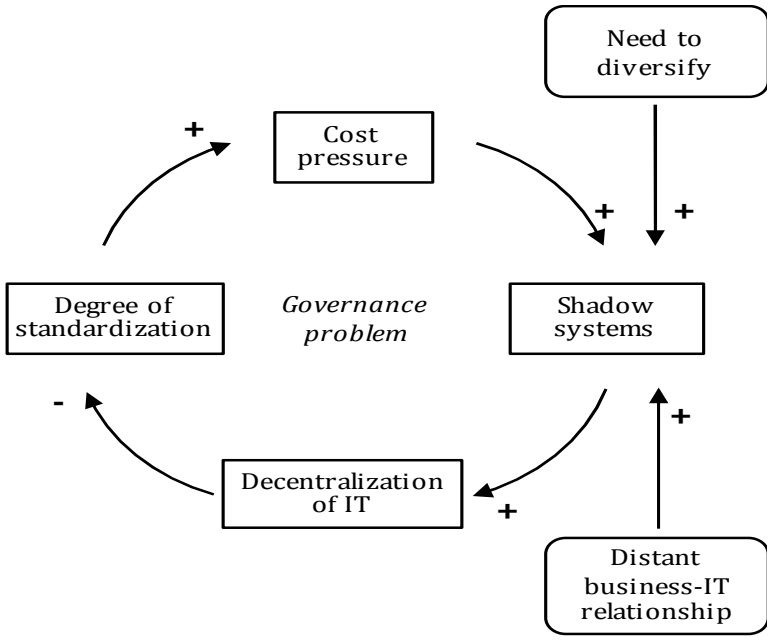

Figure 1. The Emergence of Shadow Systems and the Governance Problem

The *decentralization of IT* followed as a direct consequence because actors in those business units were able and willing to develop systems on their own. As a result, central IT had less direct access and influence on these systems and experienced a subtle loss of power. Thus, the business unit obtained a better position to justify further investments and central IT began to lose importance as a business partner. The power balance shifted. It is reasonable to refer to this trend as a "governance problem" because it weakened the central IT's ability to exercise control over applications and to align them with the company's overall goals and directives (Weill & Ross, 2004), which led to an emerging void that decentralized units filled without paying full attention to overarching goals and priorities.

In alignment with Fürstenau and Rothe (2014), we saw that this situation led to a decreasing *degree of standardization* and increasing fragmentation in the entire IT landscape. Whereas the aforementioned order book tool was an off-the-shelf software from a French provider (even though it still used an unapproved technology stack), the business units (trading, treasury, back office, and others) implemented other custom, unstandardized software, such as the algorithmic trading tool. A more fragmented, diverse, and unstandardized IT landscape emerged. As one interviewer (#1) said: "[the] disadvantages [of a quickly developed, tailor made software artifact] are obvious: the solution is neither standardized nor could it be integrated into or linked with other systems and software applications". Accordingly, a company's ability to fully exploit cost synergies and scope effects across units (Tanriverdi, 2005) decreases as costs to maintain and update the diverse systems increase. For instance, at some point, the algorithmic trading tool required a new server because its capacity overloaded. The trading unit, which had developed the system in order to simulate and perform complex algorithmic trades, refused to pay the upcoming costs and the unit considered several options. Asking central IT for support was one way for the trading unit to solve the issue. Yet, central IT lacked resources—not at least because previous saving rounds had targeted the IT budget. Hence, the central solution was too costly. While central IT budgets remain mostly transparent in the company's overall balance, IT expenditures in these budgets are also prone to be cut-down in an effort to reduce overall costs. Business units in the case company could hide such expenditures in other budgets. As an IT strategist (#7) posited: "an experienced project manager plans [his projects] with cost premiums in order to use the remaining budget to finance other, smaller projects [such as a complementing IT development]". As we can see, *cost pressures* again reinforced the business

unit's trend to developing and using shadow systems because they favored managerial actions to withdraw further resources from central IT.

4.2 Decommissioning of Shadow Systems

While business units faced constant pressure to create new shadow systems to fulfill the demand for innovative and more advanced solutions, another trend counteracted the tendency toward shadow systems. We call this feedback loop "decommissioning of shadow systems" (see Figure 2).

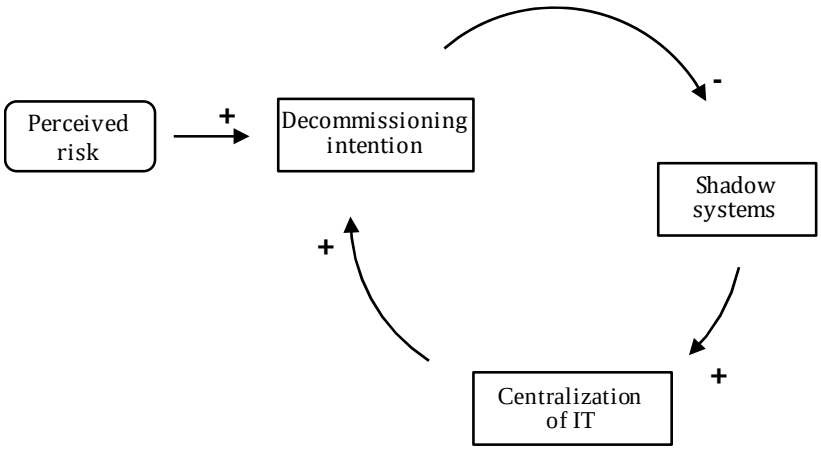

Figure 2. Decommissioning of Shadow Systems

A *perception of increased risk* initiates this cycle. The perception emerged primarily at a senior management level, and these managers passed it on to central IT due to two factors. At first, financial supervisory authorities imposed new regulations on the institute that increased its reporting and risk-management obligations. Most importantly, German regulators mandated and increasingly enforced a regulation called "MaRisk", which imposed new accountabilities on the institute such as end-to-end process transparency. Consistent with a view that the actors in an organization socially construct risks (Maguire & Hardy, 2013; Power, 2008), we observed that central IT's focused its attention on shadow systems that suffered from "severe" system-related problems such as poor design and architecture, missing documentation, reliance on single persons, and vendor-related issues. For instance, a business employee (#4) stated: "Risk is in my opinion the single most important reason for why such systems disappear. I know the creation process of such systems and in many cases it is chaotic. There is no proper documentation and the data can be distorted.". Second, central IT's focus on the risk of shadow systems also increased with the organizational restructuring. For instance, when Savings Bank outsourced the trading department to another company, it was performing a risk assessment on the order book tool and the algorithmic trading tool. Central IT eventually triggered the decommissioning of the algorithmic trading tool because it suffered from an overloaded server and lacked documentation and reliable support. An informant (#1) stated:

> *Coming to think of it, the system was doing what it was supposed to do but it was not extensible and it was hard to maintain. Another freelancer was becoming responsible for maintaining the system. This was a major security leak and a risk for the bank.*

The order book tool was in a better shape, and, because it was critical to the organization, it was relocated from the business unit to central IT ownership.

Senior management helped central IT to regain power and restricted shadow systems with four measures. First, the company set up a formal IT compliance policy with rules and procedures intended to limit and control the amount of shadow systems. For instance, it requested business units to report their business-developed systems once a year in a repository that the central IT administered. Thus, an increase in the centralization of IT led to an increase in the overall alertness towards this phenomenon. Centralization also provided resources for advancing methods and processes to make shadow systems more visible and quantify the risks associated to them. In turn, the risk quantification created confidence in the proposition that it was legitimate or even necessary to decommission them. Therefore, as Figure 2 shows, an increase in IT centralization created pressure on central IT to reveal and decommission (or centrally

govern) existing shadow system instances and, thus, diseconomies to create new shadow systems. One of the users of the order book tool, a back office employee (#4), stated:

> *When we had two systems running in parallel, we faced situations in which we didn't know who is right and who is wrong. We are a bank that trades real money. These failures have costed us a lot of money. That's why I am glad that the control is now with the IT: because we have one more control instance.*

Second, the company appointed process owners. They became responsible for all IT systems that business units used in core business processes and, thus, increased the level of central control. Third, management also cut the number of official IT locations. An IT employee (#7) commented: "They have used another trick: by cutting down the number of locations to two, they have brought the people closer together, which enabled to enact controls more easily". Fourth, senior management also pared-down the IT budgets of business units to tighten controls and to restrict the usage of shadow systems.

4.3 Counteracting Tendencies Toward and Away from Shadow Systems

As Figure 3 summarizes, the Saving Bank case suggests two counteracting forces related to shadow systems that affected the power balance in organizations. Firstly, we observed that cost pressures, a need to diversify, and a distant relationship between business and IT triggered business units to use shadow systems (see Section 4.1). These factors resulted in business units' constantly needing non-standardized solutions that provided an edge over the market. Second, the case suggests that perceptions of risk that result from an increased emphasis of compliance and governance trigger a tendency towards dissolving shadow systems (see Section 4.2). Figure 3 summarizes these dynamics. The left side of the figure shows the "governance problem", a process in which ongoing cost and differentiation pressure led business units to use more and more shadow systems. On the right side, in the "decommissioning of shadow systems" loop, management directives counteract the slipping effect towards shadow systems. However, in the case company, the central IT had insufficient authority to regain full control and to stop the business units from increasingly using shadow systems. The senior management's four measures affected the relationship between business and IT because they restricted the business users. However, the relationship remained problematic, and central IT still lacked relevant context-specific business knowledge. Thus, in the time that the management measures took to strengthen central IT and to decommission shadow systems, the business units still had opportunities to create new shadow systems.

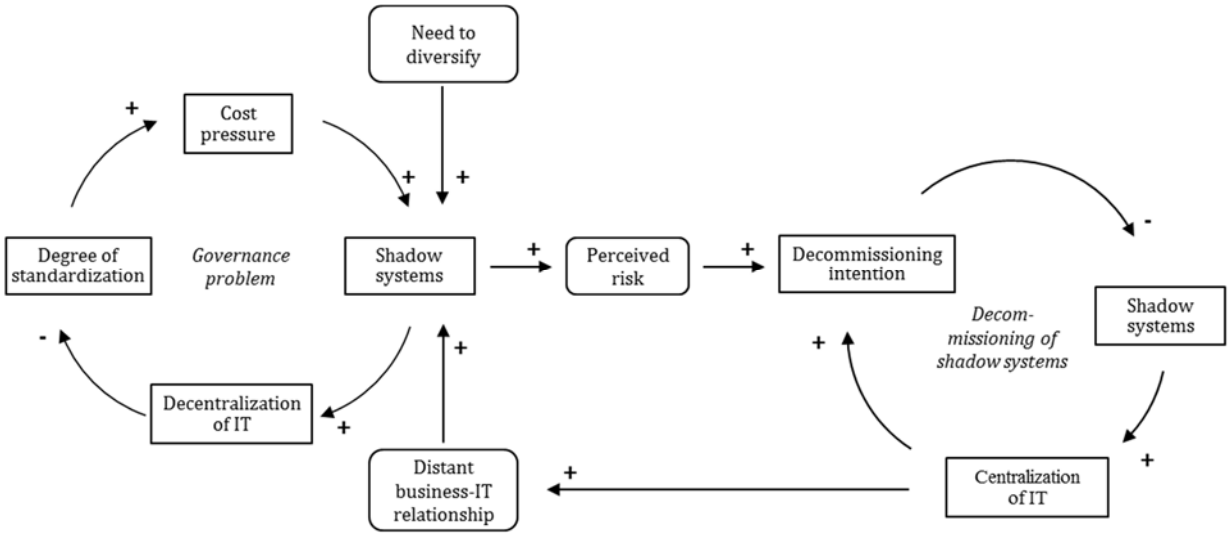

Figure 3. Counteracting Forces Toward and Away from Shadow Systems

The senior management of Savings Bank tried to counter the "governance problem" by means of an IT compliance program. However, the data suggests that shadow systems remained attractive because the problems mentioned (lack of business knowledge of IT and lack of trust) persisted. The central IT authority had insufficient power to regain full control and to stop the business units (e.g., trading, treasury, back office) from increasingly using shadow systems. Thus, in the time that senior management required to

strengthen central IT and to decommission shadow systems, the business units still had opportunities to create new shadow systems.

In summary, we found two counteracting forces: a “governance problem” and a “decommissioning of shadow systems” cycle. A regulating effect connects both forces whereby a weakening is triggered by increasing perceived risk and a rebound by an increasing distance between business and IT.

4.4 Case Discussion

Based on our data, we can conclude that, had Savings Bank strengthened the relationship between business units and IT (Sambamurthy & Zmund, 1999), bridged the knowledge gap between them (Tiwana, 2009), and sped up some development processes of central systems (György et al., 2012), it could have reduced the influx of new shadow systems. Contrary to Haag and Eckhardt (2014b) and others, this point does not concern the deviation from IT policies. Instead, it refers to shorter realization cycles (György et al., 2012) and faster decision making in IT boards (Weill & Ross, 2004). We can also speculate about the importance of enhanced communication between business units and IT as a means to improve alignment (Karpovsky & Galliers, 2015). By doing so, the company may have dampened the reinforcing cycle that increased the number of non-official systems and could have corrected it in a way so that the “decommissioning” cycle showed greater effects. Another strategy could have been to channel the need for non-standardized solutions by legitimizing reasonable exceptions to existing standards (Weill & Ross, 2004).

5 Summary and Outlook

5.1 Summary

In this paper, we address how shadow systems affect the power balance in organizations. Based on a case study of a financial institute, we observed two counteracting tendencies. First, our findings show that shadow systems strengthen the power base of end users and business units by giving them an effective means to perform their own workflows. As a result, the central IT unit gradually loses power because it has less and less context-specific business knowledge. In turn, the business units perceive it as a less and less relevant partner. We use the term “governance problem” to label this process. However, IT units may counteract the “governance problem” by exploiting the fact that shadow systems are often vulnerable to risks because they contain errors and feature unsystematically created designs. Thus, one may see formal risk-management programs as means for a central IT unit to regain power by constructing risks (that may have not been obvious before), which leads to the decommissioning of shadow systems. Both cycles concur, and, at times, one tendency may surpass the other. However, the impetus from formal programs may not be sufficient to stop the shadow system cycle if they do not address the underlying causes for why shadow systems emerge in the first place.

These findings are relevant for research on shadow IT because they highlight a long-term perspective on shadow IT. We draw attention to cyclic trends that favor the continued emergence and decline of shadow systems instead of the dominant view that focuses on a single system lifecycle perspective (e.g., Behrens 2009) and short-term governance interventions (e.g., Zimmermann et al. 2014). Not unlike other authors that have portrayed power struggles related to shadow systems (Kerr et al., 2007; Lyytinen & Newman, 2015; Spierings et al., 2012), we argue for the importance of considering coalitions of actors in attempts to understand their rise and fall. Yet, existing work has tended to look at shadow systems as a by-product of specific, focused initiatives (e.g., ERP implementations), and we add to this literature the insight that shadow systems go beyond single initiatives. We highlight the cyclic nature of shadow systems that constantly evolve and vanish in multiple areas of an organization. Moreover, we portray risk as a way in which the central IT department puts pressure on the organization and as a power-shifting construct.

5.2 Limitations and Future Directions

Before we discuss our study’s implications for broader lines of IS theory and practice, we emphasize three conditions that limit our findings’ generalizability. First, we conducted our study in the financial services industry, which affects the proposed theoretical relationships. Although we present reasonably general drivers for why shadow systems emerge, our model assumes that the company seeks profit and operates in a knowledge-intensive setting. These assumptions may be too restrictive in some industries and public organizations. However, we believe that they characterize one important mode of doing business in the

contemporary world. Second, we studied only one mid-sized bank. By doing so, we focused on a specific set of structural conditions. In particular, we studied a firm where IT and business units were clearly delineated. This assumption may be too restrictive for small organizations without a full-blown IT department. Moreover, for large corporations, a multi-tier model of the IT function may be useful (Winkler & Brown, 2014). Such a model could consider the possibility that one IT unit balances resource bottlenecks of another unit, thereby mediating the link between cost pressures and shadow systems. Our view may also be limited with respect to firms with more federal structures (see Sambamurthy & Zmund, 1999). Third, we collected a limited number of interviews and observations, and further data collections could add an interdepartmental perspective to power struggles that our study does not feature. More data could also shed further light on the motives of why individuals create shadow systems; for example, whether they intentionally create shadow systems as an instrument to amplify their own power by controlling information flows (Markus, 1983). In the context of a multinational cooperation, this behavior is known as “empire building” (Mandell, 1975; Roche, 1992). As Davenport, Eccles, and Prusak (1998) note, local actors (e.g., middle managers in different departments) could use their “information empires” in politics against each other and senior management. On a different note, future research could quantify the proposed cycles (e.g., with system dynamics) to observe cycle times and to achieve measurability.

5.3 Theoretical Implications

Our findings have broader implications for the debate on IT governance (Andriole, 2015; Tiwana & Konsynski, 2010; Tiwana et al., 2013; Weill & Ross, 2004). As a consequence of the underlying tension between responsiveness and scale (Brown & Magill, 1994; Sambamurthy & Zmund, 1999), organizations tend to oscillate between centralized and decentralized forms of organizing IT (King, 1983; Winkler & Brown, 2014). We add nuance to the debate on cyclic trends in IT governance by illustrating how managerial actions that aim to reduce costs and help firms become more competitive can overshoot and result in a “governance problem”, which advances our understanding of the mechanisms that create misalignment between business and IT. In particular, we identify shadow systems as part of a vicious circle and as an unintended, emergent consequence of continued cost and time pressures. We further add to the debate by positioning risk as a power-shifting construct and show that deliberate risk-management programs might be insufficient to effectively weaken the vicious circle. To prevent a continuous expansion of shadow systems, we advocate for the importance of building decent working relationship between business and IT as a means to enhance “operational” alignment (Gerow et al., 2014).

5.4 Practical Implications

Practically, we show that organizational programs to discontinue shadow systems often fail to achieve their goals if they do not solve the underlying communication or governance problem. The governance problem arises as a consequence of a cultural distance between business units and IT. In consequence, organizational programs and management interventions may temporarily weaken the cycle in which new shadow systems emerge, but they do not stop it from spinning, which is important because it contradicts the widely held belief that prohibition is “the most effective action to guarantee the protection of the organizational IT assets” (Haag & Eckhardt, 2014b, p. 1). Studies on shadow systems often advise organizations to acknowledge and address the risks that they bring (Silic & Back, 2014; Walters, 2013). They have also suggested valuable procedures to identify and reduce the number of shadow systems (Zimmermann & Rentrop, 2014; Zimmermann et al., 2014). Yet, we show that such measures do not develop their full potential if they do not address the underlying causes for why shadow systems emerge. Based on our findings, we suggest that organizations could do better by providing end users appropriate channels to translate their ideas into practice. Further, we believe that organizations should flank shadow systems campaigns with investments in relationship building (or bypassing it by building multidisciplinary teams). We are eager to see whether organizations pick up on these ideas in the future.

Acknowledgements

We are indebted to the responsible editors and the two anonymous reviewers for their thoughtful guidance. Furthermore, we thank participants at the 22nd Americas Conference on Information Systems (AMCIS) in San Diego, CA, for their helpful comments. An earlier and less-developed version of the manuscript was published in the AMCIS 2016 Proceedings. Daniel Furstenau is thankful for financial support by Freie Universität Berlin in the Excellence Initiative of the German Research Foundation (DFG).

References

Alter, S. (2014). Theory of workarounds. *Communications of the Association for Information Systems*, *34*, 1041-1066.

Andriole, S. J. (2015). Who owns IT? *Communications of the ACM*, *58*(3), 50-57.

Behrens, S. (2009). Shadow systems: The good, the bad and the ugly. *Communications of the ACM*, *52*(2), 124-129.

Berente, N., & Yoo, Y. (2012). Institutional contradictions and loose coupling: Postimplementation of NASA's enterprise information system. *Information Systems Research*, *23*(2), 376-396.

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective, part II: The application of theory. *MIS Quarterly*, *1*(4), 11-28.

Bothner, M. S., Smith, E. B., & White, H. C. (2010). A model of robust positions in social networks. *American Journal of Sociology*, 1*16*(3), 943-992.

Brown, C. V., & Magill, S. L. (1994). Alignment of the IS functions with the enterprise: Toward a model of antecedents. *MIS Quarterly*, *18*(4), 371-403.

Burton-Jones, A., McLean, E. R., & Monod, E. (2015). Theoretical perspectives in IS research: From variance and process to conceptual latitude and conceptual fit. *European Journal of Information Systems*, *24*(6), 664-679.

Coltman, T., Tallon, P., Sharma, R., & Queiroz, M. (2015). Strategic IT alignment: Twenty-five years on. *Journal of Information Technology*, *30*(2), 91-100.

Cropanzano, R., Howes, J. C., Grandey, A. A., & Toth, P. (1997). The relationship of organizational politics and support to work behaviors, attitudes, and stress. *Journal of Organizational Behavior*, *18*(2), 159-180.

Davenport, T. H., Eccles, R. G., & Prusak, L. (1998). Information politics. In D. A. Klein (Ed.), *The strategic management of intellectual capital* (pp. 101-120). Boston, USA: Butterworth-Heinemann.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, *14*(4), 532-550.

Foucault, M. (1995). *Discipline & punish: The birth of the prison*. London, UK: Penguin Books.

Furneaux, B., & Wade, M. (2011). An exploration of organizational level information systems discontinuance intentions. *MIS Quarterly*, *35*(3), 573-598.

Fürstenau, D., & Rothe, H. (2014). Shadow IT systems: Discerning the good and the evil. In *Proceedings of the European Conference on Information Systems.*

Fürstenau, D., Sandner, M., & Anapliotis, D. (2016). Why do shadow systems fail? An expert study on determinants of discontinuation. In *Proceedings of the European Conference on Information Systems.*

Gaß, O., Ortbach, K., Kretzer, M., Maedche, A., & Niehaves, B. (2015). Conceptualizing individualization in information systems–a literature review. *Communications of the Association for Information Systems*, 37, 64-88.

George, J. F., & King, J. L. (1991). Examining the computing and centralization debate. *Communications of the ACM*, *34*(7), 62-72.

Gerow, J. E., Grover, V., Thatcher, J., & Roth, P. L. (2014). Looking toward the future of IT-business strategic alignment through the past: A meta-analysis. *MIS Quarterly*, *38*(4), 1159-1185.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods*, *16*(1), 15-31.

Gozman, D., & Willcocks, L. (2015). Crocodiles in the regulatory swamp: Navigating the dangers of outsourcing, SaaS and shadow IT. In *Proceedings of the International Conference on Information Systems.*

Gregory, R. W., Keil, M., Muntermann, J., & Mähring, M. (2015). Paradoxes and the nature of ambidexterity in IT transformation programs. *Information Systems Research*, *26*(1), 57-80.

György, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. In *Proceedings of the International Conference on Information Systems.*

Haag, S., & Eckhardt, A. (2014a). Normalizing the shadows—the role of symbolic models for individuals' shadow IT usage. In *Proceedings of the International Conference on Information Systems.*

Haag, S., & Eckhardt, A. (2014b). Sensitizing employees' corporate IS security risk perception. In *Proceedings of the International Conference on Information Systems.*

Haag, S., Eckhardt, A., & Bozoyan, C. (2015). Are shadow system users the better IS users ? Insights of a lab experiment. In *Proceedings of the International Conference on Information Systems.*

Hauke, G. (2006). Values in strategic brief therapy: From need to value-directed living. *European Psychotherapy*, *6*(1), 77-115.

Henrich, J., & Gil-White, F. J. (2001). The evolution of prestige: Freely conferred deference as a mechanism for enhancing the benefits of cultural transmission. *Evolution and Human Behavior*, *22*(3), 165-196.

Jasperson, J., Carte, T. A., Saunders, C. S., Butler, B. S., Croes, H. J. P., & Zheng, W. J. (2002). Review: power and information technology research: A metatriangulation review. *MIS Quarterly*, *26*, 397-459.

Jones, D., Behrens, S., Jamieson, K., & Tansley, E. (2004). The rise and fall of a shadow system: lessons for enterprise system implementation. In *Proceedings of the Australasian Conference on Information Systems.*

Karpovsky, A., & Galliers, R. D. (2015). Aligning in practice: From current cases to a new agenda. *Journal of Information Technology*, *30*(2), 136-160.

Kerr, D. V., Houghton, L., & Burgess, K. (2007). Power relationships that lead to the development of feral systems. *Australasian Journal of Information Systems*, *14*(2), 141-152.

King, J. L. (1983). Centralized versus decentralized computing: Organizational considerations and management options. *ACM Computing Surveys*, *15*(4), 319-349.

Koopman, P., & Hoffman, R. R. (2003). Work-arounds, make-work, and kludges. *IEEE Intelligent Systems*, *18*(6), 70-75.

Kopper, A., & Westner, M. (2016). Towards a taxonomy of shadow IT. In *Proceedings of the Americas Conference on Information Systems.*

Leon, L. A., Abraham, D. M., & Kalbers, L. (2010). Beyond regulatory compliance for spreadsheet controls: a tutorial to assist practitioners and a call for research. *Communications of the Association for Information Systems*, *27*, 541–560.

Levina, N., & Orlikowski, W. (2009). Understanding shifting power relations within and across organizations: A critical genre analysis. *Academy of Management Journal*, *52*(4), 672-703.

Lyytinen, K., & Newman, M. (2015). A tale of two coalitions—marginalising the users while successfully implementing an enterprise resource planning system. *Information Systems Journal*, *25*(2), 71-101.

Madill, A., Jordan, A., & Shirley, C. (2000). Objectivity and reliability in qualitative analysis: Realist, contextualist and radical constructionist epistemologies. *British Journal of Psychology*, *91*(1), 1-20.

Maguire, S., & Hardy, C. (2013). Organizing processes and the construction of risk: A discursive approach. *Academy of Management Journal*, *56*(1), 231-255.

Markus, M. L. (1983). Power, politics, and MIS implementation. *Communications of the ACM*, *26*(6), 430-444.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709-734.

Mandell, S. L. (1975). The management information system is going to pieces. *California Management Review*, *17*(4), 50-56.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology* (No. 800-145). Gaithersburg, MD.

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook (2nd ed.). Thousand Oaks, CA: Sage.

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *IT Professional*, *14*(5), 53-55.

Müller, S. D., Holm, S. R., & Søndergaard, J. (2015). Benefits of cloud computing: Literature review in a maturity model perspective. *Communications of the Association for Information Systems*, 37, 851-878.

Nwankpa, J. K., & Roumani, Y. (2014). The influence of organizational trust and organizational mindfulness on ERP systems usage. *Communications of the Association for Information Systems*, *34*, 1469-1492.

Panko, R. R. (2006). Spreadsheets and Sarbanes-Oxley: Regulations, risks, and control frameworks. *Communications of the Association for Information Systems*, *17*, 647-676.

Perlow, L. A. (1999). The time famine: Toward a sociology of work time. *Administrative Science Quarterly*, *44*(1), 57-81.

Pfeffer, J. (1981). *Power in organizations*. Marshfield, MA: Pitman.

Power, M. (2007). *Organized uncertainty: Designing a world of risk management.* New York, NY: Oxford University Press.

Raden, N. (2005). *Shedding light on shadow IT: Is Excel running your business?* Santa Barbara, CA: Hired Brains.

Rains, J. (2015). *Shadow IT: The impact on technical support and the opportunities for IT*. Retrieved from http://www.informationweek.com/whitepaper/it-strategy/it-leadership/shadow-it:-the-impact-on-technical-support-and-the-opportunities-for-it/360263

Roche, E. M. (1992). *Managing information technology in multinational corporations*. Barraclough.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393-404.

Sambamurthy, V., & Zmund, R. W. (1999). Arrangements for information technology governance: A Theory of Multiple Contingencies. *MIS Quarterly*, *23*(2), 261-290.

Silic, M., & Back, A. (2014). Shadow IT—a view from behind the curtain. *Computers and Security*, *45*, 274-283.

Silva, L., & Backhouse, J. (2003). The circuits-of-power framework for studying power in institutionalization of information systems. *Journal of the Association for Information Systems*, *4*(6), 294-336.

Spierings, A., Kerr, D., & Houghton, L. (2012). What drives the end user to build a feral information system? In *Proceedings of the Australasian Conference on Information Systems.*

Strong, D., Volkoff, O., & Elmes, M. (2001). ERP systems, task structure, and workarounds in organizations. In *Proceedings of the Americas Conference on Information Systems.*

Tanriverdi, H. (2005). Information technology relatedness, knowledge management capability, and performance of multibusiness firms. *MIS Quarterly*, *29*(2), 311–334.

Tiwana, A. (2009). Governance-knowledge fit in systems development projects. *Information Systems Research*, *20*(2), 180-197.

Tiwana, A., & Konsynski, B. (2010). Complementarities between organizational IT architecture and governance structure. *Information Systems Research*, *21*(2), 288-304.

Tiwana, A., Konsynski, B., & Venkatraman, N. (2013). Information technology and organizational governance: The IT governance cube. *Journal of Management Information Systems*, *30*(3), 7-12.

Walters, R. (2013). Bringing IT out of the shadows. *Network Security*, 2013(4), 5-11.

Weick, K. E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative Science Quarterly*, *38*(4), 628-652.

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Boston, MA: Harvard Business Press.

Williams, R., & Pollock, N. (2012). Moving beyond the single site implementation study: How (and why) we should study the biography of packaged enterprise solutions. *Information Systems Research*, *23*(1), 1-22.

Winkler, T. J., & Brown, C. V. (2013). Horizontal allocation of decision rights for on-premise applications and software-as-a-service. *Journal of Management Information Systems*, *30*(3), 13-48.

Winkler, T. J., & Brown, C. V. (2014). Organizing and configuring the IT function. In H. Topi & A. Tucker (Eds.), *Computing handbook* (3rd ed., pp. 57.1–57.14). Boca Raton, FL: Taylor & Francis.

Winter, S., Berente, N., Howison, J., & Butler, B. (2014). Beyond the organizational "container": Conceptualizing 21st century sociotechnical work. *Information and Organization*, 24(4), 250-269.

Xue, Y., Liang, H., & Boulton, W. R. (2008). Information technology governance in information technology investment decision processes: The impact of investment characteristics, external environment, and internal context. *MIS Quarterly*, *32*(1), 67-96.

Yin, R. K. (2013). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage.

Zimmermann, S., & Rentrop, C. (2014). On the emergence of shadow IT—a transaction cost-based approach. In *Proceedings of the European Conference on Information Systems.*

Zimmermann, S., Rentrop, C., & Felden, C. (2014). Managing shadow IT instances—a method to control autonomous IT solutions in the business departments. In *Proceedings of the Americas Conference on Information Systems.*

Appendix A: Interview Guide (Excerpt)

- Present interviewee our definition of shadow systems
- Introductory questions (current position, relation to shadow systems in current position)
- Part A: Focus on one specific example (e.g., critical, revelatory)
  - How did the system emerge?
  - How did the system grow (capabilities; scope of use; financial and technical embeddedness)?
  - What challenges and tensions occurred?
  - Is the system still operational and, if not, what happened to the system?
- Part B: General observations
  - Is this a specific or a typical example (what makes it so)?
  - What other important points come to your mind when reflecting on this topic?
- Part C: Relationship business–IT
  - Can you describe the central IT's position/strategies with respect to shadow systems?
  - Can you describe the control that you [as business unit] have to trigger IT developments?
  - Can you describe the distance/closeness between business unit(s) and central IT unit(s)?
- Thanks and concluding remarks

Appendix B

Table B1. Examples for Data Coding as Part of the Conceptualization

Perceived risk	"Of course, because the risk awareness differs.... I think the security requirements are generally the same when it comes to pure banking but as long as it's more sales or just a website, this is often not evaluated as too risky from the institution's point of view." (#11) "The main risk that I see is that data is manipulated in a wrong way…; that you export them from the inventory [to shadow systems] and that you import them back in without proper testing and that then things go wrong." (#12) "The major reason, why such [shadow] systems disappear is because their sustained use would be by far too risky." (#5)
Distant BIT relationship (Lack of business knowledge)	"Some colleagues just don't have the time or patience to pursue the official path…. They don't want IT on board as IT lacks the knowledge and as it takes them too long to explain it to them." (#7) "The second reason would have been the missing agility and a lack of knowledge from the site of IT. Central IT wouldn't been able to implement this idea quickly." (#3)
Distance BIT relationship (Lack of trust in abilities)	"A few colleagues maybe had special know how, which central [IT] does not at all possess." (#5) "Central IT would not have been able to implement this idea quickly." (#2)
Need to diversify	"There was no solution available in the market which met the requirements of the division." (#1) "It happened because there was so much pressure. If you look at large sales units with private or business customers, they need to work on huge databases following an appropriate timeframe to create reports for executives." (#7)
Cost pressure	"There is a reason; costs need to be cut in all areas. Indeed, the most necessary [systems] has always been held available. But for this reason, self-made [shadow] solutions became more attractive." (#3) "An experienced project manager plans with cost premiums in order to use the remaining budget to finance other, smaller [shadow] projects." (#7) "Basically, that is the way your requirements get to [central IT]. However, this is heavily formalized, resources are scare. Therefore, if someone wants to create something quickly, there is little choice than doing it all by themselves [using shadow systems]." (#11)
Decommissioning intention	"This occurred very often with solutions made by student employees.... These systems stopped working the way they should and we had to turn them off." (#4) "With regards to VBA [visual basic application] or MS Office-based applications I know, that business units still use them as they find the risk to be bearable. IT works flat out on their decommissioning in order to try to bring them under their control." (#1)
Centralization of IT	"When we had two systems running in parallel, we faced situations in which we didn't know who is right and who is wrong. We are a bank that trades real money. These failures cost us a lot of money. That's why I am glad that the control is now with IT: Because we have one more control instance." (#2) "When volumes get big enough, we–as [an internal] service provider–would naturally say: 'ok, offering standardized products is now worth the effort.'." (#11) "Then, in turn, decentralization of IT is reduced; not the content itself, but the technology…. So in the end you only need a supply of content from these externals [business units]." (#11)

About the Authors

Daniel Furstenau is a postdoctoral researcher at the Department of Information Systems at Freie Universität Berlin, Germany. He earned his PhD from Freie Universität Berlin in 2014. He is an active member of the Association for Information Systems and has been a visiting researcher at Copenhagen Business School (Denmark) and University of California, San Diego (US). His research focuses on IT architecture and IT governance,and the intersection of both. His research has been published in proceedings of leading IS conferences such as the International Conference on Information Systems, the European Conference on Information Systems, and the Americas Conference on Information Systems.

Hannes Rothe is an Assistant Professor for Educational Service Engineering and IT Entrepreneurship at Freie Universität Berlin. He earned his PhD from Freie Universität Berlin in 2015. His research interests include educational service engineering, service systems and ecosystems, and shadow IT systems. He also serves as the coordinator of Freie Universität Berlin's entrepreneurship education. His research has been published in *International Journal on E-Learning*, *Proceedings of the Hawaii International Conference on System Sciences*, *Proceedings of the European Conference on Information Systems*, and *Proceedings of the Americas Conference on Information Systems*, among others.

Matthias Sandner has been a member of the work group of Professor Martin Gersch at the Department of Information Systems at Freie Universität Berlin. He earned his MSc in Information Systems in 2016. He is currently serving as a Business/IT consultant at Senacor Technologies. His research interest include IT management and digital innovation. His research has been published in *Proceedings of the European Conference of Information Systems* and *Proceedings of the Americas Conference on Information Systems*.