# Shadow IT, Risk, and Shifting Power Relations in Organizations

*Full paper*

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

**Hannes Rothe**
Freie Universität Berlin
hannes.rothe@fu-berlin.de

**Matthias Sandner**
Freie Universität Berlin
matthias.sandner@fu-berlin.de

**Dimitrios Anapliotis**
Freie Universität Berlin
dimitrios.anapliotis@fu-berlin.de

## Abstract

We draw on notions of power and the social construction of risk to understand the persistence of shadow IT within 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 IT. A distant business-IT relationship, a lack of IT business knowledge and changing business needs can create repeated cost and time pressures that make business units draw on shadow IT. The perception of risk can trigger an opposing power shift back through the decommissioning and recentralization of shadow IT. However, empirical findings suggest that the weakening tendency of formal programs may not be sufficient to stop the shadow IT cycle spinning if they fail to address the underlying causes for the shadow IT emergence. These findings highlight long-term dynamics associated with shadow IT and pose "risk" as a power-shifting construct.

**Keywords**

Shadow IT, Risk, Power Relations, IT Governance

## Introduction

This article concerns the importance of power relations between business units and central IT units to understand the persistence of shadow IT systems within organizations. By shadow IT systems, we refer to autonomous software systems or extensions to existing systems which are neither developed nor controlled by a central IT department (Zimmermann et al. 2014; Fürstenau and Rothe 2014). The term "shadow IT" has increasingly grown in practical and academic attention, fueled by the emergence of cloud computing (Mell and Grance 2011), software-as-a-service (Winkler and Brown 2013), bring-your-own-device (Miller et al. 2012), and other important trends in the technological landscape toward decentralized and user-driven computing innovations (György et al. 2012).

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

Although some organizations explicitly allow *shadow IT* as they believe in its 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 (see for instance Panko 2006).

As the introductory sentence to this section suggests, many organizations fail to eliminate or reduce the amount of shadow IT despite serious attempts and repeated efforts to do so (Rains 2015; Walters 2013). This observation is paradoxical as it suggests that most organizations use more formal risk management tools and still achieve less of the desired outcome (a reduction of shadow IT). Often times, shadow IT persists or returns even though managers have started efforts to eliminate them.

The long-term dynamics that drive the persistence of shadow IT are rarely analyzed in detail. The literature on shadow IT has produced a rich contextual understanding of what shadow IT is and what schemes can be implemented to govern and control shadow IT (Zimmermann and Rentrop 2014; Zimmermann et al. 2014). Yet, it fails to account for the dynamic complexity driving the ongoing rise and fall of shadow IT in contemporary organizations with hundreds and thousands of decentralized devices and systems. It also says relatively little about why many organizations fail to get rid of shadow IT systems. Thus, it tends to overvalue the control that can be exerted by managers and other interest groups to influence the evolution of shadow IT systems in organizations. To analyze the long-term dynamics associated with shadow IT persistence, we draw on theories of power and the social construction of risk. This leads us to the following research question:

*How does shadow IT 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 find support for our view that the emergence and decommissioning of shadow IT is a multi-faceted process that unfolds over time: The simultaneous presence of various factors can trigger a self-reinforcing process in which particular shadow IT systems gain critical importance for an organization. In consequence, the power of the shadow IT organization increases, undermining the control of the central IT unit. We label this tendency as "governance problem" because it results in a void in the exercise of decision rights and an increasing imbalance in favor of decentralized goals and priorities. In consequence, the IT landscape drifts apart. Managerial attempts to eliminate shadow IT systems by constructing them as a "risk" may then run dry and the inflow of shadow IT continues as the underlying governance problem persists.

To arrive at these contributions, this article is organized as follows: Section 2 introduces the theoretical and conceptual background. In section 3, we refer to the methods of this study. Section 4 presents results. Section 5 summarizes the findings and discusses implications and future research opportunities.

## Conceptual Background

***Shadow IT is a sociotechnical phenomenon.*** Our starting point is the observation that organizational work systems consist of individuals and organizational structures contributing to the success of technical solutions. According to this view, social (human and organizational) elements and technical systems are deeply "intertwined in complex webs of mutual causality" (Winter et al. 2014, p. 253). This is known as the sociotechnical systems view (Bostrom and Heinen 1977; Winter et al. 2014).

We contend that shadow IT must be understood as a sociotechnical phenomenon. Firstly, research on shadow IT shows that individuals are key for establishing a shadow IT system. Understanding their intentions and motivations is thus central (Haag et al. 2015). Shadow IT can help individuals to work around the limitations of existing organizational systems or processes (Alter 2014; Strong et al. 2001). In addition, shadow IT is often more readily available, more cost-effective, and assessed as being easier-to-use than central systems (György et al. 2012). Secondly, over time, establishing organizational structures and processes becomes more important for the survival of a shadow IT system. Without proper support, a shadow IT system stays small and shallow (Behrens 2009). The "hit-by-a-bus" scenario (Behrens 2009) describes a situation in which business processes supported by a shadow IT system are threatened as key individuals leave the organization. Thus, sustainable support structures for shadow IT systems are seen as vital by some scholars (Zimmermann et al. 2014). Taken all together, we can see the importance of *both realms,* the technical and the social, to understand the phenomenon of shadow IT.

***Shadow IT affects power relations in organizations.*** One important implication from taking a sociotechnical perspective on organizational work systems is that shadow IT must be viewed as an instrument of power and a mechanism to influence power relations (see also Spierings et al. 2012). By power, we refer to a personal value that describes an individual's ability to exert influence (Hauke 2006).

Power is usually associated with related concepts such as "social status" (Bothner et al. 2010), "prestige" (Henrich and Gil-White 2001), and a feeling of control and dominance. Power relations affect the actions taken by individuals in groups and organizations (Weick 1993). In particular, a feeling of control can be used to trigger others' action by drawing on direct command, strategic manipulation and politics, or techniques of observation and anticipatory obedience (Foucault 1995). For long, power has been a central theme in the IS literature (Jasperson et al. 2002; Markus 1983) and we have learnt from many studies that IT tends to reinforce the existing power base in organizations. 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 IT—as a form of decentralized computing by individual users, work groups, and business units—is subject to power struggles as it potentially changes 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 IT systems. According to her view (p. 128), "shadow systems are exposed to a greater depth and range of politics than formal systems".

Based on this reasoning, our starting point is the observation that shadow IT will often emerge if a business unit does not perceive the ability (has the power) to influence the actions taken by a central IT department to fulfill its demands. Prior research indicates that this inability may arise if the official IT unit lacks resources (see Winkler and Brown 2014), business knowledge (see Tiwana 2009; Winkler and Brown 2013), or agility (see György et al. 2012). Thus, the central IT "refuses" to act and shadow IT appears as a "quick fix" or "workaround" (Alter 2014) enabling action. A consistent explanation to this pattern—yet, one that is absent in the literature—is that the central IT is dominated by another business unit (or senior manager) that becomes a "preferred partner". 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 IT. In particular, shadow IT is oftentimes a reaction to novel business needs (Behrens 2009; Jones et al. 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 and Orlikowski 2009). Moreover, the inherent ambiguity of novel situations creates openings for the reconfiguration of power relations (Levina and Orlikowski 2009). Whereas many shadow IT systems start as small systems with a limited user base and a narrow scope, these systems grow over time as the functional scope or the number of stakeholders expand. This will, in turn, again challenge existing power relations in organizations. Shadow IT 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 IT.

***Shadow IT as a "risk" that can shift power relations.*** In consequence of a growing importance of shadow IT, 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 2009). Shadow IT brings many challenges for security and privacy (Silic and Back 2014) and IT governance (Zimmermann et al. 2014). Risks arise, for instance, from single person reliance (Behrens 2009), poor code quality, design, and documentation (Raden 2005), errors and fraud (Panko 2006), poor architectures (Fürstenau and Rothe 2014), and vendor-related issues (Furneaux and Wade 2011; Tanriverdi 2005). Thus, shadow IT systems may be more susceptible to contextual changes such as organizational or IT transformations (Behrens 2009; Gregory et al. 2015). If shadow IT becomes a risk it may be easier to argue for its decommissioning or recentralization. Thus, our argument is that the depiction of shadow IT as a risk can be an instrument of the central IT to regain power by recentralizing computing resources.

***Summary.*** We put forward three arguments. First, we contended that shadow IT affects the power relations between a business unit creating shadow IT and the central IT, as well as between business units (in the empirical analysis, we focus on the first relationship). Second, we argued that power relations shift over time with the rise and fall of shadow IT systems. Third, we argued that the construction of shadow IT as a risk can be a way for the central IT to regain power. However, to date we have little systematic knowledge on the way in which these factors interact *over time* and how shadow IT actually *changes* the existing power relations in organizations. Yet, a more systematic understanding of the dynamic interaction

between shadow IT, 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 et al. 2015; Gerow et al. 2014; Tiwana et al. 2013) and may also shed light on why shadow IT persists or returns despite repeated efforts to eliminate it.

# Methods

***Case context.*** To address our research question on the relation of shadow IT, risk, and power in organizations, we conducted a qualitative single case study (Yin 2013) in a mid-sized German bank which we anonymize as Savings Bank. A case method was appropriate to the study because it allowed to explore the phenomenon in a real-world context and to inform theory-building efforts. The banking industry was selected because of the importance to balance risks associated with shadow IT in a highly-regulated environment with the need for innovation in a competitive market. 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 Panko 2006). On the other hand, direct banking and the internet put increased pressure on established institutes creating resource scarcity and thus potential power struggles. The case company was founded in 1848 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 the investment banking was outsourced to another institute. During this process, the bank delayed 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 IT systems.

***Data collection.*** Data was collected from interviews, observations, and archive material. We conducted 8 semi-structured interviews over a 4-month period in 2015 (see Table 1). To balance opposing views, we consulted experts from both the business units and IT, among them *shadow IT developers*, *users*, and *IT governance* roles. Their company experience ranged from 6 to 25 years. Interviews lasted between 45 and 60 minutes. All interviews were tape-recorded and transcribed. In addition, one of the authors had several years of working experience with the institute (2012-2014) and was able to leverage this first-hand experience. As a business unit employee, he participated in numerous workshops and meetings where questions regarding specific shadow IT systems were discussed. We triangulated the data by a range of internal and external documents, e.g. system documentations and architecture plans.

| No. | Area | Role | Exp. (years) |
|---|---|---|---|
| #1 | Treasury | Developer | 21 |
| #2 | Trading | Developer / user | 8 |
| #3 | Trading | Developer / user | 19 |
| #4 | Back Office | User | 12 |

| No. | Area | Role | Exp. (years) |
|---|---|---|---|
| #5 | Treasury | User | 6 |
| #6 | IT strategy | IT governance | 25 |
| #7 | Management | IT governance | 11 |
| #8 | Management | IT governance | 10 |

**Table 1. Expert interviews**

***Data analysis.*** Following established approaches in qualitative data analysis (Miles and Huberman 1994), we analyzed the data in several steps. First, we identified factors driving the emergence and discontinuation of shadow IT in the case company. To do so, we developed a coding scheme based on existing theoretical constructs (Figure 1-3 show results). We refined the scheme further in an "abductive" process (Gioia et al. 2012) drawing on empirical insights. To gain in-depth empirical insights, we developed case stories for two shadow IT systems. The stories serve as information system biographies (Williams and Pollock 2012) shedding light on the entire lifecycle of the systems. Based on these materials, we prepared feedback loop diagrams (Perlow 1999) to abstract from our empirical insights and synthesized these into a graphical model. The resulting model is supposed to add theory building (Eisenhardt 1989) as it establishes relationships between theoretical constructs which have not been expressed previously (Burton-Jones et al. 2015).

# Results

This section presents results. We first introduce two feedback cycles regarding the emergence and discontinuation of shadow IT. Then, we integrate these cycles and discuss their interrelationship.

***Emergence of shadow IT and the governance problem.*** Our data confirmed that several reasons existed why shadow IT appeared in the case company. Table 2 summarizes them. A prerequisite was the company's lax compliance policy. The company did not restrict the extension of Microsoft Excel or Access by Macros, which let many users consider this alternative as it was readily available.

These reasons, as listed in Table 2, typically occurred in combination. To illustrate this, we draw from an example of a shadow IT system for market data delivery which we anonymize as "order book tool". The order book tool was introduced by the treasury department. It was built to process market data and place automatic orders. The first important reason for the emergence of the system was the *necessity to diversify* the product portfolio in a competitive market place. For instance, the order book tool promised to speed up the delivery process of market data by several milliseconds providing an edge over the market. One of the shadow IT developers (#1) 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". A second reason for the emergence of shadow IT systems in general and the order book tool in particular was *lacking business knowledge of the central IT unit*. At first, a solution from central IT was taken into consideration. Yet, it was rejected as the business unit in which the demand emerged assumed that the central IT lacked relevant knowledge. Furthermore, time-to-delivery was too long. For instance, one IT employee (#6) noted that "some colleagues just don't have the time or patience to pursue the official path … they don't want IT onboard as IT lacks the knowledge and as it takes them too long to explain it to them". Finally, several interviewees confirmed that a *distant relationship* between the business unit and central IT was an important driver for the emergence of shadow IT. As an example, we refer to the observation that central IT was located in a building separate from the business units. The business units were also reserved to negotiate with central IT. For instance, the same employee from the central IT (#6) 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 together 'business' and 'IT' 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 IT in the case company was a complex process in which the need to diversify, lacking business knowledge of IT, and a distant business-IT relationship formed jointly the reason for the emergence of a shadow IT system.

| Reason | Explanation | # Interviewees |
|---|---|---|
| Lacking business knowledge of IT | The tasks of business units require context-specific business knowledge that was often not available in the IT department | 6 |
| Distant business-IT relationship | The business units feel that the central IT is 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 offered by IT were perceived as too expensive (in comparison to shadow IT); often they did not fit the business unit budget | 3 |

**Table 2. Reasons for emergence of shadow IT at Savings Bank**

The emergence of shadow IT started a vicious circle spinning which we refer to as the "governance problem", depicted in Figure 1. As expected from the sociotechnical view, the growth of shadow IT was triggering a need for support and maintenance personnel. This need was fulfilled by internal employees and by contracting external parties. For instance, the order book tool was operated by power users within the treasury department and by contracting external IT consultants. Another shadow IT system within the

treasury department, an algorithmic trading system, was maintained by business unit employees and temporary staff. With the increasing number of shadow IT systems and with higher levels of technical skills as well as emotional attachment to them within business units, shadow IT grew in importance and criticality. The *decentralization of IT* followed as a direct consequence. It resulted in a subtle loss of central IT power. Thus, the business unit was getting in a better position to justify further investments and the central IT unit 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 weakens the central IT's ability to exercise control over applications and to align them with the company's overall goals and directives (Weill and Ross 2004), leading to a void that is filled by decentralized units without paying full attention to overarching goals and priorities. As Fürstenau and Rothe (2014), we could see that this leads to a declining degree of standardization and increasing fragmentation in the entire IT landscape. This in turn resulted in increasing costs pressures as the company failed to fully exploit cost synergies and scope effects across units (Tanriverdi 2005). These cost pressures, again, reinforced the trend toward shadow IT because they favored managerial actions to withdraw further resources from the central IT unit.

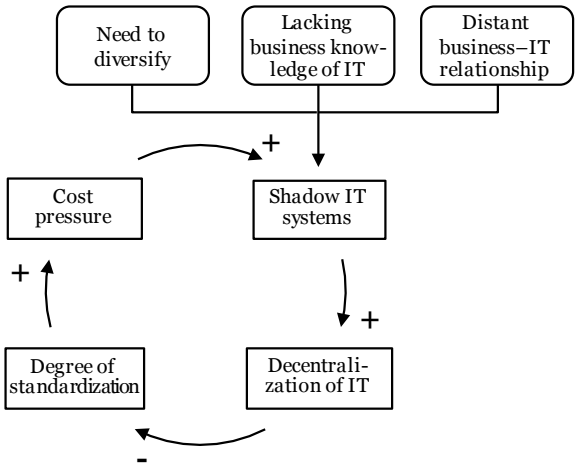


**Figure 1. The emergence of shadow IT and the governance problem**

***Decommissioning of shadow IT.*** While there was constant pressure to create new shadow IT to fulfill the demand for innovative and more advanced solutions, another trend counteracted the tendency toward shadow IT. We call this feedback loop "decommissioning of shadow IT", depicted in Figure 2.

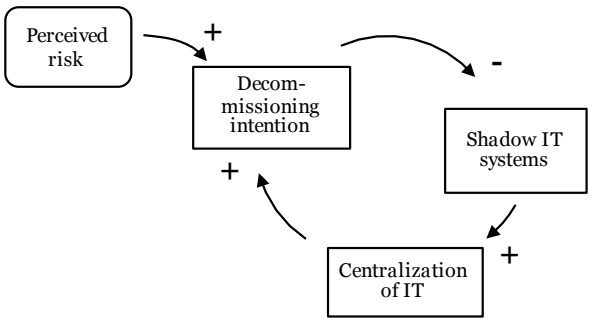


**Figure 2. Decommissioning of shadow IT**

A *perception of increased risk* initiates this cycle. The perception emerged primarily at a senior management level and was passed on to central IT unit as a result of two factors. At first, financial supervisory authorities imposed new regulations on the institute which increased reporting and risk management obligations. Consistent with a view that risks become constructed (Power 2009; Maguire and Hardy 2013), we observed that this directed attention to shadow IT suffering from "severe" system-related problems such as poor design and architecture, missing documentation, reliance on single persons, and vendor-related

issues. For instance, the shadow IT developer of the order book tool (#6) 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". Secondly, the attentiveness to risks also increased with the organizational restructuring. For instance, when the treasury department was outsourced to another company, the order book tool and the algorithmic trading tool were undergoing a risk assessment. The algorithmic trading tool became decommissioned as it suffered from an overloaded server and as it was lacking documentation and reliable support. An informant (#3) stated: "Coming to think of it, the system was doing what it was supposed to do but it was not extendible 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 as it was critical to the organization, it was relocated to central IT governance.

Senior management facilitated a regain of central IT power and restricted shadow IT by four measures. (1.) The company set up a formal IT compliance policy introducing rules and procedures intended to limit and control the amount of shadow IT. For instance, business units were requested to report their business-developed systems once a year in a repository that was administered by the central IT. Thus, an increase in the centralization of IT led to an increase in the alertness to and provided resources for an advancement of methods to make shadow IT systems visible and quantify the risks associated to them, which in turn created confidence in the proposition that it was legitimate or even necessary to decommission them; therefore, as shown in Figure 2, an increase in IT centralization created pressure to decommission (or centrally govern) existing shadow IT instances as well as diseconomies to create new shadow IT systems. One of the shadow IT developers of the order book tool (#2) 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". (2.) The company appointed process owners. They became responsible for all IT systems being used within the processes increasing the level of central control. (3.) Management also cut the number of official IT locations. An IT employee (#6) 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". Finally, (4.) senior management also pared-down IT-budgets of business units to tighten controls and to restrict the usage of shadow IT.

***Counteracting tendencies toward and away from shadow IT.*** As summarized in Figure 3, we found two counteracting forces: On the left, a trend *toward* shadow IT—expressing a reinforcing need for non-standardized solutions that provide an edge over the market—and, on the right, a weakening tendency *away from* shadow IT—triggered by the perception of risks that results from an increased emphasis of compliance and governance in contemporary organizations.

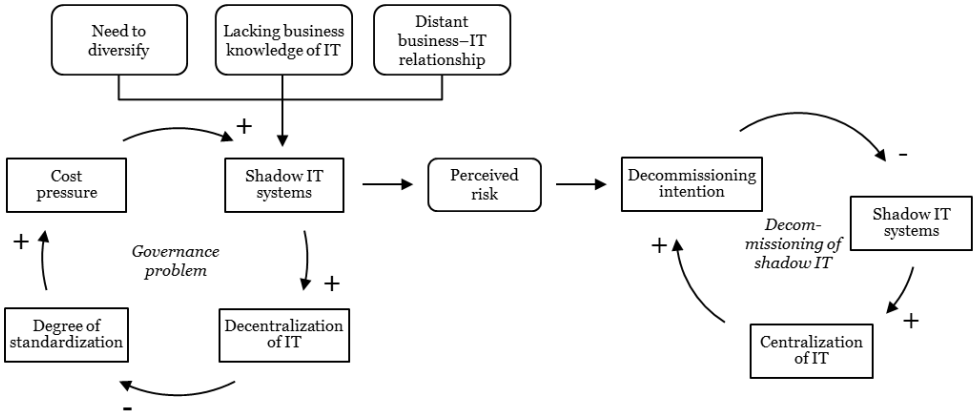


**Figure 3. Counteracting forces toward and away from shadow IT**

In the case company, a natural reaction was to tackle the "governance problem" by introducing an IT compliance program. Yet, the data suggests that existing pressure and knowledge deficits of the central IT were so dominant that the attractiveness of shadow IT continued and the governance problem was not

resolved effectively. The mistrust between central IT and business unit also persisted. The central IT authority was insufficient to regain full control and to stop the trend toward shadow IT. Thus, within the time that was required to strengthen central IT and to decommission shadow IT, there were still opportunities to create new shadow IT solutions.

***Case discussion.*** Based on our data, we can conclude that strengthening the relationship between business units and IT (Sambamurthy and Zmund 1999), bridging the knowledge gap (e.g., by the means of multidisciplinary teams; Tiwana 2009), and speeding up some development processes of central systems (György et al. 2012) could have reduced the inflow of new shadow IT in the company. This point does not concern the deviation from IT compliance rules. Instead, it refers to shorter realization cycles (György et al. 2012) and faster decision-making in IT boards (Weill and Ross 2004). We can also speculate on the importance of an enhanced communication between business units and IT as a means to improve alignment (Karpovsky and 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 "de-commissioning"-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 and Ross 2004).

## Summary and Outlook

***Summary.*** This paper aimed to address the question *how shadow IT affects the power balance in organizations*. Based on a case study of a financial institute, we observed two counteracting tendencies. First, we found that shadow IT strengthens the power base of end users and business units by giving them effective means to perform their own workflows. This triggers a gradual process of continued power decline of the central IT unit because it is exposed to less and less context-specific business knowledge and is thus perceived as a less and less relevant partner for the business units. We used the term "governance problem" to label this tendency. However, IT units may counteract the "governance problem" by exploiting the tendency that the design of shadow IT systems often makes them vulnerable to risks as they contain errors and have not been designed in a sustainable manner. Formal risk management programs may thus be seen as means for the central IT unit to regain power by constructing risks (that may have not been obvious before) leading to the decommissioning of shadow IT systems. Both cycles concur and at times one tendency may surpass the other. However, the weakening tendency of formal programs may not be sufficient to stop the shadow IT cycle spinning if they do not address the underlying causes for the emergence of shadow IT. These findings are relevant for research on shadow IT as they highlight a long-term perspective on shadow IT. By doing so, we draw attention to cyclic trends favoring the continued emergence and decline of shadow IT instead of the dominant view that focusses on a single system lifecycle perspective (e.g. Behrens 2009) and short-term governance interventions (e.g. Zimmermann et al. 2014). Moreover, our contribution was to conceptualize 'risk' as a means of pressure by the central IT and as a power-shifting construct.

***Limitations and outlook.*** Before sketching implications for broader lines of IS theory and practice, we emphasize three conditions that limit the transferability of the findings we have presented. First, our study was located in the financial services industry, which affects the proposed theoretical relationships. Although we presented reasonably general drivers for the emergence of shadow IT, our model however assumes that the company is profit-driven and is operating in a knowledge-intensive setting. These assumptions may be too restrictive in some industries and public organizations. However, we believe that it characterizes one important mode of doing business in the contemporary world. Second, our study was restricted to one case of a 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 (see Winkler and Brown 2014) to account for options of one IT unit substituting for resource shortcomings of another as a means to mediate the link between cost pressure and shadow IT. Our view may also be limited with respect to firms with more federal structures (see Sambamurthy and Zmund 1999). Third, our study was restricted to a limited number of interviews and observations and further data collections could add an interdepartmental perspective to power struggles which has not been part of the present study. As a next step, future effort could be devoted to quantification (e.g. by system dynamics) to observe cycle times and to achieve measurability of the presented cycles.

***Theoretical implications.*** Our findings have broader implications for the debate on IT governance (Tiwana et al. 2013). As a consequence of the underlying tension between responsiveness and scale (Brown

and Magill 1994; Sambamurthy and Zmund 1999), organizations tend to reproduce the pattern of oscillating between centralized and decentralized forms of organizing IT (King 1983; Winkler and Brown 2014). We add nuance to the debate on cyclic trends in IT governance by illustrating how managerial actions aiming at achieving the goal of reducing costs and becoming more competitive can overshot and result in a "governance problem", advancing our understanding of the mechanisms that create misalignment between business and IT. In particular, we identify shadow IT as part of a vicious cycle and unintended, emergent consequence of continued cost and time pressures. We further added to the debate by positioning risk as a power-shifting construct and we showed that deliberate risk management programs may be insufficient to effectively weaken the "vicious circle" toward shadow IT. To reduce the long-term trend toward shadow IT, we thus advocated for the importance of building decent working relationship between business and IT as a means to enhance "operational" alignment (Gerow et al. 2014).

***Practical implications.*** Practically, our main contribution was to show that organizational programs to discontinue shadow IT will 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 weaken the cycle of new shadow IT emerging temporarily but they do not stop the cycle spinning. Studies on shadow IT often advise organizations to acknowledge and address the risks that shadow IT brings (Silic and Back 2014; Walters 2013). They have also suggested valuable procedures to identify and reduce the amount of shadow IT systems (Zimmermann and Rentrop 2014; Zimmermann et al. 2014). Yet, we have seen from this study that such measures do not develop their full potential if they do not address the underlying causes for the emergence of shadow IT. Based on our findings, our suggestions are thus two-fold. First, we suggest that organizations could do better by providing end users appropriate channels to translate their ideas into practice. Second, we believe that organizations should flank shadow IT campaigns with investment 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.

## REFERENCES


Alter, S. 2014. "Theory of Workarounds," *Communications of the AIS* (34: Article 55), pp. 1041–1066.

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

Bostrom, R. P., and Heinen, J. S. 1977. "MIS Problems and Failures: A Socio- Technical Perspective PART II : The Application of Theory," *MIS Quarterly* (1:4), pp. 11–28.

Bothner, M. S., Smith, E. B., and White, H. C. 2010. "A Model of Robust Positions in Social Networks," *American Journal of Sociology* (116:3), pp. 943–992.

Brown, C. V, and Magill, S. L. 1994. "Alignment of the IS Functions with the Enterprise: Toward a Model of Antecedents," *MIS Quarterly* (18:4), pp. 371–403.

Burton-Jones, A., McLean, E. R., and Monod, E. 2015. "Theoretical Perspectives in IS Research," *European Journal of Information Systems* (24:6), pp. 664–679.

Coltman, T., Tallon, P., Sharma, R., and Queiroz, M. 2015. "Strategic IT Alignment: Twenty-five Years on," *Journal of Information Technology* (2015:30), pp. 91–100.

Eisenhardt, K. M. 1989. "Building Theories from Case Study Research," *Academy of Management Review* (14:4), pp. 532–550.

Foucault, M. 1995. *Discipline & Punish: The Birth of the Prison*, New York: Vintage Books.

Furneaux, B., and Wade, M. 2011. "An exploration of organizational level information systems discontinuance intentions," *MIS Quarterly* (35:3), pp. 573–598.

Fürstenau, D., and Rothe, H. 2014. "Shadow IT systems: discerning the good and the evil," in *ECIS 2014 Proceedings*.

Gerow, J. E., Grover, V., Thatcher, J., and Roth, P. L. 2014. "Looking Toward the Future of IT-Business Strategic Alignment Through the Past: A Meta-Analysis," *MIS Quarterly* (38:4), pp. 1159–1185.

Gioia, D. A., Corley, K. G., and Hamilton, A. L. 2012. "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," *Organizational Research Methods* (16:1), pp. 15–31.

Gregory, R. W., Keil, M., Muntermann, J., and Mähring, M. 2015. "Paradoxes and the Nature of Ambidexterity in IT Transformation Programs," *Information Systems Research* (26:1), pp. 57–80.

Györy, A., Cleven, A., Uebernickel, F., and Brenner, W. 2012. "Exploring the shadows: IT governance approaches to user-driven innovation.," in *ECIS 2012 Proceedings*.

Haag, S., Eckhardt, A., and Bozoyan, C. 2015. "Are Shadow System Users the Better IS Users ? – Insights of a Lab Experiment," in *ICIS 2015 Proceedings*, pp. 1–20.

Hauke, G. 2006. "Values in Strategic Brief Therapy: From Need to Value-directed Living," *European Psychotherapy* (6:1), pp. 77–115.

Henrich, J., and 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), pp. 165–196.

Jasperson, J., Carte, T. A., Saunders, C. S., Butler, B. S., Croes, H. J. P., and Zheng, W. J. 2002. "Review: Power and information technology research: A metatriangulation review," *MIS Quarterly* (26), pp. 397–459.
Jones, D., Behrens, S., Jamieson, K., and Tansley, E. 2004. "The rise and fall of a shadow system: Lessons for enterprise system implementation," in *ACIS 2004 Proceedings*.
Karpovsky, A., and Galliers, R. D. 2015. "Aligning in practice: from current cases to a new agenda," *Journal of Information Technology* (2015:30), pp. 1–25.
King, J. L. 1983. "Centralized versus decentralized computing: organizational considerations and management options," *ACM Computing Surveys* (15:4), pp. 319–349.
Levina, N., and Orlikowski, W. 2009. "Understanding shifting power relations within and across organizations: A critical genre analysis," *Academy of Management Journal* (52:4), pp. 672–703.
Maguire, S., and Hardy, C. 2013. "Organizing Processes and the Construction of Risk: a Discursive Approach," *Academy of Management Review*, (56:1), pp. 231–255.
Markus, M. L. 1983. "Power, Politics, and MIS Implementation," *Communications of the ACM* (26:6), pp. 430–444.
Mell, P., and Grance, T. 2011. "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," No. 800-145, NIST Special Publication, Gaithersburg, MD.
Miles, M. B., and Huberman, A. M. 1994. *Qualitative data analysis* (2nd ed.), Thousand Oaks, Calif: SAGE.
Miller, K. W., Voas, J., and Hurlburt, G. F. 2012. "BYOD," *IT Professional* (14:5), pp. 53–55.
Panko, R. R. 2006. "Spreadsheets and Sarbanes-Oxley: Regulations, risks, and control frameworks," *Communications of the Association for Information Systems* (17:29), pp. 647–676.
Perlow, L. A. 1999. "The Time Famine: Toward a Sociology of Work Time," *Administrative Science Quarterly* (44:1), p. 57-81.
Power, M. 2009. *Organized Uncertainty: Designing a World of Risk Management*, New York: Oxford Univ. Press, US.
Raden, N. 2005. "Shedding light on shadow IT: Is Excel running your business?," No. January 2005, *DSSResources.com* (http://dssresources.com/papers/features/raden/raden02262005.html).
Rains, J. 2015. "Shadow IT: The Impact on Technical Support and the Opportunities for IT," *HDI Research Brief* (http://www.informationweek.com/whitepaper/it-strategy/it-leadership/shadow-it:-the-impact-on-technical-support-and-the-opportunities-for-it/360263?gset=yes&).
Rentrop, C., and Zimmermann, S. 2012. "Shadow IT-Management and Control of Unofficial IT," in *ICDS 2012, The Sixth International Conference on Digital Society*, pp. 98–102.
Sambamurthy, V., and Zmund, R. W. 1999. "Arrangements for Information Technology Governance: A Theory of Multiple Contingencies," *MIS Quarterly* (23:2), pp. 261–290.
Silic, M., and Back, A. 2014. "Shadow IT - A view from behind the curtain," *Computers and Security* (45:14), pp. 274–283.
Spierings, A., Kerr, D., and Houghton, L. 2012. "What Drives the End User to Build a Feral Information System?," in *ACIS 2012 Proceedings*.
Strong, D., Volkoff, O., and Elmes, M. 2001. "ERP Systems, Task Structure, and Workarounds in Organizations," in *AMCIS 2001 Proceedings*.
Tanriverdi, H. 2005. "Information Technology Relatedness, Knowledge Management Capability, and Performance of Multibusiness Firms," *MIS Quarterly* (29:2), pp. 311–334.
Tiwana, A. 2009. "Governance-Knowledge Fit in Systems Development Projects," *Information Systems Research* (20:2), pp. 180–197.
Tiwana, A., Konsynski, B., and Venkatraman, N. 2013. "Special Issue: Information Technology and Organizational Governance: The IT Governance Cube," *Journal of Management Information Systems* (30:3), pp. 7–12.
Walters, R. 2013. "Bringing IT out of the shadows," *Network Security* (2013:4), pp. 5–11.
Weick, K. E. 1993. "The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster," *Administrative Science Quarterly* (38:4), pp. 628–652.
Weill, P., and Ross, J. W. 2004. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Boston and Mass: Harvard Business School Press.
Williams, R., and Pollock, N. 2012. "Research Commentary - Moving Beyond the Single Site Implementation Study," *Information Systems Research* (23:1), pp. 1–22.
Winkler, T. J., and 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), pp. 13–48.
Winkler, T. J., and Brown, C. V. 2014. "Organizing and Configuring the IT Function," in *Computing Handbook*H. Topi and A. Tucker (eds.) (3rd ed.), Boca Raton, Florida: Taylor & Francis Ltd, pp. 57.1–57.14.
Winter, S., Berente, N., Howison, J., and Butler, B. 2014. "Beyond the organizational 'container': Conceptualizing 21st century sociotechnical work," *Information and Organization* (2014:24), pp. 250–269.
Xue, Y., Liang, H., and Boulton, W. R. 2008. "Informaton Technology Governance in Information Technology Investment Decision Processes: The Impact of Investment Characteristics, External Environment, and Internal Context," *MIS Quarterly* (32:1), pp. 67–96.
Yin, R. K. 2013. *Case Study Research: Design and Methods Essential guide to qualitative methods in organizational research,* Applied Social Research Methods Series (5th ed., Vol. 5), Thousand Oaks, CA: Sage Publications.
Zimmermann, S., and Rentrop, C. 2014. "On The Emergence of Shadow IT - A Transaction Cost-Based Approach," in *ECIS 2014 Proceedings*.
Zimmermann, S., Rentrop, C., and Felden, C. 2014. "Managing Shadow IT Instances – A Method to Control Autonomous IT Solutions in the Business Departments," in *AMCIS 2014 Proceedings*.