Managing Shadow IT Instances – A Method to Control Autonomous IT Solutions in the Business Departments

Completed Research Paper

Stephan Zimmermann
Konstanz University of Applied Sciences
stephan.zimmermann@htwg-konstanz.de

Christopher Rentrop
Konstanz University of Applied Sciences
christopher.rentrop@htwg-konstanz.de

Carsten Felden
TU Bergakademie Freiberg
carsten.felden@bwl.tu-freiberg.de

Abstract

Information Technology (IT) used for business processes is not only provided by the organization's IT department. Business departments and users autonomously implement IT solutions outside of the organizational IT service management. This phenomenon is called Shadow IT. Opportunities for innovation and flexibility, and problems in security, compliance, and efficiency call for its management. Following design science research and guided by a multiple-case study, this paper provides a method to manage Shadow IT instances. The designed measures to identify, evaluate and control these are theoretically justified by informal organization research, risk maps, and Transaction Cost Theory. The modes to control Shadow IT instances, registration, coordination of related activities, or renovation, follow efficient and adaptive governance structures and consider risk-based parameters. Applying the method turns Shadow IT into a business-located IT, preserving the opportunities resulting from autonomy. The findings contribute to IT Governance research regarding IT activities at business and user level.

Keywords

Shadow IT, IT Governance, Transaction Cost Theory, Informal Organization, Risk Management.

Introduction

Two-thirds of IT managers acknowledge "Shadow IT" as an existing phenomenon in their organization (Smyth and Freeman 2007; Chejfec 2012). A reason is that business departments and users implement IT autonomously to support their processes. The importance of this long-standing phenomenon rises due to increasingly tech-savvy users, easy access to web-based solutions, and available end user computing tools (Barker and Fiedler 2011). Unlike formal solutions, which are registered in the configuration management and planned within the service portfolio (van Bon et al. 2007), Shadow IT is not embedded in the IT service management. "The term Shadow IT describes business process supporting IT systems, IT service processes, and IT staff. They are deployed autonomously within business departments and by IT users. Thereby, Shadow IT entities are involved neither technically nor strategically in the IT service management of the organization …" (Zimmermann and Rentrop 2012)[1]. Occurrences of Shadow IT are applications, spreadsheet and database solutions, cloud services, mobile devices, hardware, support structures, or a combination thereof. Shadow IT promises flexibility for the business and may leverage user-driven innovations (Behrens 2009). However, several managerial problems and inefficiencies occur (Behrens 2009). Processes in research and practice aim to manage Shadow IT and to deal with these

[1] An appropriate and differentiating definition of Shadow IT is missing in English literature. Therefore, a translated definition from a German-speaking reference had to be used in this paper.

opportunities and risks. The development of measurable indicators for Shadow IT management should be possible. Thus, this research aims towards the design and evaluation of a theoretically justified and practically applicable method to manage Shadow IT.

Information Systems (IS) research has begun to address Shadow IT in the domain of IT Governance (György et al. 2012). Existing approaches to deal with the phenomenon offer a fundamental IT Governance orientation. However, theory-based and empirically tested mechanisms to implement and specify these approaches are missing. In this context, our research contributes to the discussion on autonomy and the allocation of decision rights and IT activities in the scope of IT and business departments. This provides a practical insight into the definition of IT Governance structures and extends the related research.

In the following chapter we discuss the status quo, refine the problem, and derive research questions. We then describe our research approach with its theoretical background regarding informal organization, risk management and Transaction Cost Theory, and the applied design science methodology. Next, we present the multiple-case study, which guided the method design and evaluation, we outline developed steps and measures, demonstrate their application, and evaluate the final method. Hereafter, we discuss the results in an IT Governance context. We conclude with a summary and implications for practice and research.

Status Quo

To identify relevant prior research we systematically reviewed literature (Webster and Watson 2002) on Shadow IT. *Shadow systems*, *feral systems*, *grey IT*, *rogue IT* and *hidden IT* are equivalent keywords used in literature for *Shadow IT*. We combined these with the keywords *information technology*, *information services*, *information systems* and *information security*, and queried several academic databases (EBSCOhost, ScienceDirect, ProQuest, IEEE Xplore, ACM Digital Library, AISeL, Jstor), IS journals (based on AIS senior scholars' basket) and proceedings of established IS conferences (ACIS, AMCIS, ECIS, HICSS, ICIS, PACIS) limited to abstract, title, and keywords. From initially 33 hits a total of 17 papers remained after removing duplicates and irrelevant papers. Finally, we conducted a backward and a forward search to avoid missing references.

The review results show that discussion on Shadow IT has grown in recent years. Contributions focus on the phenomenon and its risks and opportunities (Behrens 2009; Shumarova and Swatman 2008). Examples for risks are hazards to IT security (Walters 2013) or compliance (Silvius and Dols 2012), and inefficiencies during Shadow IT implementations or in the handling of business and other IT service processes (Jones et al. 2004). However, not just negative, also positive effects have been highlighted, such as flexibility or innovation potential (Behrens 2009). Several contributions describe general drivers for the emergence of the phenomenon, like misalignment (György et al. 2012; Behrens and Sedera 2004; Jones et al. 2004), power aspects (Spierings et al. 2012; Kerr et al. 2007) or individual behavior (Ortbach et al. 2013). Only few papers can be found on how to deal with the phenomenon. György et al. (2012) derive fundamental IT Governance approaches regarding Shadow IT from the perspective of top managers in practice. According to this, organizations follow IT-control, user-orientated, or user-driven approaches. Other authors introduce general potentials of and policies for a convergence between the enterprise architecture and Shadow IT (Tambo and Baekgaard 2013) and procedural approaches to access Shadow IT (Rentrop and Zimmermann 2012a, 2012b). These concepts present a part of necessary steps, but need to be theoretically founded and empirically investigated.

Thus, the challenge for research and practice is to develop more fine-grained approaches to measure Shadow IT related issues, to manage the phenomenon in consideration of its risks and opportunities, and to redefine adaptive and efficient IT Governance structures, processes and rights (Weill and Ross 2004) regarding IT autonomy for business departments and users. To progress in the questions of management and governance mechanisms, it is of interest to have a closer look at existing Shadow IT instances and how to control them. This research aims to develop a method to manage these instances with theoretically justified and practically applicable steps based on the following research questions (RQs):

RQ1: What measures are necessary to manage Shadow IT instances?

RQ2: How can organizations define adaptive and efficient IT Governance structures for autonomous IT solutions in the business departments?

Research Approach

This chapter describes the theoretical background for designing the method to manage Shadow IT instances. We present similarities of Shadow IT and informal organizational structures, we explain the connection to risk management, and introduce transaction cost arguments to explain Shadow IT emergence. Furthermore, we present the applied design science research approach based on a multiple-case study and show that this methodology is appropriate.

Theoretical Background

Shadow IT characteristics can be viewed similar to those of informal organizational structures (Selznick 1948), which emerge besides mandated formal structures and represent connections, attitudes or procedures of employees such as social networks or unofficially executed processes (Nadler et al. 1992; Chan 2002). Both, Shadow IT and informal structures, differ from formal rules. They result from peoples' need to fill gaps in formal structures to cope with tasks (Behrens and Sedera 2004, Chan 2002) or to substitute neglected formal structures (Rank 2008). Both phenomena usually emerge spontaneously, driven by employees on the bottom-level. Informal structures are seen as indispensable in organizations (Barnard 1968) as part of the governance (Williamson 1994). They are important for the adaptability and performance, but similar to Shadow IT also induce problems due to the violation of rules, inconsistencies with formal structures, and their lack of transparency (Soda and Zaheer 2012; Gulati and Puranam 2009). Informal structures are difficult to control because of their invisibility, however, their management seems to be necessary due to their importance (Cross and Prusak 2002; Nadler et al. 1992). Therefore, research examines approaches to access, measure, evaluate, and control informal structures (Tichy et al. 1979; Krackhardt and Hanson 1993; Nie et al. 2010), which can be applied to manage Shadow IT.

Another basis for Shadow IT management can be found in risk management research. Risk management focuses on the understanding and managing of uncertainties and hazards (DeLoach 2000). Prior research on Shadow IT has shown that several risks can occur within its implementation and utilization (Behrens 2009). Thus, instruments of risk management may be valuable to manage Shadow IT instances and related risks. Popular and convenient instruments to analyze risks are risk maps (Cox 2008). They illustrate single risks in a portfolio regarding the categories probability of occurrence and impact. The evaluation is based on statistical analysis and subjective interpretations. The classification recommends management actions and priorities to mitigate or to monitor risks (Norrman and Jansson 2004).

Understanding the reasons why Shadow IT emerges is important to manage it. Besides aspects of power (Spierings et al. 2012) or individual behavior (Ortbach et al. 2013), Transaction Cost Theory is valuable in this context (Zimmermann and Rentrop 2014). Shadow IT results from the decision of business departments and users to fill gaps in the offered formal IT and thus, to improve their work performance (Behrens and Sedera 2004). This decision results from two options on how the business side can fulfill an IT need: Either implementing a solution autonomously or formally initiating a demand at the IT department. This option represents a make-or-buy decision (Walker and Weber 1984) substantiated in Transaction Cost Theory (Coase 1937; Williamson 1975). Transaction costs to organize economic exchange occur in addition to the production costs for the exchanged capabilities themselves (Coase 1937). This concept is used to explain why institutions insource or outsource capabilities. Thereby, transaction costs are influenced by the bounded rationality and opportunism of the actors (Williamson 1985). The transactions vary in their asset specificity, uncertainty and frequency (Williamson 1985). Based on this differentiation, the theory aims at organizing transactions in the most efficient way and simultaneously at maintaining organizational adaptation to environmental changes by using governance structures (Williamson 2005). From the perspective of business departments and users, transaction costs exist in the internal exchange relation with the IT department when requesting for an IT solution. If they assume that the transaction costs for the exchange process are higher than their own initial production costs for an autonomous solution, they implement Shadow IT. Thereby, due to their bounded rationality, they cannot evaluate if this is beneficial from the perspective of the entire organization. Thus, the principles of Transaction Cost Theory may be valuable to find adaptive and efficient governance structures in this internal relation of business and IT department (Zimmermann and Rentrop 2014).

Research Methodology

The study follows design science research (Hevner et al. 2004). The primary goal is to develop a new artefact and thereby to address the research questions. The process of building artefacts in terms of a prescription-driven research is applicable to solve management problems (Van Aken 2004; Gregor and Jones 2007). By demonstrating procedural steps and measures, the proposed IS artefact represents a method focusing on an organizational issue (Braun et al. 2005). The artificial process behind the method construction follows the approved paradigm of design theory (March and Smith 1995; Peffers et al. 2008).

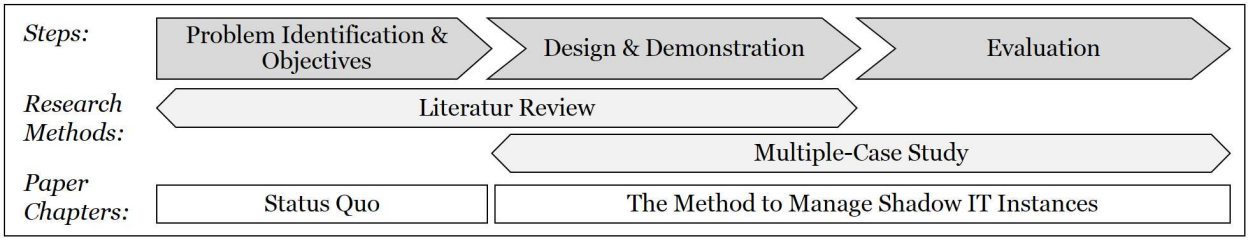

Figure 1. Research Methodology: Design Science Process based on Peffers et al. (2008)

The artefact objectives specify the needs in order to solve the identified problem, to design a satisfying method, and to demonstrate and evaluate it (Figure 1). The above status quo on Shadow IT outlines the problem identification and objectives. Design and demonstration of the research are justified by using a theoretical foundation and exploratory evidences from a multiple-case study (Yin 2014). Due to the complexity of the topic, iterations of three case studies were necessary starting with a prototype method based on prior research and the working experiences of the authors with Shadow IT (Flick 2009). Finally, the method is evaluated using qualitative evidences to prove its utility, quality and efficacy (Hevner et al. 2004). Following this process, we aim to ensure the conduction of good method design. Figure 2 summarizes our research foundation based on the design science research cycle model of Hevner (2007).

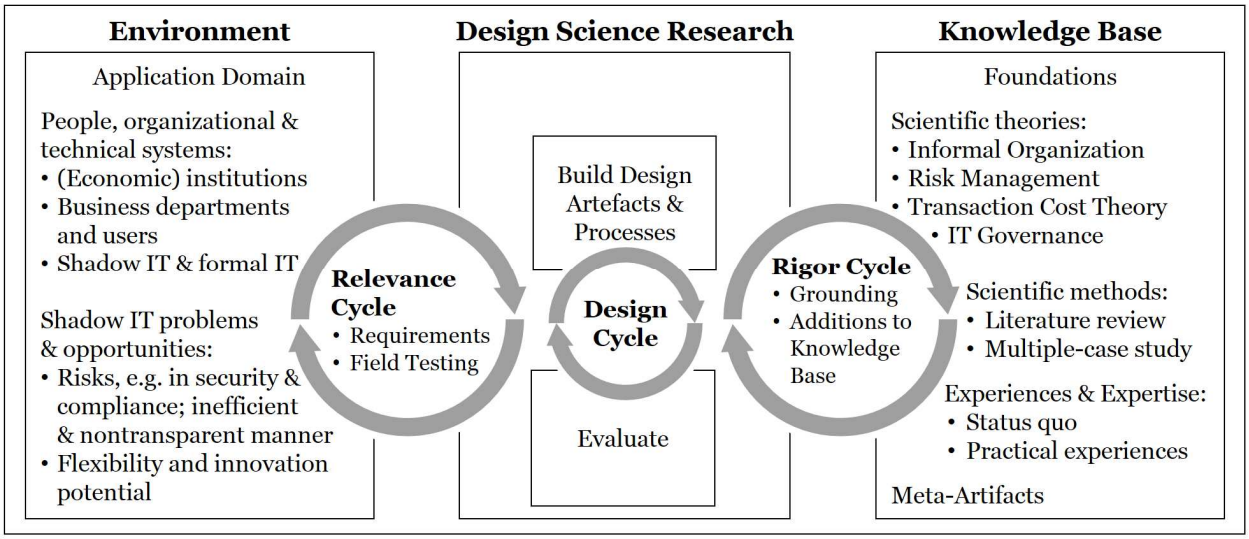

Figure 2. Research Foundation: Design Science Research Cycles based on Hevner (2007)

The Method to Manage Shadow IT Instances

Based on the problem identification in the status quo, this chapter presents the realization of the artefact design. After describing the multiple-case study, we provide an overview of the method including the theoretical justification of each step and the demonstration in the cases. Finally, we evaluate the method.

Multiple-Case Study

A multiple-case study guided the method design and evaluation. Case studies enable an in-depth analysis of a phenomenon in its real environment and a multiple structure is often considered as more compelling (Yin 2014). To facilitate theoretical and literal replication (Yin 2014) we used a purposive sampling strategy. For comparison reasons and to facilitate continuity we selected 3 German and Swiss companies. By designing and evaluating the intended method consecutively based on each case, we reached the point of saturation (Corbin and Strauss 2008) after the third case. As we aimed at a method that can be applied for different economic institutions and business processes, we chose companies from various industries and analyzed different processes and departments (Table 1). Relying on our research questions, different Shadow IT instances from multiple cases represent the multiple units of analysis.

	Industry	Country	Employees	Selected Processes / Departments	Informants
A	Insurance	Switzerland	1.300	Benefits Statements	Business: 2; IT: 1
B	Engineering	Germany	47.500	Order Management (Manufacturing Unit)	Business: 5; IT: 5; Management: 3
C	Electronic manufacturer	Germany	5.500	Corporate Marketing	Business: 3; IT: 1; Management: 2

Table 1. Multiple-Case Study: Company Profiles

The case studies were conducted consecutively between July 2012 and June 2013, each spanning 3 to 4 months. The case studies B and C were initiated with the executive management and the IT department, case study A merely with the IT department. We used data triangulation techniques by applying internal documents (process models, manuals), technical artefacts (software inventory tools, help desk reports), interviews, and contextual observations as sources of evidence (Yin 2014). This triangulation of multiple perspectives (Denzin 2009) was important because of the hidden character of Shadow IT and as the newly constructed measures affect different organizational groups. Employees from the IT departments assisted in building the basic knowledge about the enterprise architecture. In each case at least two business informants with a detailed perspective on the relevant business activities and deployed IT solutions were interviewed. The results were reviewed and the method was evaluated in several feedback loops with the informants and in a final discussion with the involved parties.

Method Design

This section describes each step to manage Shadow IT instances including the theoretical justification and the demonstration based on the case studies (see Table 2). The details of demonstration also serve as a proof-of-concept (Peffers et al. 2008) and are applied for the subsequent evaluation.

<table>
<tr><td></td><td colspan="3">Steps to manage Shadow IT instances</td><td></td></tr>
<tr><td>Theory basis</td><td>1) Identification</td><td>2) Evaluation</td><td>3) Control</td><td></td></tr>
<tr><td>Informal organization</td><td>Sources: technical analysis, documents, interviews</td><td rowspan="2">Evaluation portfolio
Criteria:
– Relevance & criticality
– Quality
– Size</td><td rowspan="3">Control alternatives:
– Registration in IT service management
– Renovating the instance
– Coordinating activities between business & IT
Functional/technological consolidation & prioritization</td><td rowspan="3">Demonstration details</td></tr>
<tr><td>Risk map</td><td></td></tr>
<tr><td>Transaction Cost Theory</td><td colspan="2"></td></tr>
</table>

Table 2. Method Overview

Step 1: Identify Shadow IT Instances in the Business Processes

To identify Shadow IT instances in each case, we initially used techniques from enterprise architecture documentation (Lankhorst 2009; Rentrop and Zimmermann 2012a) and sources of evidence proposed by case study research (Yin 2014). Manuals and process models (Cases A, B), existing architecture documentations and service catalogues (Cases A, C), software inventory tools (Case C), and service desk reports or former queries on Shadow IT (Cases B, C) allow an initial identification of IT solutions and the distinction of formal and shadow solutions. IT informants verified and complemented the results of this preliminary stage. Afterwards business informants with strong knowledge in their field of activities were interviewed following pre-tested, semi-structured guidelines (Myers and Newman 2007). Each interview took 1 to 2 hours. The developed interview guidelines address the explanation of the interview goal to identify all IT solutions supporting the business processes and questions about the identified Shadow IT. These questions focus on the description of each instance and its relation to the process, to other solutions, to data flow and to supporting and developing activities. Based on the answers, process support maps (Buckl et al. 2007) were drawn including the Shadow IT instances and their components. Based on Case B, Figure 3 exemplarily illustrates how the results can be presented. With this procedure, 6 Shadow IT instances were identified in Case A, 52 in B and 41 in C. Business and IT informants were interviewed a second time to confirm the results, to detail the descriptions and in preparation for the next step.

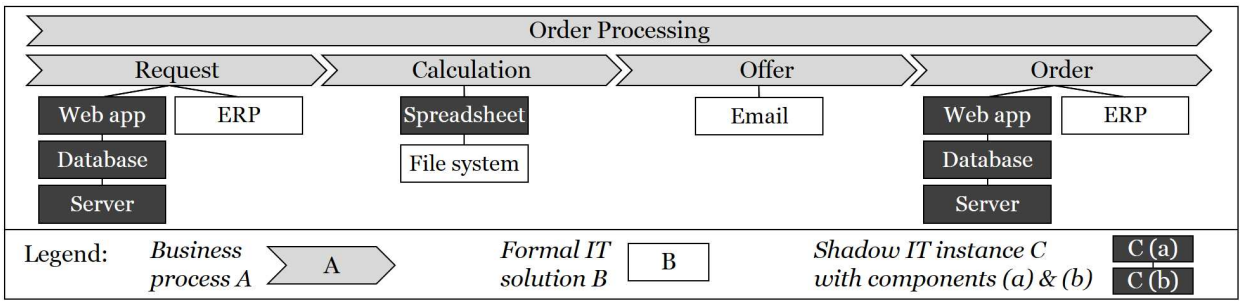

Figure 3. Process Support Map with Shadow IT

Step 2: Evaluate the Shadow IT Instances

Based on step 1 and the second turn of interviews, step 2 covers the evaluation of the identified instances. This procedure follows research to evaluate informal structures (Krackhardt and Hanson 1993; Nie et al. 2010). Derived from the connection of Shadow IT and risk management, the evaluation itself can be achieved by applying the principles of risk maps as a convenient instrument to analyze risks (Cox 2008).

For each case a detailed evaluation of Shadow IT instances was determined and transferred into a portfolio (Rentrop and Zimmermann 2012b). In the final version (Figure 4), the portfolio illustrates on the y-axis the aggregation of relevance and criticality of an instance, representing the business impact in a risk map. These assessment criteria combine the sub-criteria strategic significance of the instance and its criticality for business processes, IT security, compliance, and official IT services. On the x-axis the quality of an instance is classified, which is related to the probability of occurrence in a risk map. Relevant items to evaluate the quality refer to the system itself, the engineering process, appending services, the information quality and the quality of process handling. Furthermore, the portfolio illustrates the size of each instance considering the number of users and the amount of engaged resources.

In the case studies each instance was evaluated based on its description and the formerly described feedback loop with the business and IT informants. By using a scoring model for the different sub-criteria (0 = low, 10 = high) and weighting them individually for each company, the instances were rated (Rentrop and Zimmermann 2012b). Due to the vague variables, this qualitative measurement followed a subjective interpretation. One informant from each analyzed business process and all IT informants were involved to achieve a high validity. In each case the resulting portfolio was discussed and adapted in a closing meeting, in Case A and B with all parties involved and in C with the IT informants and managers. Figure 4 presents the results from these three cases.

Step 3: Control the Shadow IT Instances

The purpose of evaluation is to build a basis to control each Shadow IT instance. Following informal organization research this is necessary to align informal structures with company goals (Krackhardt and Hanson 1993). Mechanisms to address informal structures vary from accepting them, promoting them, aligning them with formal processes, and trying to replace them (Krackhardt and Hanson 1993; Nie et al. 2010). Thus, the question is how informal structures need to be redesigned within the governance of an organization. For Shadow IT similar actions are conceivable (György et al. 2012; Tambo and Baekgaard 2013). Another basis for control can be derived from risk maps, which point out options of action (Cox 2008). Risks with a severe impact and a likely probability of occurrence are usually not tolerable. These risks should be mitigated. In case of a rare impact and a minor probability, the risks can be tolerated and should be monitored. In between these positions risk mitigation is optional. These risks should be kept as low as reasonably practicable, considering economic factors and proportionality (Bowles 2003).

Furthermore, principles from Transaction Cost Theory provide additional control arguments. Shadow IT results from prohibitively high transaction costs assumed by the business for the exchange relation with the IT department. The question is which governance structures are the most efficient and adaptive from the perspective of the entire organization (Williamson 2005). To answer this question and to overcome bounded rationality and opportunism of the actors, the characteristics of transactions, their asset specificity, uncertainty and frequency are important (Williamson 1985). According to Williamson (2005) unexpected adoptions become more difficult in case of bilateral dependency with an exchange partner if specific assets and resources are involved. In this situation an own production of services or components tends to be more efficient and adaptive. Uncertainty regarding future adaptions enforces this. Instead, in case of non-specific services or components and certainty, sourcing the service from a partner is advantageous. This also applies for frequently performed transactions, as economies of scale are achieved.

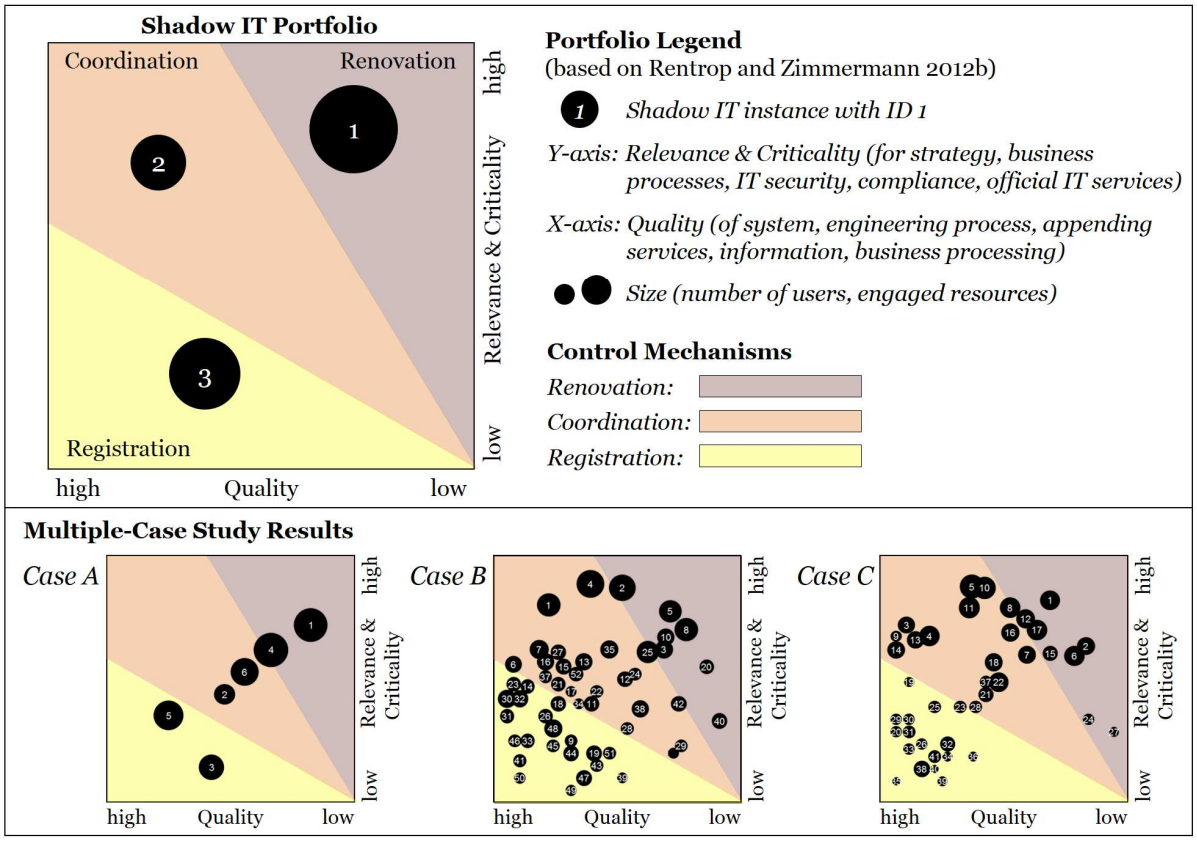

Figure 4. Evaluation and Control of Shadow IT Instances

Step 3 is a result of applying these theoretical perspectives. Based on the previous evaluation and the discussions with the involved parties, several control mechanisms were conducted for the identified instances. Resultant mechanisms are renovation, coordination, and registration (Figure 4). Other criteria like the degree of innovation or redundancies among the solutions (Rentrop and Zimmerman 2012b) can also support the prioritization of actions. In the case of not beneficial instances, their abandonment may be considered. However, in the case studies no solution of this kind was found.

Following the needs of action in risk maps, Shadow IT instances in the upper right corner of the portfolio are the most problematic ones. In the case studies there was a tendency to renovate them with IT support by rebuilding, by consolidating similar solutions, or by integrating into official solutions. E.g., in Case A, a self-developed, interdepartmental solution to handle open customer issues was replaced by a workflow system. In Case B, the involved parties decided to rebuild and integrate an innovative, web-based product database into the official IT architecture. This solution was originally developed by the business department and hosted on an autonomously sourced web server.

For those Shadow IT instances with a high relevance and a relatively high level of quality, IT activities were newly coordinated between business and IT department. The aim was to find the best form of organizational exchange based on transaction cost principles as widely discussed in this field of research (Williamson 2005). This coordination focuses on the question which activities should stay within the business, preserving an informal character, and which should be transferred to the IT department. This allocation issue can be resolved based on the asset specificity, the frequency, and the uncertainty of activities related to a Shadow IT instance. A typical example from Cases B and C was the adoption of hardware-related tasks by the IT department, while other activities of these Shadow IT instances remained in the business. This new allocation was justified by the low asset specificity of hardware-related tasks from the business perspective and the frequently performed and experienced activities for these tasks in the IT. Other examples of such task transfers appeared when different technologies were used for Shadow IT. As the IT department had capabilities to standardize and to integrate solutions – non-specific for a particular business department and frequently executed – the activity of technology consolidation better fit for the IT. In contrast, asset specific activities were kept in the business, e.g., solutions with specific calculations and thorough business knowledge requirements. Also less frequently executed tasks, e.g., conforming rarely used spreadsheet solutions, were assigned to the business. Finally, most activities stayed in the business for instances with an uncertain usage in the future, like prototypes or ideas. These examples show how autonomy in the business can be kept. Thus, the positive effects of Shadow IT, its adaptability and innovative potential are revealed. Furthermore, in achieving a better fit of task allocation and professionalism, production and transaction costs are reduced. Additionally, risks are also mitigated using this form of coordination, as IT activities are reallocated in considering the impact of an instance.

Finally, instances in the lower left corner of the portfolio with relativity high quality are located in an area of possible acceptance following risk map argumentation. Examples from the case studies were autonomously sourced applications, hardware devices, simple shop-floor IT and small spreadsheet solutions. In the case studies, those instances were registered in the IT service management and further monitored. The action of a mere registration is also supported by Transaction Cost Theory. These instances are mostly small and the de facto production costs tend to be lower from a global organizational view than necessary transaction costs in the exchange with the IT department.

Figure 4 illustrates the control mechanisms as areas in the portfolio and the case study results. The control step requires at least to bring and keep the instances out of the shadow, turning them into a business-located IT. The scale of the three areas may depend on the fundamental IT Governance orientation of an organization in considering IT-control, user-orientated or user-driven approaches to address Shadow IT (György et al. 2012). Nevertheless, for the three cases no specific approaches existed.

Method Evaluation

Evaluating new IS artefacts is a substantial element in design science research to show "how well does it work" (March and Smith 1995). In this section we therefore examine the utility, quality and efficacy of the designed method (Hevner et al. 2004).

The successful application in multiple cases proves the method's utility. This can be seen in the demonstration of each step (Peffers et al. 2008), and in the assessment by the involved parties of each

case. With the final design, both research questions raised in the problem identification can be answered. The artefact describes the necessary measures to manage Shadow IT instances considering the positive and negative effects (RQ1). Allocating activities for business-located IT based on specificity, frequency and uncertainty indicates the definition of efficient and adaptive governance structures (RQ2). The artefact output has met our objectives to develop a practically applicable and theoretically justified method.

The results from 17 interviews with feedback loops yielded that the method is easy to apply, risks are reduced, transparency rises, task execution becomes more efficient, and Shadow IT opportunities are realized due to a high business autonomy. Furthermore, the method can be conducted with low efforts. The participants interpreted the method results as a snap-shot of the current situation as well as a good foundation for the further definition of IT Governance regarding Shadow IT. As the last step of evaluation we compared the final method with all gathered case evidences to proof its reliability and validity.

Discussion

The designed method contributes to IT Governance research. It enables managers to turn Shadow IT instances into a governed business-located IT. In contrast, prior research focuses on a fundamental orientation to address Shadow IT but not on the implementation of these approaches (György et al. 2012; Tambo and Baekgaard 2013). By focusing on the instances' relevance and quality in the designed method, a prioritization of action is conducted. Transparency in the enterprise architecture is ensured due to the Shadow IT identification and registration. The instances are not excluded from IT service management anymore and thus, outside of the shadow. Risks are mitigated due to the renovation of problematic solutions. Finally, the flexibility and innovative capacity behind Shadow IT is not given away. Instead, coordination realigns the instance-related activities. In allocating the activities between business and IT departments adaptability is kept, efficiency and professionalism are increased.

Focusing the question "who executes which activities" extends the research discussion on IT Governance structures (Weill and Ross 2004) to decision rights on the business and user level as well as on the level of an individual IT solution. Applying transaction cost principles provides the most efficient and adaptive way to answer this question. Allowing business-located IT activities or solutions realizes the opportunities of autonomy and thus, increases the contribution of IT to competitive advantages. Furthermore, the designed method fosters the harmonization process of business IT alignment (Luftman 2000). Necessary user-driven solutions and needs are exposed, communication between the involved parties is encouraged, and the business side is integrated in IT-specific challenges.

Although the method focuses on existing instances, the results are valuable for upcoming Shadow IT and the definition of IT Governance structures, processes and rights in this context. Organizations can apply the argumentation of the control step to organize occurring ideas and needs for IT solutions on business and user level. Policies for business-located IT can be derived and structures and processes to support business-located IT can be developed. This reveals the opportunities of business autonomy for IT.

Conclusion

The method to manage Shadow IT instances designed in this paper presents a management artefact to identify and evaluate the current Shadow IT in organizations as well as to derive ways to control the instances found, which is necessary due to various risks and opportunities of Shadow IT. The modes of control follow the implementation of governance structures in the most efficient and adaptive way and in consideration of risk-based parameters. Preserving Shadow IT opportunities in this process means that certain activities of a Shadow IT instance stay in the business departments, while others are transferred to the IT department. The allocation depends on the asset specificity, frequency and uncertainty of the IT activities related to the considered instance. The research results contribute to IT Governance research and imply that governance structures for IT activities need to be extended on business and user level. Decision-makers and researchers addressing the question of business autonomy for IT may use these insights to adjust governance concepts and to improve business IT alignment.

The selection of cases might pose some limitations for this research. Generalization could be enhanced by investigating more cases from other industries and with a different governance orientation. Another limitation might be the focus on companies from Germany and Switzerland. Furthermore, we participated

in the discussions during the design process. We are aware of this interviewer bias and tried to reduce it through involving several parties and experts. Finally, our research is solely based on qualitative data as the vague variables of Shadow IT, transaction costs and risk parameters are difficult to quantify.

Based on the designed method, further research may focus on the long-term management of Shadow IT and thus on IT Governance policies for business-located IT. Furthermore, questions in enterprise architecture management appear about how to guarantee a continuous recording and monitoring of decentralized business-located IT and how to provide suitable technologies for user-driven processes. Prior research on end user computing platforms can be valuable for this. Finally, further research on user-driven IT innovations may focus on the promotion of business-located processes, the distribution of innovations into the organization and the hand-over process to the IT department for established solutions. Within the scope of Shadow IT and IT Governance, we believe the designed method and the achieved insight in this paper provide an initial point for future research.

REFERENCES

Barnard, C. I. 1968. *The Functions of the Executive* (11th ed.), Cambridge, MA: Harvard University Press.

Barker, S., and Fiedler, B. 2011. "Decision Makers, Strategists or Just End-users? Redefining End-User Computing for the 21st Century: A Case Study," *Journal of Organizational and End User Computing* (23:2), pp. 1-14.

Behrens, S., and Sedera, W. 2004. "Why Do Shadow Systems Exist after an ERP Implementation? Lessons from a Case Study," in *Proceedings of the 8th Pacific Asia Conference on Information Systems,* Shanghai, China, Paper 136, pp. 1712-1726.

Behrens, S. 2009. "Shadow Systems: The Good, the Bad and the Ugly," *Communications of the ACM* (52:2), pp. 124-129.

Bowles, D. S. 2003. "ALARP evaluation: using cost effectiveness and disproportionality to justify risk reduction," in *Proceedings of the ANCOLD 2003 Conference on Dams*, pp. 89-104.

Braun, C., Wortmann, F., Hafner, M., and Winter, R. 2005. "Method construction - A core approach to organizational engineering," in *Proceedings of the 2005 ACM symposium on Applied Computing*, H. M. Haddad, A. Omicini, R. L. Wainwright, and L. M. Leibrock (eds.), Santa Fe, NM, pp. 1295-1299.

Buckl, S., Ernst, A., Lankes, J., Matthes, F., Schweda, C., and Wittenburg, A. 2007. "Generating Visualizations of Enterprise Architectures using Model Transformations," *Enterprise Modelling and Information Systems Architectures* (2:2), pp. 1-12.

Chan, Y. E. 2002. "Why haven't we mastered alignment? The importance of the informal organization structure," *MIS Quarterly Executive* (1:2), pp. 97-112.

Chejfec, T. 2012. *Shadow IT survey v3*. http://chejfec.com/2012/11/03/shadow-it-infographic/shadow-it-survey-v3/. Accessed 24 February 2014.

Coase, R. 1937. "The Nature of the Firm," *Economica* (4:16), pp. 386-405.

Cox, A. L. 2008. "What's Wrong with Risk Matrices?" *Risk Analysis* (28:2), pp. 497-512.

Corbin, J.M., and Strauss, A.L. 2008. *Basics of Qualitative Research – Techniques and Procedures for Developing Grounded Theory* (3rd ed.), Los Angeles, CA: Sage Publications.

Cross, R., and Prusak, L. 2002. "The people who make organizations go-or stop," *Harvard Business Review* (80:6), pp. 104-112.

DeLoach, J. W. 2000. *Enterprise-Wide Risk Management: Strategies for Linking Risk and Opportunity*, London, UK: Financial Times/Prentice-Hall.

Denzin, N. K. 2009. *The research act*: *A theoretical introduction to sociological methods*, New Brunswick, NJ: AldineTransaction.

Flick, U. 2009. *An introduction to qualitative research* (4th ed.), Los Angeles, CA: Sage Publications.

Gregor, S., and Jones, D. 2007. "The Anatomy of a Design Theory," *Journal of the Association for Information Systems* (8:5), pp. 312-335.

Gulati, R., and Puranam, P. 2009. "Renewal through reorganization: The value of inconsistencies between formal and informal organization," *Organization Science* (20:2), pp. 422-440.

György, A., Cleven Anne, Uebernickel Falk, and Brenner, W. 2012. "Exploring the Shadows: IT Governance approaches to user-driven Innovation," in *Proceedings of the 20th European Conference on Information Systems,* Barcelona, Spain, Paper 222.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp. 75-105.

Hevner, A. R. 2007. "A Three Cycle View of Design Science Research," *Scandinavian Journal of Information Systems* (19:2), Article 4, pp. 1-6.

Jones, D., Behrens, S., Jamieson, K., and Tansley, E. 2004. "The Rise and Fall of a Shadow System: Lessons for Enterprise System Implementation," in *Proceedings of the 15th Australasian Conference on Information Systems,* Hobart, Australia, Paper 96.

Kerr, D., Houghton, L., and Burgess, K. 2007. "Power Relationships that Lead to the Development of Feral Systems," *Australasian Journal of Information Systems* (14:2), pp. 141–152.

Krackhardt, D., and Hanson, J. R. 1993. "Informal networks: the company behind the chart," *Harvard Business Review* (71:4), pp. 104-111.

Lankhorst, M. 2009. *Enterprise architecture at work*: *Modelling, communication and analysis*, (2nd ed.) Berlin, Germany: Springer.

Luftman, J. 2000. "Assessing Business-IT Alignment Maturity," *Communications of the Association for Information Systems* (4:1), Article 14.

March, S. T., and Smith, G. F. 1995. "Design and natural science research on information technology," *Decision Support Systems* (15:4), pp. 251-266.

Myers, M. D., and Newman, M. 2007. "The qualitative interview in IS research: Examining the craft," *Information and Organization* (17:1), pp. 2-26.

Nadler, D., Gerstein, M. S., Shaw, R. B., and Associates 1992. "Transforming the Informal Organization," in *Organizational Architecture*: D*esigns for Changing Organizations*, Nadler, D., Gerstein, M. S., Shaw, R. B., and Associates (eds.), San Francisco, CA: Jossey-Bass, pp. 133-135.

Nie, K., Lin, S., Ma, T., and Nakamori, Y. 2010. "Connecting informal networks to management of tacit knowledge," *Journal of Systems Science and Systems Engineering* (19:2), pp. 237-253.

Norrman, A., and Jansson, U. 2004. "Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident," *International Journal of Physical Distribution and Logistics Management* (34:5), pp. 434-456.

Ortbach, K., Bode, M., and Niehaves, B. 2013. "What Influences Technological Individualization? – An Analysis of Antecedents to IT Consumerization Behavior," in *Proceedings of the 19th Americas Conference on Information Systems,* Chicago, IL.

Rank, O. N. 2008. "Formal structures and informal networks: Structural analysis in organizations," *Scandinavian Journal of Management* (24:2), pp. 145-161.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2008. "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems* (24:3), pp. 45-77.

Rentrop, C., and Zimmermann, S. 2012a. "Shadow IT: Management and Control of unofficial IT," in *Proceedings of the 6th International Conference on Digital Society*, Valencia, Spain, pp. 98-102.

Rentrop, C., and Zimmermann, S. 2012b. "Shadow IT Evaluation Model," in *Proceedings of the Federated Conference on Computer Science and Information Systems,* Wrocław, Poland, pp. 1023-1027.

Selznick, P. 1948. "Foundations of the Theory of Organization," *American sociological review* (13:1), pp. 25-35.

Shumarova, E., and Swatman P. A. 2008. "Informal eCollaboration Channels: Shedding Light on "Shadow CIT"," in *Proceedings of the 21st Bled eConference*, Bled, Slovenia, pp. 371-394.

Silvius, A., and Dols, T. 2012. "Factors influencing Non-Compliance behavior towards Information Security Policies," in *Proceedings of the International Conference on Information Resources Management,* Vienne, Austria, Paper 39.

Smyth, K., and Freeman, J. 2007. *Blue Prism Rogue IT Survey 2007*. Blue Prism, 1-5.

Soda, G., and Zaheer, A. 2012. "A network perspective on organizational architecture: performance effects of the interplay of formal and informal organization," *Strategic Management Journal* (33:6), pp. 751-771.

Spierings, A., Kerr, D., and Houghton, L. 2012. "What Drives the End User to Build a Feral Information System?" *Proceedings of the 23rd Australasian Conference on Information Systems, Geelong, Australia*.

Tambo, T., and Baekgaard, L. 2013. "Dilemmas in Enterprise Architecture Research and Practice from a Perspective of Feral Information Systems," *Proceedings of the 17th IEEE Enterprise Distributed Object Computing Conference Workshops*, Vancouver, BC, Canada, pp. 289-295.

Tichy, N. M., Tushman, M. L., and Fombrun, C. 1979. "Social Network Analysis for Organizations," *The Academy of Management Review* (4:4), pp. 507-519.

Van Aken, Joan E. 2004. "Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules," *Journal of Management Studies* (41:2), pp. 219-246.

Van Bon, J., Jong, A. de, Kolthof, A., Pieper, M., Rozemeijer, E., Tjassing, R., van der Veen, A., and Verheijen, T. 2007. *IT Service Management*: *An Introduction*, Zaltbommel, Netherlands: Van Haren Publishing.

Walker, G., and Weber, D. 1984. "A Transaction Cost Approach to Make-or-Buy Decisions," *Administrative Science Quarterly* (29:3), pp. 373-391.

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

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), pp. 13-23.

Weill, P., and Ross, J. W. 2004. *IT Governance*: *How top performers manage IT decision rights for superior results*, Boston, MA: Harvard Business School Press.

Williamson, O. E. 1975. *Markets and hierarchies, analysis and antitrust implications*: *A study in the economics of internal organization*, New York: Free Press.

Williamson, O. E. 1985. *The economic institutions of capitalism*: *Firms, markets, relational contracting*, New York: Free Press.

Williamson, O. E. 1994. "Visible and Invisible Governance," *The American Economic Review* (84:2), pp. 323-326.

Williamson, O. E. 2005. "The Economics of Governance," *The American Economic Review* (95:2), pp. 1-18.

Yin, R. K. 2014. *Case study research*: *Design and methods* (5th ed.), Los Angeles, CA: Sage Publications.

Zimmermann, S., and Rentrop, C. 2012. "Schatten-IT," *HMD - Praxis der Wirtschaftsinformatik* (49:288), pp. 60-68.

Zimmermann, S., and Rentrop, C. 2014. "On the Emergence of Shadow IT – A Transaction Cost-Based Approach," in *Proceedings of the 22nd European Conference on Information Systems,* Tel Aviv, Israel.